A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

IP Solutions

Servicdokumentation
10/2025

P31003-H31B0-S100-06-0020

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Inhalt

1 Ziel dieses Dokumentes 23

2 Gateways HG 3500 und HG 3575 24
2.1 Begriffe 24
2.1.1 Schlüsselbegriffe 24
2.1.2 Fax- bzw. Modem-Übertragung und -Erkennung 27
2.1.3 Codec-Standards 28
2.1.4 Sprachqualität 28
2.1.5 Jitter-Buffer 31
2.1.5.1 Funktionalität des Jitter-Buffers 31
2.1.5.2 Modes des Jitter-Buffers 32
2.1.5.3 Abwägungen beim Einstellen der Verzögerung bei statischem Jitter-Buffer 33
2.1.5.4 Clock Drift bei statischem Jitter-Buffer 34
2.1.5.5 Minimalverzögerung bei adaptivem Jitter-Buffer 36
2.1.5.6 Paketverlustkontrolle bei adaptivem Jitter-Buffer 36
2.1.5.7 Parameter zur Konfiguration des Jitter-Buffers 37
2.1.6 Laufzeit und dadurch bemerkbare Effekte 38
2.1.6.1 Allgemeine Hinweis zur Verzögerung 38
2.1.6.2 Verzögerung und Echo 38
2.2 Architektur und Systemanforderungen 39
2.2.1 Voraussetzungen 39
2.2.2 Strombedarf 39
2.2.3 Netzwerk-Anforderungen 39
2.2.4 Netzwerkdaten 41
2.2.4.1 TOS Byte 42
2.2.5 Bandbreitenbedarf 47
2.2.5.1 Codierung 47
2.2.5.2 Samplingzeit 47
2.2.5.3 IP-Overhead 48
2.2.5.4 Bandbreitenbedarf pro Verbindung 48
2.2.5.5 Voice Activity Detection (VAD) 50
2.2.5.6 Hinweise zu DMC 51
2.2.6 B-Kanäle 52
2.2.6.1 B-Kanal-Konfiguration 54
2.2.6.2 Anzeige der aktuell verfügbaren/konfigurierten B-Kanäle (mögliche IP-basierte Verbindungen) 55
2.2.7 Verkehrsbezogene Hinweise 55
2.3 Unterstützte Gateways 56
2.3.1 HG 3500 (Common Gateway) 56
2.3.1.1 Allgemeine Informationen 56
2.3.1.2 Baugruppentausch 57
2.3.1.3 Leistungsumfang 58
2.3.1.4 Einschränkungen 61
2.3.2 HG 3575 62
2.3.2.1 Allgemeine Informationen 62
2.3.2.2 Baugruppentausch 62
2.4 Leistungsmerkmale und Einschränkungen 63
2.4.1 Direct Media Connection (DMC) 63
2.4.2 Sprachkomprimierung 64
2.4.3 Voice Activity Detection (VAD) 65
2.4.4 Comfort Noise Generation (CNG) 66
2.4.5 Echo-Cancellation 66

2.4.6 Redundante LAN-Schnittstelle..... 67
2.4.7 Security..... 67
2.4.7.1 Administrationszugriff..... 67
2.4.7.2 Zugriff auf SNMP..... 67
2.4.7.3 Sicherheit bei der CorNetTC Registrierung..... 67
2.4.7.4 Anschaltung der IP-Gateways im Internet bzw. über externe Provider..... 67
2.4.8 Ressource Manager (RM)..... 67
2.4.9 Einschränkungen..... 68
2.4.9.1 Loadware-Update oder Reset der Baugruppe..... 68
2.4.9.2 Mögliche IP-Hops..... 69
2.5 Ladekonzept der Gateway-Baugruppen..... 69
2.5.1 Wichtige Hinweise..... 69
2.5.2 Hinweise zur Loadware der IP-Gateways..... 69
2.5.3 Ladekonzepte..... 70
2.5.4 Update der Loadware mit Hilfe des Web Based Managements..... 71
2.5.5 Update der Loadware mit Hilfe des „LW Update Manager“..... 72
2.5.6 Allgemeine Hinweise zum Ladevorgang..... 73
2.6 Konfigurationsdaten im lokalen Flash speichern (local Backup & Restore)..... 73
2.6.1 Überblick..... 73
2.6.2 Leistungsmerkmalbeschreibung..... 73
2.6.3 Hochlauf-Szenarien..... 74
2.6.4 Konfiguration..... 75
2.6.5 Besonderheiten..... 76
2.7 Nachladbarkeit des FPGA auf der STMI4-/NCUI4- Baugruppe..... 76
2.8 Standby Board HG 3500..... 82
2.8.1 Leistungsmerkmalbeschreibung..... 82
2.8.2 Benutzeroberfläche..... 86
2.8.3 Serviceinformationen..... 86
2.8.4 Generierung..... 89
2.8.5 Service-Aktionen nach automatischer Umschaltung..... 93
2.8.6 Relevante AMOs..... 94
2.9 DLS-Client-Bootstrapping..... 99
2.9.1 Bootstrapping mit PIN Modus „Keine PIN“..... 99
2.9.2 Bootstrapping mit PIN Modus „Standard PIN“ oder „Individuelle PIN“..... 100
2.10 Zurücksetzen einer NCUI-Baugruppe..... 100
2.10.1 Gründe für das Zurücksetzen der NCUI..... 100
2.10.2 Methoden zur Übertragung der Loadware..... 100
2.10.3 Wichtige Hinweise..... 100
2.10.4 Verfahren..... 101
2.11 Zurücksetzen einer STMIX-Baugruppe..... 104
2.11.1 Allgemeine Beschreibung..... 104
2.11.2 Vorbereiten der erforderlichen Dateien..... 105
2.11.3 Tool-Konfiguration für das Flashen..... 106
2.11.4 STMIX USB-Konfiguration..... 110
2.11.5 STMIX-Reflash..... 112
2.11.6 STMIX- und STMIY-Werksreset..... 118
2.12 Gateway HG 3575 - Ändern der mit AMO STMIB einstellbaren Parameter..... 119
2.12.1 TYP GLOBAL - Ändern des Ruhebitmusters..... 120
2.12.2 TYP IFDATA - Ändern schnittstellenspezifischer Parameter des Access Point..... 121
2.12.3 TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang..... 122
2.12.4 TYP ASC - Ändern der Payload QoS-Einstellung des Access Points..... 124
2.12.5 TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP Paketgröße, Voice Activity Detection und T.38 Fax..... 125
2.12.6 TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen..... 126
2.12.7 TYP DSP - Jitterbuffergröße des Access Points..... 126

2.12.8 TYP DMCDATA - Ändern der Einstellung des Access Points für die Unterstützung von Direct Media Connections....126
2.12.9 TYP H323 - Ändern der H323-Einstellungen des Access Points....127
2.12.10 TYP JB - Konfiguration des Jitter-Buffers....128
2.12.11 TYP SIGQOS - Qualitätsüberwachung für die Signalisierungsverbindung über IP....128
2.12.12 TYP SNMP - Ändern der Community Strings für Lesezugriff....128
2.12.13 TYP MGNTDATA - Verwaltungsdaten und Backup-Server....131
2.12.14 TYP WBMDATA - Ändern von Login und Passwort für WBM....131
2.12.15 TYP GWSECTOR - Ändern der Sektor-Nummer des Access Points für den Resource Manager....132
2.12.16 TYPE DLSDATA - Konfigurieren von DLS Data....132
2.12.17 Rücksetzen der Parameter auf Default-Werte....133
2.13 Hinweise zum Einrichten eines Common Gateways HG 3500....133
2.13.1 Änderungen der Common Gateway Konfiguration....133
2.13.2 AMOs....134
2.13.3 Regeln....134
2.13.4 Einschränkungen....136
2.13.5 Konfigurationsschritte im Überblick....136
2.14 Gateway HG 3500 - Ändern der mit AMO CGWB einstellbaren Parameter....136
2.14.1 TYP ASC - Ändern der Payload QoS-Einstellung im Host System....137
2.14.2 TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP-Paketgröße und Voice Activity Detection....137
2.14.3 TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen....138
2.14.4 TYP DMCDATA - Ändern der Einstellung der HG 3500 für die Unterstützung von Direct Media Connections....138
2.14.5 TYP DSP - Ändern der DSP (Signalprozessor)-Einstellung einer HG 3500....139
2.14.6 TYP GLOBIF - Ändern des Ruhebitmusters und schnittstellenspezifischer Parameter....139
2.14.7 TYP GWSECTOR - Ändern der Sektor-Nummer der HG 3500 für den Resource Manager....140
2.14.8 TYP MGNTDATA - Verbindung zum OpenScape 4000 Assistant....141
2.14.9 TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang....142
2.14.10 TYP WBMDATA - Ändern von Login und Passwort für WBM....143
2.14.11 TYP JB - Konfiguration des Jitter-Buffers....143
2.14.12 Rücksetzen der Parameter auf Default-Werte....144
2.15 Codec-Einstellungen....144
2.15.1 HFA und Trunking....144
2.15.2 IPDA....145
2.16 Multiple Feature Support Konfiguration am Common Gateway (Beispiel)....146
2.16.1 Wichtige Hinweise / Einschränkungen....146
2.16.2 Konfiguration der Funktionsblöcke mit AMO BFDAT....146
2.16.3 Konfigurieren der Common Gateway Baugruppe mit AMO BCSU....151
2.16.4 Einrichten von SIP Trunking....153
2.16.5 Nicht abgeschlossener und abgeschlossener Funktionsblock....153
2.16.5.1 Nicht abgeschlossener Funktionsblock....154
2.16.5.2 Abgeschlossener Konfigurationsblock....155
2.17 Ressource Manager Funktionalität....155
2.17.1 Allgemeines....155
2.17.2 Schlüsselbegriffe....156
2.17.2.1 Sektor....156
2.17.2.2 Cluster....157
2.17.2.3 Sektor-Pfad....157
2.17.2.4 Definitionen....158
2.17.3 Konfigurationsregeln....159
2.17.4 Verwendete Bandbreiten....160
2.17.5 Einrichtung des Ressource Managements für eine HFA-Konfiguration....160
2.17.5.1 Ausgangssituation....161
2.17.5.2 Codec-Einstellungen für die HFA-Teilnehmer....162
2.17.5.3 Sektoren für das LAN/WAN....162

2.17.5.4 Zuordnung der HFA-Teilnehmer zu den Sektoren....163
2.17.5.5 Sektorpfade definieren....168
2.17.5.6 Sektorpfade zuordnen....168
2.17.6 Einrichtung des Ressource Managements für eine IPDA-Konfiguration mit TDM-Teilnehmern....178
2.17.6.1 Ausgangssituation....178
2.17.6.2 Sektoren für das LAN/WAN....179
2.17.6.3 Sektoren für die Gateways....179
2.17.6.4 Zuordnung der Gateways zu ihren Sektoren....180
2.17.6.5 Sektorpfad definieren....180
2.17.6.6 Sektorpfad zuordnen....180
2.17.7 Einrichtung des Ressource Managements für eine IPDA-Konfiguration mit TDM-Teilnehmern und HFA im Access Point....189
2.17.7.1 Ausgangssituation....190
2.17.7.2 Einstellungen für die HFA-Teilnehmer....191
2.17.7.3 Sektoren für das LAN/WAN....192
2.17.7.4 Sektoren für die Gateways....192
2.17.7.5 Zuordnung der HFA-Teilnehmer zu den Sektoren....193
2.17.7.6 Zuordnung der Gateways zu ihren Sektoren....193
2.17.7.7 Sektorpfade definieren....193
2.17.7.8 Sektorpfade zuordnen....193
2.17.8 Anmerkungen und Einschränkungen....199
2.17.9 Diagnose....200
2.18 Command Line Interface CLI beim HG 3500....200
2.18.1 Allgemeine Informationen....200
2.18.2 Allgemeine Operationen....201
2.18.3 Zugriffskontrolle....201
2.18.4 Gateway-Setup....201
2.18.5 Handling von Images/Dateien....202
2.18.6 Wartung....202
2.18.7 SSL für WBM....204
2.18.8 DLS....204
2.18.9 Ändern von Login und Passwort für WBM/CLI....206
2.19 Command Line Interface CLI beim HG 3575 V4....206
2.20 SNMP Support HG 3500 / HG 3575....206
2.21 IP-Ports....276
2.21.1 Allgemeine Informationen....276
2.21.2 Port-Bereich....277
2.21.2.1 Masterverbindungen IP-Trunking + DMC (IP-Trunking und IPDA)....277
2.21.2.2 Master-Verbindungen IPDA (HG 3575/HG 3500) + DMC (HG 3575)....277
2.21.3 Hinweise für Netzwerkadministratoren....278
2.21.4 Beispiele....278
2.21.4.1 Payload....278
2.21.4.2 Signalisierung....278
2.21.4.3 SNMP....280
2.21.4.4 Diagnose....281
2.22 WBMs der Baugruppen....281
2.23 Diagnosemöglichkeiten HG 3500 / HG 3575....281
2.24 Gateways HG 3500 und HG 3575 - Ändern von Gateway UI MODUS....282
2.25 FAQ - Häufig gestellte Fragen....284

3 OpenScape 4000 SoftGate....289
3.1 Überblick....289
3.1.1 Funktionsüberblick....289
3.1.2 Varianten....289
3.1.3 Leistungsmerkmale....290
3.1.4 LAN Interfaces....292

3.1.5 Ports ... 293
3.1.6 Vorteile ... 293
3.1.7 Einschränkungen ... 294
3.1.8 Diagnosehinweise bezüglich peripherer Einbauteilungen ... 295
3.1.9 Hardware-Voraussetzungen ... 295
3.2 OpenScape 4000 SoftGate Upgrade ... 295
3.2.1 Upgrade über Loadware Update Manager ... 296
3.2.2 Upgrade über lokales WBM des OpenScape 4000 SoftGate ... 297
3.3 Mediatrix Gateways ... 299
3.3.1 Freigegebene Mediatrix Gateways ... 299
3.3.2 Hinweise zur Konfiguration ... 300
3.3.3 Konfigurationsbeispiele ... 300
3.3.3.1 ISDN (S0) Teilnehmer (Mediatrix 44xx) ... 300
3.3.3.2 S0-Trunking (Mediatrix 44xx) ... 307
3.3.3.3 ISDN (S0) Daten-Verbindungen (Mediatrix 44xx) ... 316
3.3.3.4 S2-Schnittstelle (Mediatrix 36xx) ... 323
3.3.3.5 Analoge Teilnehmer (Mediatrix 41xx) ... 332
3.3.3.6 Analog Trunking (Mediatrix 1204) ... 339
3.3.4 Fehlersuche mit syslog für Mediatrix 44xx und 36xx ... 351
3.4 Videoverbindungen ... 354
3.4.1 Einschränkungen ... 354
3.4.2 Szenarien ... 355
3.4.3 Merkmale ... 355
3.4.4 Konfiguration ... 355
3.5 Music on Hold - OpenScape 4000 SoftGate zur Bereitstellung von Wartemusik oder Ansagen ... 355
3.5.1 Leistungsmerkmalbeschreibung ... 356
3.5.2 Serviceinformationen ... 356
3.5.3 Generierung (Beispiel) ... 358
3.5.4 Relevante AMOs ... 360
3.6 Gatekeeper-Redundanz für HFA/SIP-Teilnehmer ... 360
3.6.1 Leistungsmerkmalbeschreibung ... 361
3.6.1.1 Lösungskonzept ... 361
3.6.1.2 Umschaltung ... 361
3.6.1.3 Voraussetzungen für eine Umschaltung ... 362
3.6.1.4 Umschalt-Vorgang ... 362
3.6.1.5 Gatekeeperredundanz mit APE ... 368
3.6.2 Service-Informationen ... 368
3.6.3 Generierung (Beispiel) ... 370
3.6.4 Relevante AMOs ... 377
3.7 Survivable OpenScape 4000 SoftGate ... 378
3.7.1 Leistungsmerkmalbeschreibung ... 378
3.7.2 Serviceinformationen ... 380
3.7.3 Generierung (Beispiel) ... 380
3.8 IPv6 ... 380
3.8.1 Leistungsmerkmalbeschreibung ... 381
3.8.2 Service-Informationen ... 381
3.8.3 Generierung (Beispiel) ... 381
3.8.3.1 Wichtiger Hinweis ... 381
3.8.3.2 IPv6-Netzwerkanbindung für OpenScape 4000 SoftGate und STMIX/STMIY (Trunking) ... 382
3.8.3.3 Interne IPv6-Konnektivität ... 385
3.8.3.4 Sicherung und Wiederherstellung des NGS ... 387
3.8.4 Relevante AMOs ... 389
3.9 Load Balancing ... 390
3.9.1 Leistungsmerkmalbeschreibung ... 390
3.9.2 Serviceinformationen ... 390
3.9.3 Generierung (Beispiel) ... 391

3.9.3.1 SIP Load Balancer Einstellungen....391
3.9.3.2 Ausgehende/eingehende Rufe über SIP Load Balancing Server....392
3.9.3.3 Registrierung von Gateways....394
3.9.3.4 Registrierung einer UC Media Server Farm....395
3.10 Secure Remote Subscriber....397
3.10.1 Leistungsmerkmalbeschreibung....397
3.10.1.1 Serverseitige SoftGate Destination NAT (DNAT)-Option....398
3.10.2 Serviceinformationen....399
3.10.2.1 Voraussetzungen....399
3.10.2.2 Allgemein....400
3.10.2.3 Beschränkungen....402
3.10.2.4 DMZ....402
3.10.2.5 Software-Lifecycle der IP-Endgeräte via DLS und HTTPS....406
3.10.3 Generierung (Beispiel)....410
3.10.3.1 Deployment Service (DLS) und DLS Contact-Me Proxy (DCMP) - Tipps & Tricks....416
3.11 Picture CLIP....421
3.11.1 Leistungsmerkmalbeschreibung....422
3.11.2 Serviceinformationen....423
3.11.3 Generierung (Beispiel)....423
3.11.3.1 Konfiguration des OpenScape 4000 SoftGate....423
3.11.3.2 Telefonkonfiguration....425
3.11.3.3 LDAP-Verzeichnisserver-Konfiguration....428
3.11.3.4 LDAP-Zugang testen....430
3.12 MFC-R2....432
3.12.1 Leistungsmermalbeschreibung....432
3.12.2 Serviceinformation....432
3.12.3 Generierung (Beispiel)....432
3.13 OpenScape Cordless E-Integration....434
3.13.1 Leistungsmerkmalbeschreibung....434
3.13.2 Serviceinformationen....436
3.13.3 Generierung (Beispiel)....437
3.14 WBMs der Baugruppen....438
3.15 Zentralisierte IP für HFA....438
3.15.1 WBM-GUI-Verbesserungen....440

4 LAN-Konnektivität (LAN-Trennung / LAN-Redundanz)....443
4.1 Separate LAN-Konnektivität für Administration und VoIP....443
4.1.1 Leistungsmerkmalbeschreibung....443
4.1.2 Dienstinformationen....443
4.1.3 Generierung (Beispiel)....444
4.1.3.1 Konfiguration für Common Gateway (HG 3500/ HG 3575), STMIX und STMIY....444
4.1.3.2 Konfiguration für OpenScape 4000 SoftGate oder Enterprise Gateway....445
4.1.4 Relevante AMOs....446
4.2 Separate LAN-Schnittstellen für HFA und SIP....447
4.2.1 Leistungsmerkmalbeschreibung....447
4.2.2 Generierung (Beispiel)....448
4.3 LAN-Redundanz....449
4.3.1 Leistungsmerkmalbeschreibung....449
4.3.2 Redundante LAN-Schnittstellen (Bonding)....449
4.3.2.1 Leistungsmerkmalbeschreibung....449
4.3.2.2 Generierung (Beispiel)....450

5 OpenScape Access und OpenScape Branch....452

6 OpenScape Enterprise Gateway....453

7 Large Enterprise Gatekeeper (LEGK)....454

7.1 Allgemeine Informationen....454
7.1.1 Übersicht....454
7.1.2 Gatekeeper Funktionalität....454
7.1.2.1 Allgemeines....454
7.1.2.2 Schlüsselbegriffe....455
7.1.3 Gatekeeper Einschränkungen....455
7.2 Leitfaden für eine Installation eines IP-Features....455
7.3 Einrichtung des Leistungsmerkmals....456
7.3.1 Wichtige Hinweise....456
7.3.2 Betriebstechnische Generierungsreihenfolge....457
7.3.3 Aktivieren des Large Enterprise Gatekeeper....457
7.3.4 Einrichten der Flexama Speicher in der Datenbasis....459
7.3.4.1 Anzahl der internen und externen Gateways....459
7.3.4.2 Anzahl der internen HG 3500 Gateways eines Systems....460
7.3.4.3 Anzahl der LCR-Waehlmuster für Wählmuster-Pool 1 bis 8....460
7.3.4.4 Anzahl der Cache-Elemente für Cache Pool 1 bis 8....461
7.3.5 Einrichten einer HG 3500 am LAN Segment....462
7.3.5.1 Einrichten des HG 3500 Gateways....463
7.3.6 Einrichten der HG 3500 Rufnummer....480
7.3.7 Einrichten des IP-Trunking im LCR....482
7.3.8 Einrichten von Sätzen und Endgeräten....486
7.3.8.1 Einrichten von Sätzen....487
7.3.8.2 Einrichten von Endgeräten....487
7.3.9 Ändern der Systembandbreiten....487

8 HiPath Feature Access (HFA)....490
8.1 Überblick....490
8.2 Anwendungsbeispiel....491
8.2.1 Leistungsmerkmalbeschreibung....491
8.2.1.1 Technischer Hintergrund....492
8.2.1.2 HFA Teilnehmerregistrierung....492
8.2.2 Benutzeroberfläche....494
8.2.3 Einschränkungen....495
8.2.4 Generierung....495
8.2.4.1 Konfiguration der HG 3500-Baugruppe....495
8.2.4.2 Einrichten der HFA-Teilnehmer....496
8.2.5 Generierung über OpenScape 4000 Assistant....496
8.2.5.1 Einrichtung der HG 3500 über den OpenScape 4000 Assistant....496
8.2.5.2 Einrichten eines HFA-Teilnehmers über den OpenScape 4000 Assistant....500
8.2.6 Löschen....501
8.2.7 Tuning der Sprachqualität....501
8.2.8 Einschalten der Sprachkomprimierung....503
8.2.9 Relevante AMOs....503
8.3 FAQs (häufig gestellte Fragen)....510

9 Mobile HFA Logon....513
9.1 Leistungsmerkmalbeschreibung....513
9.1.1 Mobility-Sitzung....513
9.1.2 Shared Desk Area - gemeinsamer Arbeitsbereich....515
9.2 Benutzeroberfläche....517
9.2.1 Aktivierung/Deaktivierung per KZP....517
9.2.1.1 HFA-Logon....518
9.2.1.2 HFA-Logoff....518
9.2.2 Aktivierung über Menü....518
9.2.3 Aktivierung mit AMO ACTDA....519
9.3 Voraussetzungen....519

9.4 Service Informationen....520
9.4.1 Mobile HFA in Verbindung mit anderen Leistungsmerkmalen....520
9.4.1.1 OpenStage-Endgerät in Verbindung mit einem optiClient....520
9.4.1.2 Leistungsmerkmal „Fangen“ an der „besuchten“ Anlage....521
9.4.1.3 Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))....521
9.4.2 Einschränkung....521
9.4.3 Sprachunterstützung....521
9.4.4 Funktionsabläufe bei Logon....522
9.5 Generierung....522
9.5.1 Beispiel 1: Zwei HFA-Teilnehmer auf demselben Host....523
9.5.2 Beispiel 2: Zwei HFA-Teilnehmer an verschiedenen Anlagen....523
9.5.3 Relevante AMOs....525

10 IP Distributed Architecture (IPDA)....534
10.1 Leistungsmerkmalbeschreibung IPDA....534
10.1.1 Skalierbare Erhöhung der Anlagenkapazität....536
10.1.2 Verteilte Durchschaltung....536
10.1.3 Zeitsynchronisation....536
10.1.4 Rufszenarien....537
10.1.4.1 Access Point interner Ruf....537
10.1.4.2 Ruf zwischen 2 Access Points....538
10.1.4.3 Ruf zwischen Access Point und Zentralsystem....539
10.1.4.4 Amtszugang / Vernetzung....540
10.1.5 Survivability für Signalisierung und Payload....540
10.1.5.1 Signaling Survivability....541
10.1.5.2 Payload Survivability....541
10.1.6 Signaling und Payload Separation (SPS)....542
10.1.6.1 Leistungsmerkmalbeschreibung....542
10.1.6.2 Voraussetzungen....542
10.1.6.3 Konfiguration....543
10.1.7 Redundante LAN-Schnittstelle....543
10.1.8 LAN-Überwachung....543
10.1.8.1 Leistungsmerkmalbeschreibung....543
10.1.8.2 Service Information....544
10.1.8.3 Generierung (Beispiel)....545
10.1.8.4 Relevante AMOs....545
10.1.9 Verschiedene Zeitzonen - Different Time Zones (DTZ)....546
10.1.10 A-Law/µ-Law Konvertierung im AP-Shelf....546
10.1.11 Ansagen, Töne und MFV-Wähltonempfänger pro Access Point....546
10.1.12 Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point....546
10.1.13 Weitere Eigenschaften....546
10.2 Einrichtung des Leistungsmerkmals IPDA....547
10.2.1 OpenScape 4000 LAN Segment....548
10.2.2 Access Point....569
10.2.2.1 Einrichten eines „networked“ Access Points....571
10.2.2.2 Einrichten eines „direct link“ Access Points....581
10.2.2.3 Ändern der mit AMO STMIB einstellbaren Parameter eines Access Points....592
10.2.2.4 Löschen eines Access Point....592
10.2.2.5 Lokale Konfiguration eines Access Point....595
10.2.2.6 Referenztakt im Access Point....598
10.2.2.7 Laden neuer Loadware auf eine HG 3575....598
10.2.2.8 Update der Loadware in einem Access Point bei RMX-Hochrüstung (Gilt für neues Fix Release/ Minor Release)....600
10.2.2.9 Hinweise zum Austauschen von HG 3575 Baugruppen....601
10.2.2.10 Hinweise zum 19" Access Point AP 3500 IP....602
10.2.2.11 Hinweise zum 19" Access Point AP 3700 IP....603

10.2.3 HG 3500 als HG 3570 im OpenScape 4000 System....604
10.2.4 Teilnehmersätze in Access Points....610
10.2.5 Sonderrouten....618
10.2.5.1 Sonderrouten zwischen Access Points....619
10.2.5.2 Sonderrouten zwischen Access Point und OpenScape 4000 LAN Segment....622
10.2.6 Signaling Survivability....630
10.2.7 Qualitätsüberwachung für die Signalisierungsverbindung über IP....631
10.2.7.1 Begrenzung der nutzbaren Signalisierungsbandbreite (Traffic Shaping)....631
10.2.7.2 Überwachung der Umlaufzeit von Signalisierungsmeldungen (Round Trip Delay)....633
10.2.7.3 Überwachung des Meldungsdurchsatzes....635
10.2.7.4 Erweiterte Kriterien für Signaling Survivability....636
10.2.7.5 Ausgabe von statistischen Informationen zur Signalisierungsverbindung....637
10.2.7.6 Fehlermeldungen aus der Qualitätsüberwachung für die Signalisierungsverbindung über IP....638
10.2.8 Source Dependent Routing....640
10.2.9 Payload Survivability....645
10.2.9.1 Wann wird Payload Survivability genutzt?....646
10.2.9.2 Wie wird Payload Survivability eingerichtet?....649
10.2.9.3 Payload Survivability in OpenScape 4000 Netzen....657
10.2.9.4 Einschränkungen....659
10.2.10 Signaling und Payload Separation (SPS)....659
10.2.10.1 Auswirkungen auf Leistungsmerkmale mit SPS....660
10.2.10.2 Auswirkungen auf Leistungsmerkmale mit SPS....662
10.2.10.3 Konfiguration....666
10.2.11 Anrufumlenkung im Survivability-Modus zu einem anderen Access Point....667
10.2.11.1 Voraussetzungen....667
10.2.11.2 Benutzerszenarien....667
10.2.11.3 Anwendungsfälle....669
10.2.11.4 Generierung....674
10.2.12 Externe Music-On-Hold....674
10.2.13 Hinweise zu CMI....678
10.2.14 IP-Adressänderungen....678
10.2.14.1 Adressänderung in einem Netz Segment, in dem Access Points angeschlossen sind....679
10.2.14.2 Änderung der Adresse des Survivability-Netzes....681
10.2.14.3 Änderungen im OpenScape 4000 LAN Segment....682
10.2.15 A-Law/µ-Law Konvertierung im AP-Shelf....687
10.2.15.1 Leistungsmerkmalbeschreibung....687
10.2.15.2 Serviceinformationen....687
10.2.15.3 Generierung (Beispiel)....688
10.2.16 Verschiedene Ansagen, Töne und DTMF DialTone Empfänger pro Access Point....688
10.2.16.1 Leistungsmerkmalbeschreibung....688
10.2.16.2 Serviceinformation....689
10.2.16.3 Generierungsbeispiel....690
10.2.16.4 Relevante AMOs....692
10.2.17 Verschiedene Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point....693
10.2.17.1 Leistungsmerkmalbeschreibung....694
10.2.17.2 Serviceinformation....694
10.2.17.3 Generierung (Beispiel)....696
10.2.17.4 Relevante AMOs....697
10.3 Lastkalkulation....698
10.3.1 Lastkalkulation für Access Points....701
10.3.2 Lastkalkulation für eine HG 3500....708
10.3.3 Berechnungsgrundlagen - Aufbau der Payload Pakete....714
10.3.3.1 MTU-Paket....714
10.3.3.2 Aufbau des Ethernet MAC Frames....716
10.3.3.3 Aufbau des IP Frames....717
10.4 Lokale Administration des Access Points am CLI mittels Terminal....717

10.4.1 Networked Access Point....718
10.4.2 Direct Link Access Point....720
10.4.3 Zuordnung der Parameternamen im LW-CLI zu den AMO-Parametern....722
10.5 Arbeitsblätter - IPDA-Konfiguration....724
10.6 Hinweise für Netzwerkadministratoren....733
10.6.1 Zentralprozessor....733
10.6.2 HG 3500 Voice Gateway....733
10.6.3 Access Points mit HG 3575....735
10.6.4 Redundante LAN-Schnittstelle....737
10.7 IPDA-Assistent....739
10.7.1 Funktionen....739
10.8 FAQ - Häufig gestellte Fragen....741

11 Access Point Emergency (APE)....750
11.1 Leistungsmerkmalbeschreibung Access Point Emergency....750
11.1.1 Einsatz-Szenarien für Access Point Emergency....750
11.1.1.1 LAN-Szenario....750
11.1.1.2 LAN-/WAN-Szenario....751
11.1.1.3 Filialen- (WAN) Szenario....752
11.1.2 Access Point Emergency und Signaling Survivability....753
11.1.3 Survivability Unit im AP 3700 IP....754
11.1.4 Survivability Unit am OpenScape 4000 SoftGate....754
11.1.5 Zuordnung von Access Points/OpenScape 4000 SoftGates zur Survivability Unit....755
11.1.6 Umschaltung in den Emergency-Betrieb....755
11.1.7 Rückschaltung in den Normalbetrieb....756
11.1.8 Konfigurationsdaten....757
11.1.9 Übernahme von Systemausgaben und Patches....758
11.1.10 Verbindung zwischen den Teilsystemen (Inseln)....758
11.1.11 Zeitsynchronisation....759
11.1.12 Lizenzierung der Leistungsmerkmale....759
11.1.13 Unterstützung von Applikationen im Emergency-Betrieb....760
11.2 Einrichtung des Leistungsmerkmals APE (Access Point Emergency)....760
11.2.1 Einrichten oder Ändern eines CC-AP/Survivable OpenScape 4000 SoftGate in der OpenScape 4000....761
11.2.2 Löschen eines CC-AP/Survivable OpenScape 4000 SoftGate in der OpenScape 4000....763
11.2.3 Einrichten/Ändern einer Emergency Gruppe....764
11.2.4 Löschen einer Emergency Gruppe....769
11.2.5 Einrichten von Access Points/OpenScape 4000 SoftGates für AP Emergency....769
11.2.6 Beispiele für die Dimensionierung der Gewichtung....772
11.2.7 Access Points/OpenScape 4000 SoftGates aus AP Emergency Konfiguration entfernen....773
11.2.8 Löschen der gesamten AP Emergency Konfiguration....774
11.2.9 Einrichten der Display-Anzeige für AP Emergency am Endgerät....774
11.2.10 Festlegen der Umschalteverzögerung....775
11.2.11 Abfragen der Verbindungsdaten....777
11.2.11.1 Abfragen der Verbindungsdaten über Configuration Management....777
11.2.11.2 Abfragen der Verbindungsdaten über AMO....777
11.2.12 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates....779
11.2.12.1 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates über Configuration Management....780
11.2.12.2 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates über AMO....780
11.2.13 Zeitsynchronisation zwischen Host System und CC-AP/Survivable OpenScape 4000 SoftGate....783
11.2.14 Erstinbetriebnahme des CC-AP/Survivable OpenScape 4000 SoftGate....783
11.2.14.1 Vorbereitung....783
11.2.14.2 CC-AP....783
11.2.14.3 Survivable OpenScape 4000 SoftGate....784
11.2.15 Verifizieren / Abnahme der AP-Emergency Konfiguration....784

11.3 Backup & Restore....784
11.3.1 Konfiguration von OpenScape 4000 Assistant Backup & Restore im OpenScape 4000 Host System....784
11.3.1.1 Einrichten eines AP Backup-Servers mit OpenScape 4000 Assistant Backup & Restore....785
11.3.1.2 Einrichten eines Zeitplans für den Backup....787
11.3.1.3 Durchführen des ersten Backup....789
11.3.1.4 Handhabung von OpenScape 4000 Assistant Backup & Restore bei größeren Änderungen am System....789
11.3.1.5 Prüfen der regelmäßigen Aktivitäten von OpenScape 4000 Assistant Backup & Restore....790
11.3.2 Konfiguration von OpenScape 4000 Assistant Backup & Restore am CC-AP/Survivable OpenScape 4000 SoftGate....790
11.3.2.1 Einrichten des AP Backup-Servers am CC-AP/Survivable OpenScape 4000 SoftGate....791
11.3.2.2 Einrichten eines regelmäßigen Backup der Konfigurationsdaten auf Harddisk....792
11.4 Service-Szenarien....793
11.4.1 Hochrüstung des AP-Emergency Servers (neues Fix Release/Minor Release)....793
11.4.2 DSCXL2-Austausch im AP-Emergency Server....794
11.5 Arbeitsblätter - APE-Konfiguration....794
11.6 Hinweise für Netzwerkadministratoren....796
11.6.1 Survivability Unit für AP-Emergency....796
11.7 Kurzanleitung zum Einrichten eines AP Emergency (IPDA)....798
11.7.1 Einleitung....798
11.7.2 Voraussetzung....799
11.7.3 Einrichtungsschritte in OpenScape 4000....801
11.7.4 Einrichtungsschritte im CC-AP....806
11.7.5 Verifizieren / Abnahme der AP-Emergency Konfiguration....813
11.8 FAQ - Häufig gestellte Fragen....813

12 Verschiedene Zeitzonen - Different Time Zones (DTZ)....816
12.1 Leistungsmerkmalbeschreibung....816
12.2 Service Information....817
12.3 Generierungsbeispiel....817
12.3.1 Einrichten der Zeitklassen....819
12.3.2 Zuweisen der Zeitklassen zu einem AP-Shelf....822
12.3.3 Zuweisen der Zeitklassen zu einem HFA-Teilnehmer....822
12.3.4 Löschen einer Zeitklasse....823
12.3.5 Löschen der Sommerzeitumschaltung....825
12.3.6 Ändern von System-Zeit/Datum mit AMO DATE....825
12.4 Relevante AMOs....826

13 Signaling Survivability....829
13.1 Leistungsmerkmalbeschreibung....829
13.1.1 Wie wird die Störung erkannt?....830
13.1.2 Was wird als Alternativweg für die Signalisierung verwendet?....832
13.1.2.1 Signaling Survivability über das öffentliche Amt....833
13.1.2.2 Signaling Survivability über alternatives LAN....834
13.1.3 HSR über UDP....835
13.2 Serviceinformationen....836
13.3 Generierung (Beispiel)....838
13.3.1 Signaling Survivability über das öffentliche Amt....838
13.3.1.1 Konfiguration der OpenScape 4000....838
13.3.1.2 Konfiguration des Modems....842
13.3.1.3 Konfiguration des Routers....843
13.3.2 Signaling Survivability über alternatives LAN....852
13.3.2.1 Konfiguration der OpenScape 4000....853
13.3.2.2 Konfiguration der LAN-Schnittstelle....854
13.3.2.3 Konfiguration des Routers....855

13.3.2.4 Austausch einer defekten NCUI-Baugruppe durch eine neue NCUI-Baugruppe..... 855
13.3.3 Ist Signaling Survivability gerade aktiv? (AB-UCSU).....856
13.4 Relevante AMOs..... 862

14 SIP-Konnektivität..... 865
14.1 Übersicht.....865
14.1.1 Schnittstellen..... 865
14.1.1.1 SIP-Teilnehmer.....865
14.1.1.2 UFIP-Geräte.....865
14.1.1.3 SIP-Trunking.....865
14.1.2 Unterstützte RFCs (Anfrage für Kommentare) für SIP-Schnittstellen.....865
14.1.3 Verwendete Baugruppen.....870
14.1.4 Konfigurieren des Gateway-Ports..... 870
14.2 SIP-Teilnehmer..... 871
14.2.1 SIP-Endpunkte.....871
14.2.2 Service-Informationen.....871
14.2.3 Leistungsmerkmale.....873
14.2.4 Einschränkungen.....878
14.2.4.1 Einschränkungen der System-Leistungsmerkmale.....878
14.2.4.2 Einschränkungen der Terminal-Leistungsmerkmale.....878
14.2.4.3 Allgemeine Einschränkungen.....879
14.2.5 Konfiguration.....879
14.2.5.1 STMI2/4- und STMIX-Baugruppenkonfiguration.....880
14.2.5.2 Konfigurieren eines SIP-Teilnehmers..... 880
14.2.5.3 Entfernen eines SIP-Teilnehmers..... 881
14.2.5.4 Ändern eines SIP-Teilnehmers..... 881
14.2.5.5 DMC aktivieren/deaktivieren..... 882
14.2.5.6 SIP Session Timer..... 882
14.2.5.7 Teilnehmer Parameter.....883
14.2.5.8 Briefkastensignalisierung (MWI)..... 884
14.2.5.9 SIP-Teilnehmer als DR-Taste eines Tischtelefons.....885
14.2.5.10 SIP-Peer-Filtering.....885
14.2.5.11 Anrufweiterleitung.....886
14.2.5.12 Anzeige der SIP-Teilnehmer.....887
14.2.5.13 Besetzter Override, Notfall-Einbruch und Notabschaltung für SIP (UFIP)-Abonnenten..... 887
14.2.5.14 UFIP in Pickup Group.....888
14.2.5.15 Relevante AMOs.....890
14.3 SIP-Trunking..... 895
14.3.1 SIP-Q-Trunking.....895
14.3.1.1 Leistungsmerkmale..... 895
14.3.1.2 Einschränkungen.....897
14.3.1.3 Konfiguration..... 898
14.3.2 Native SIP Trunking..... 898
14.3.2.1 Leistungsmerkmale..... 898
14.3.2.2 Einschränkungen.....899
14.3.2.3 Anwendungsfälle..... 900
14.3.2.4 Konfiguration..... 901
14.3.3 SIP-Trunk Profile..... 901
14.3.3.1 Allgemeine Informationen..... 901
14.3.3.2 Standardprofile..... 902
14.3.3.3 Aktivieren der SIP-Trunk Profile..... 903
14.3.3.4 Menü „SIP-Trunk-Profile“..... 904
14.3.3.5 Parameter für den Expertenmodus..... 908
14.3.3.6 Konfiguration von SIP-Trunks mit Registrierung.....917
14.4 Built-in SBC..... 923
14.4.1 Generelle SBC Anforderungen (Quelle Wikipedia).....923

14.4.2 Built-in SBC Funktion....924
14.5 SIP-Carrier / SIP Service Provider konfigurieren....926
14.5.1 Motivation....927
14.5.2 Grundlegendes zur Konfiguration....927
14.5.2.1 Konfiguration....927
14.5.2.2 Hinweise....928
14.5.3 Szenario 1: Gateway direkt an SIP-Carrier....928
14.5.3.1 Ausgangssituation....928
14.5.3.2 AMO-Konfiguration....929
14.5.3.3 Konfiguration im WBM des Gateways....933
14.5.4 Szenario 2: Gateway über Session Border Controller an SIP-Carrier....934
14.5.4.1 Ausgangssituation....935
14.5.4.2 AMO-Konfiguration....936
14.5.4.3 HG 3500-Konfiguration in WBM....936
14.5.4.4 Konfiguration im Session Border Controller....938
14.5.4.5 SG vHG direct connectivity (USEWANIF)....938
14.5.5 SIP Provider: Telekom Deutschland GmbH DeutschlandLAN SIP-Trunk....938
14.5.5.1 Serviceinformationen....939
14.5.5.2 Einschränkungen....940
14.5.5.3 Konfiguration....941
14.5.5.4 Verbindungsbeispiele....945
14.5.5.5 Konfigurationsbeispiel OpenScape SBC....947
14.5.5.6 Konfigurationsbeispiel OpenScape SBC (CompanyFlex)....961
14.5.5.7 Häufig gestellte Fragen – FAQ....964
14.5.6 Nahübersprechen NAT Unterstützung für SG vHG Boards....964
14.5.6.1 AMO-CGWB Konfigurationen....965
14.5.7 SIP Amtsleitungen mit Nahübersprechen Ziel NAT (STMIX)....966
14.5.7.1 Wichtige Informationen....966
14.5.7.2 Konfigurationsmöglichkeiten....967
14.5.8 Notrufe von mehreren Standorten über zentralisierten SIP-Trunk....967
14.5.9 Notrufe....968
14.6 Konfiguration SIP-Q-Trunking / Native SIP Trunking....969
14.6.1 Konfiguration mit Hilfe von AMOs....969
14.6.1.1 Trunking-Protokoll....970
14.6.1.2 Einrichten einer (v)HG 3500 als internes Gateway....970
14.6.1.3 Backup & Restore der WBM-Konfigurationsdaten....977
14.6.1.4 Abfragen des Linkstatus....978
14.6.1.5 Vorgehen bei Erweiterung um weitere HG 3500 Gateways im Netz....978
14.6.1.6 Relevante AMOs....978
14.6.2 Konfiguration mit Hilfe des OpenScape 4000 Assistant....981
14.6.2.1 Gateway HG 3500 konfigurieren....981
14.6.2.2 IPGW löschen....983
14.6.2.3 IPGW-Baugruppendaten ändern....984
14.6.3 Konfiguration mit Hilfe von SIP-Trunk-Profilen im WBM....984
14.6.4 SIP-Q-Trunking zwischen OpenScape 4000 und OpenScape Voice....985
14.6.4.1 Einschränkungen....985
14.6.4.2 Konfiguration OpenScape 4000....985
14.6.4.3 Konfiguration OpenScape Voice....989
14.6.5 Nummernmanagement zwischen OpenScape 4000 und OpenScape Voice für Italien....991
14.7 Konfigurationsanleitung für OpenScape 4000/OpenScape Voice Networking....992
14.7.1 Allgemein....992
14.7.2 Einleitung und Übersicht....993
14.7.3 Anforderungen und freigegebene Kombinationen....993
14.7.4 Konfiguration auf OpenScape 4000....993
14.7.4.1 Einstellungen für STMI2/STMI4....994
14.7.5 Konfiguration für OpenScape Voice....1011

14.7.5.1 OpenScape Voice Endpoint Profile..... 1012
14.7.5.2 OpenScape Voice Endpoint..... 1013
14.7.5.3 IP-Adresse für OpenScape 4000 im Fall der Digest-Authentifizierung als vertrauenswürdig einstufen..... 1017
14.7.6 DNS-SRV für HG 3500..... 1018
14.7.6.1 Beispiel einer Web-Schnittstelle für Geo-Separated OpenScape Voice mit TLS-Konfiguration. 1019
14.7.6.2 Beispiel für Branch mit Geo-Separated OpenScape Voice und TLS..... 1020
14.7.7 Signaling and Payload Encryption (SPE)..... 1021
14.7.8 Richtung von OpenScape Voice zu OpenScape 4000..... 1031
14.7.9 OpenScape Voice-Richtung für die internationale Wahl – Rufnummern auf internationale Nummer erweitern..... 1034
14.7.9.1 Für 5- oder 6-stellige Nebenstellenwahl..... 1034
14.7.9.2 Wählen mit Ortsvorwahl..... 1035
14.7.9.3 Wählen mit Ortsvorwahl (geschlossene Nummerierung)..... 1036
14.7.9.4 Wählen mit Landesvorwahl..... 1037
14.7.9.5 Wählen mit Landesvorwahl (geschlossene Nummerierung)..... 1038
14.7.9.6 Wählen mit Landesvorwahl..... 1039
14.7.9.7 Wählen mit Landesvorwahl (geschlossene Nummerierung)..... 1040
14.7.9.8 Nummerntyp auf „International“ ändern..... 1041
14.7.9.9 Internationale Nummer für „HOME DN“ anpassen..... 1042
14.7.9.10 Konfiguration der Standartrichtung, wenn die Nummer in „HOME DN“ nicht übereinstimmt... 1043
14.7.9.11 Komplette internationale Nummernwahl für einzelne externe Zielnummer..... 1044
14.7.10 Schleifenerkennung für OpenScape Voice..... 1045
14.7.11 Einschränkungen..... 1045
14.8 Interworking mit Microsoft Lync Communication Server 2010/2013..... 1046
14.8.1 Wichtige Hinweise..... 1046
14.8.2 Leistungsmerkmalbeschreibung..... 1046
14.8.3 Realisierung..... 1047
14.8.4 Serviceinformationen..... 1047
14.8.4.1 Einschränkungen..... 1047
14.8.4.2 Verfügbare Leistungsmerkmale..... 1048
14.8.5 Konfigurationsbeispiel..... 1051
14.8.5.1 OpenScape 4000..... 1051
14.8.5.2 Microsoft Lync Server/Mediation Server..... 1053
14.9 Skype for Business..... 1059
14.9.1 Funktionsüberblick..... 1059
14.9.1.1 Verfügbare Funktionen (Überblick):..... 1060
14.9.1.2 Funktionsbeschreibung im Detail..... 1060
14.9.2 Einschränkungen..... 1063
14.9.3 Spezifische Konfiguration..... 1064
14.9.3.1 OpenScape-4000-Routing..... 1064
14.9.3.2 Konfiguration von vHG 3500 WBM..... 1064
14.9.3.3 Konfiguration von Skype for Business Server 2015..... 1066
14.9.3.4 Hinzufügen von OpenScape 4000 vSTMI als Gateway zur Topologie von Skype for Business Server 2015..... 1066
14.9.3.5 Definition eines Wählplans..... 1070
14.9.3.6 Erstellung einer VoIP-Richtlinie..... 1071
14.9.3.7 Definition einer Trunk-Konfiguration..... 1073
14.10 MS Teams DR mit Audiocodes SBC..... 1074
14.10.1 Funktionsüberblick..... 1074
14.10.2 Einschränkungen und Hinweise..... 1074
14.10.3 Konfiguration..... 1075
14.11 MS Teams Direct Routing mit OpenScape SBC..... 1075
14.11.1 Netzwerktopologie..... 1075
14.11.2 Konfiguration OpenScape 4000..... 1076
14.11.2.1 AMO-Konfiguration..... 1076

14.11.2.2 STMIX/STMIY vHG WBM-Konfiguration....1076
14.11.3 OpenScape SBC-Konfiguration....1078
14.11.3.1 Kernbereichsschnittstelle....1078
14.11.3.2 SIP Server....1079
14.11.3.3 Zertifikate....1082
14.11.3.4 Teams Medienprofil....1084
14.11.3.5 OpenScape 4000-Medienprofil....1085
14.11.3.6 Allgemeine Medieneinstellungen....1086
14.11.3.7 Externe Endpunkte....1087
14.11.4 MS Teams Direct Routing-Konfiguration....1093
14.11.5 Verfügbare Funktionen (Überblick)....1094
14.11.6 Allgemeine Einschränkungen und Begrenzungen....1094
14.12 SIP-URI-Wahl....1094
14.12.1 Video-Auswahl....1095
14.12.1.1 Anrufweiterleitung von externen alphanumerischen SIP URIs....1096
14.12.1.2 SIP-URI-Wahl über die CSTA-Schnittstelle....1096
14.12.1.3 SIP-Q-Support....1096
14.12.2 Video-Einwahl....1097
14.12.2.1 Anrufverarbeitung - Einladungen von OS-SBC (Internet)....1098
14.12.2.2 URI-Mapping-Dienst....1098
14.12.3 SIP-URI-Format für ausgehende Videowahl....1098
14.12.4 MS Teams DR mit Audiocodes SBC....1098
14.12.5 Einschränkungen....1098
14.12.6 Konfiguration....1098

15 OpenScape Mobile Pro Client....1101
15.1 Überblick....1101
15.1.1 Allgemeine Einschränkungen und Begrenzungen....1103
15.1.1.1 Einschränkungen des kombinierten OSMO Pro-Modus....1104
15.1.1.2 Hinweise für SIP-Gerät als OpenScape Mobile Client Deskphone....1104
15.1.2 Konfiguration....1105
15.1.3 Konfigurationsbeispiel....1107
15.1.3.1 Konfiguration aufseiten von OpenScape 4000....1107
15.1.3.2 CICA-Konnektivität zu OS4K....1111
15.1.3.3 Konfiguration von OpenScape Mobile Client....1111
15.1.3.4 OpenScape SBC-Konfigurationsbeispiel....1112
15.1.3.5 Facade and UC configuration....1124

16 Unify Phone Konnektivität....1125
16.1 Überblick....1125
16.1.1 Leistungsmerkmale....1125
16.1.2 Architektur....1126
16.2 Interaktion mit Merkmalen und Einschränkungen....1126
16.3 Konfiguration....1128
16.3.1 Connector-Konfiguration....1128
16.3.1.1 **Konfigurieren des Unify Phone Telephony Connectors**....1128
16.3.1.2 OpenScape 4000 konfigurieren....1128
16.3.1.3 OpenScape SBC konfigurieren....1132
16.3.2 Benutzerkonfiguration....1135
16.3.2.1 Unify Video konfigurieren....1135
16.3.2.2 OpenScape 4000 konfigurieren....1136
16.4 Massenmigration aus dem Kreislauf....1139

17 H323-/H323-Annex-Konnektivität....1141
17.1 Überblick....1141
17.2 MVF-Außerband-Signalisierung....1141
17.3 Konfigurationsbeispiel....1142

17.3.1 Konfiguration mit Hilfe von AMOs....1142
17.3.1.1 Trunking-Protokoll....1142
17.3.1.2 Einrichten einer (v)HG 3500 als internes Gateway....1142
17.3.1.3 Backup & Restore der WBM-Konfigurationsdaten....1149
17.3.1.4 Abfragen des Linkstatus....1150
17.3.1.5 Vorgehen bei Erweiterung um weitere HG 3500 Gateways im Netz....1150
17.3.1.6 Relevante AMOs....1150
17.3.2 Konfiguration mit Hilfe des OpenScape 4000 Assistant....1151
17.3.2.1 Gateway HG 3500 konfigurieren....1151
17.3.2.2 IPGW löschen....1153
17.3.2.3 IPGW-Baugruppendaten ändern....1154

18 Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))....1155
18.1 Leistungsmerkmalbeschreibung....1155
18.1.1 Verschlüsselte Signalisierungs- und Payload-Verbindungen....1155
18.1.2 Szenarien - Überblick....1156
18.1.3 Lösungskonzepte....1156
18.1.3.1 PKI (Public Key Infrastructure)....1156
18.1.3.2 Signalisierungsverschlüsselung....1158
18.1.3.3 TLS Version....1158
18.1.3.4 Zertifikatsprüfungsstufe....1159
18.1.3.5 Minimale Länge der RSA-Schlüssel....1161
18.1.3.6 ECDSA-Zertifikate....1162
18.1.3.7 Maximales Intervall für Schlüssel-Neuaushandlung....1162
18.1.3.8 Sichere Neuaushandlung erzwingen (RFC 5746)....1162
18.1.3.9 Sprachverschlüsselung....1163
18.1.4 MIKEY (Multimedia Internet KEYing)....1164
18.1.4.1 MIKEY Option 0....1164
18.1.4.2 MIKEY Option 1....1165
18.1.5 Session Description (SDES)-Protocol....1165
18.1.6 Master Encryption Key (MEK)....1165
18.1.7 Sichere SIP-Verbindungen....1165
18.1.7.1 SIP-Q-Trunking....1166
18.1.7.2 Native SIP-Trunking....1167
18.1.7.3 SIP-Teilnehmer....1167
18.2 Service-Informationen....1168
18.2.1 Einschränkungen....1168
18.2.2 Zertifikate generieren....1169
18.2.3 Unterstützte Zertifikate....1169
18.2.4 Zertifikate erneuern....1170
18.2.5 Baugruppentausch....1170
18.2.6 STMI Standby-Baugruppe....1170
18.2.7 Aktivieren/Deaktivieren des Leistungsmerkmals SPE für Funktionsbereiche in der Anlage....1170
18.2.8 Anschließen des Gateways....1171
18.2.9 SPE in Verbindung mit Mobile HFA....1171
18.2.9.1 Terminologie....1171
18.2.9.2 Voraussetzung....1172
18.2.9.3 Szenarien mit homogenem HiPath 4000/OpenScape 4000 Netzwerk bei aktivierter SPE....1172
18.2.9.4 Szenarien in einem Netzwerk mit SPE-aktivierten Knoten und SPE-deaktivierten Knoten....1173
18.2.9.5 Netzweite Nutzung von Mobile HFA....1175
18.3 Konfiguration....1175
18.3.1 Voraussetzungen....1176
18.3.2 Aktivieren/Deaktivieren von SPE bei Gateways mit AMO CGWB....1177
18.3.3 Aktivieren/Deaktivieren von SPE bei Trunks....1178
18.3.3.1 SPE bei analogen / TDM Trunks....1179
18.3.3.2 SPE für IP-Trunking....1179

18.3.3.3 Deaktivierung von SPE für SIP-Q/Native SIP-Trunking....1187
18.3.4 Aktivieren/Deaktivieren von SPE bei Endgeräten....1187
18.3.4.1 SPE bei analogen/TDM-Endpunkten....1187
18.3.4.2 SPE bei IP-Endgeräten....1188
18.3.4.3 Konfiguration....1188
18.3.4.4 Signalisierung auf dem Display....1192
18.3.4.5 Deaktivieren von SPE bei Endgeräten....1194
18.3.5 Aktivieren/Deaktivieren von SPE bei Access Points....1195
18.3.5.1 Neuer Access Point in einem aktiven SPE-System....1197
18.3.5.2 Deaktivieren von SPE bei Access Points mit Soft-Restart....1197
18.3.6 Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate....1198
18.3.6.1 Leistungsmerkmale....1198
18.3.6.2 Einschränkungen....1199
18.3.6.3 Konfiguration....1199
18.4 Generieren von SPE-Zertifikaten mit OpenScape 4000 Assistant....1201
18.4.1 SPE Root-Zertifikat....1201
18.4.1.1 Öffnen des Dialogs „SPE Root Certificate“....1201
18.4.1.2 Neues Stammzertifikat erzeugen....1202
18.4.1.3 Anzeigen/Herunterladen des neuen SPE Root-Zertifikats....1204
18.4.2 SPE-Zertifikat....1204
18.4.2.1 Öffnen des Dialogs „SPE Certificate“....1205
18.4.2.2 Erstellen eines neuen SPE-Zertifikats....1205
18.4.2.3 Anzeigen/Herunterladen des neuen SPE-Zertifikats....1208
18.5 Verteilung von Zertifikaten mit dem WBM des Gateways....1209
18.5.1 SPE CA-Zertifikat für SIP-Trunking importieren....1209
18.5.2 Importieren eines SPE-Zertifikats auf einem Gateway....1210
18.5.3 Importieren eines SPE-Zertifikats auf einem vHG3500 HFA....1210
18.5.4 Zertifikate und Sicherheit an vHFA- und WAN-Schnittstellen....1211
18.6 Deployment Service (DLS)....1211
18.6.1 Verteilung von Zertifikaten an Gateways....1212
18.6.1.1 Erzeugen eines virtuellen IP Device....1212
18.6.1.2 Scannen der IP Devices (IP-Gateways)....1216
18.6.1.3 Verteilung eines SPE-Zertifikats....1220
18.6.1.4 Verteilung eines SPE-Zertifikats....1223
18.6.1.5 Bootstrap-Reset....1227
18.6.2 Verteilung von Zertifikaten an Teilnehmer....1228
18.6.2.1 Verteilen eines CA-Zertifikats....1228
18.6.2.2 Scannen der IP Devices (Endgeräte)....1230
18.7 AutoSPE-Konfiguration....1233
18.7.1 OpenScape 4000....1234
18.7.2 Deployment Service DLS....1234
18.7.2.1 Zeitserver DLS....1234
18.7.2.2 Vorbereitungen DLS....1235
18.7.3 Endgeräte-Konfiguration....1236
18.7.3.1 Vorbereitungen....1236
18.7.3.2 Zeitserver....1237
18.7.4 Automatische Zertifikatserstellung....1237
18.7.5 Sprachverschlüsselung aktivieren....1238
18.7.6 Zertifikate überprüfen....1239
18.7.7 SPE überprüfen....1239
18.7.8 Hinzufügen neuer Gateways nach der AutoSPE-Aktivierung....1239
18.8 MTLS-Implementierung für CGW und SG....1241
18.8.1 SYSTEMEINSTELLUNG....1241
18.8.2 AKTIVIEREN DER ERZWUNGENEN SICHEREN TLS-NEUAUSHANDLUNG (RFC 5746)....1241
18.8.3 GERÄTEEINSTELLUNG....1242
18.8.3.1 OPENSTAGE-TELEFONE....1242

18.8.3.2 OPTIPOINT-TELEFONE....1242
18.8.4 DLS-GERÄTEEINSTELLUNG....1243
18.8.4.1 PROTOKOLLEINSTELLUNG....1243
18.8.4.2 Hochladen des Zertifikats....1244
18.8.4.3 HOCHLADEN DES CA-ZERTIFIKATS....1245
18.8.5 HFA-IMPLEMENTIERUNG....1247
18.8.5.1 CGW....1247
18.8.5.2 SOFTGATE....1251
18.8.6 UFA-IP-Implementierung....1256
18.8.6.1 CGW und SoftGate....1256

19 Payload Switching DMC....1260
19.1 Leistungsmerkmalbeschreibung....1260
19.2 Direct Media Connect (DMC) in Verbindung mit HFA-Teilnehmer....1260
19.2.1 Leistungsmerkmalbeschreibung....1260
19.2.1.1 Hintergrund....1260
19.2.1.2 Hinweise zu Direct Media Connection DMC....1261
19.2.1.3 Überlegungen zur Bandbreite....1262
19.2.1.4 Szenarien....1264
19.2.1.5 Domänenkonzept....1266
19.2.1.6 DMC-Interworking mit HiPath 3000....1267
19.2.2 Service Informationen....1269
19.2.2.1 Leistungsmerkmale mit DMC....1270
19.2.2.2 Aktivierung von Leistungsmerkmalen bei aktiver DMC....1270
19.2.3 Generierung....1271
19.2.3.1 DMC-Berechtigung....1271
19.2.3.2 Maximale Anzahl von DMC-Verbindungen bei IP-Baugruppen....1271
19.2.3.3 Sprachpausenerkennung (Voice Activity Detection, VAD)....1271
19.2.3.4 Domänen....1272
19.2.3.5 H.323 Stack bei IPDA-Baugruppen....1272
19.2.3.6 Tipps zur Fehlerbeseitigung....1273
19.2.4 Relevante AMOs....1274
19.3 Direct Media Connect (DMC) in Verbindung mit SIP-Teilnehmern....1276
19.3.1 Leistungsmerkmalbeschreibung....1276
19.3.2 Einschränkung....1278
19.3.3 Szenarien....1278
19.3.3.1 SIP-Teilnehmer an gleicher OpenScape 4000....1279
19.3.3.2 SIP-Teilnehmer an einer anderen OpenScape 4000....1279
19.3.3.3 SIP-Teilnehmer an einer OpenScape Voice....1280
19.3.3.4 SIP-Teilnehmer an HiPath 3000....1281
19.3.3.5 HFA-Teilnehmer an gleicher OpenScape 4000....1282
19.3.3.6 HFA-Teilnehmer an einer anderen OpenScape 4000....1282
19.3.3.7 HFA-Teilnehmer an HiPath 3000....1284
19.3.3.8 TDM-Teilnehmer/Netzwerk an einem abgesetzten Shelf einer OpenScape 4000....1285
19.3.3.9 TDM-Teilnehmer/Netzwerk an einer anderen OpenScape 4000 hinter einem abgesetzten Shelf....1285
19.3.3.10 TDM-Teilnehmer an einer anderen OpenScape 4000....1286
19.3.3.11 TDM-Teilnehmer an HiPath 3000....1288
19.4 Direct Media Connect (DMC) in Verbindung mit OpenScape 4000 SoftGate....1289

20 T.38 Fax....1298
20.1 Definition....1298
20.2 Leistungsmerkmalbeschreibung....1298
20.2.1 Wichtige Hinweise....1298
20.2.2 Einschränkungen....1299
20.2.2.1 Verzögerungsprobleme im Szenario mit 2 und mehr IP-Hops und bestimmten Faxgeräten....1299

20.2.2.2 DMC-Problem mit AP1120....1299
20.2.2.3 DMC nicht mit MTX41xx eingerichtet....1300
20.2.2.4 Der Parameter „USE Previous Media Negotiation“ muss eingestellt sein....1300
20.2.3 Common Gateway....1301
20.2.4 OpenScape 4000 SoftGate....1301
20.2.5 IPDA....1302
20.3 Szenarien....1302
20.4 Serviceinformationen....1305
20.4.1 OpenScape 4000 SoftGate....1305
20.4.2 IPDA (NCUI/STMI)....1305
20.5 Generierung (Beispiel)....1306
20.6 Relevante AMOs....1307

21 IP-Endgeräte....1309
21.1 Unterstützte IP-Endgeräte....1309
21.2 Baugruppen....1309
21.3 optiPoint-IP-Endgeräte....1309
21.3.1 Allgemeine Informationen....1310
21.3.2 optiPoint 410/420....1310
21.3.2.1 Endgerätetypen....1310
21.3.2.2 Adapter und Zusatzgeräte....1311
21.3.2.3 Module bei optiPoint-Endgeräten....1311
21.3.2.4 Tastenlayout bei optiPoint-Endgeräten....1312
21.3.3 OpenStage WL3/WL4....1312
21.3.4 Weitere Adapter und Anschlüsse....1313
21.3.4.1 OpenStage Belegtlampenfeld....1313
21.3.4.2 optiPoint Recorder Adapter....1314
21.3.4.3 optiPoint Acoustic Adapter....1315
21.3.4.4 Mikrofon und Lautsprecher Anschluss....1315
21.3.4.5 Headset Anschluss....1316
21.3.4.6 Kontakt Anschluss....1317
21.4 OpenStage IP-Endgeräte....1317
21.4.1 Hardware und allgemeine Leistungsmerkmale....1317
21.4.2 Tastenbelegung....1318
21.4.3 Beistellgeräte (Key Module)....1318
21.4.4 OpenStage in Verbindung mit optiClient....1318
21.4.5 Belegtlampenfeld....1319
21.5 OpenScape Desk Phone IP 35G/55G HFA....1320
21.5.1 Hardware und allgemeine Leistungsmerkmale....1320
21.5.2 Tastenbelegung....1320
21.5.3 Beistellgeräte....1320
21.6 OpenScape Desk Phone CP HFA....1321
21.6.1 Hardware und allgemeine Merkmale....1321
21.6.2 Tastenbelegung....1321
21.6.3 Tastenmodule....1321
21.7 Serviceinformation....1322
21.8 Generierung IP-Endgeräte....1322
21.8.1 HFA (IP) Endgerät an STMI....1323
21.8.2 PC hinter HFA (IP) Endgerät....1324
21.8.3 HFA (IP) Endgerät und USB für Simple Dialer....1325
21.8.4 OpenStage WL3/WL4-Konfiguration....1325
21.8.5 OpenStage Konfiguration....1327
21.8.6 OpenScape Desk Phone IP Konfiguration....1330
21.8.7 Desk Phones CP-Konfiguration....1330
21.9 Löschen am IP-Anschluss....1336
21.9.1 Alle Geräte einer Rufnummer am IP-Anschluss löschen....1336

21.9.2 Non-Voice-Dienste am IP-Anschluss löschen....1337
21.9.3 Beistellgerät des IP-Endgerätes löschen....1337
21.9.4 Busy Lamp Field am IP-Endgerät löschen....1337
21.9.5 Adapter des IP-Endgerätes löschen....1337

Index....1342

1 Ziel dieses Dokumentes

Dieses Dokument soll einen Überblick über die Gateways HG 3500 und HG 3575 geben. Es wird nur die Grundkonfiguration der Baugruppen beschrieben. Detaillierte Informationen zu speziellen Funktionen wie IP Distributed Architecture und Access Point Emergency (IPDA & APE), HiPath Feature Acces (HFA), Large Enterprise Gatekeeper usw. finden Sie in den entsprechenden Abschnitten.

2 Gateways HG 3500 und HG 3575

2.1 Begriffe

2.1.1 Schlüsselbegriffe

Um Missverständnisse zu vermeiden, sollen hier einige Schlüsselbegriffe genauer definiert werden, die im weiteren Text häufiger verwendet werden.

<table>
<tr><td>Knoten:</td><td>Bezeichnet ein Gerät mit einem Port/Anschluss in einem Netz.
Das kann ein Router sein, eine CGW-Baugruppe, oder ein beliebiger Computer. Wird häufig auch „Host“ genannt.</td></tr>
<tr><td>LAN Segment:</td><td>Teil eines Netzwerks, in dem alle Knoten auf Schicht 2 (Ethernet MAC) direkt miteinander kommunizieren. Die Knoten sind also am gleichen freigegebenen („shared“) Medium angeschaltet und über Hubs oder Layer-2-Switches miteinander verbunden. D.h. sie kommunizieren ohne Router (Schicht 3). Die Kommunikation zu Knoten außerhalb dieses Segments muss über Router gehen.</td></tr>
<tr><td>IP-Adresse:</td><td>4-stellige Internet-Adresse, z. B. 172.16.222.45. Der Begriff wird hier immer für die individuelle, vollständige und eindeutige Adresse eines Knotens verwendet.</td></tr>
<tr><td>Netzmaske:</td><td>Internet-Adressen teilen sich in einen Netzwerk- und einen Knoten-spezifischen Anteil auf. Die Größe der Anteile ist je nach Klasse der Adresse (bestimmt durch die erste Stelle der Adresse) unterschiedlich.
<table>
<tr><td>Byte</td><td>1</td><td>2</td><td>3</td><td>4</td><td></td></tr>
<tr><td>Klasse</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>A</td><td>Netz [1 .. 126]</td><td>Knoten</td><td>Knoten</td><td>Knoten</td><td></td></tr>
<tr><td>B</td><td>Netz [128 .. 191]</td><td>Netz</td><td>Knoten</td><td>Knoten</td><td></td></tr>
<tr><td>C</td><td>Netz [192 .. 223]</td><td>Netz</td><td>Netz</td><td>Knoten</td><td></td></tr>
</table></td></tr>
</table>

	Durch die Netzmaske können in einem Netz Subnetze erzeugt werden. Zur Adressierung werden bestimmte Bits des Knotenanteils verwendet. Die Netzmaske legt durch die gesetzten Bits fest, welche Stellen der IP-Adresse als Netz-, Subnetz-Anteil zu bewerten sind. Die verbleibenden Stellen (nicht gesetzte Bits in der Maske) kennzeichnen den Knotenanteil.	
Netzadresse:	In diesem Dokument wird der Begriff Netzadresse für den gesamten Netz- **und** Subnetz-Anteil der IP-Adresse verwendet. Eine beliebige IP-Adresse bitweise UND-verknüpft mit der Netzmaske ergibt die Netzadresse.	
VLAN-Tagging	Nach IEEE 802.1 p/q gibt es 2 Funktionen, die über ein gemeinsames Tag gesteuert werden: die **Priorität** und die **VLAN-ID** . Meist wird generell von VLAN-Tagging gesprochen, sobald das Tag genutzt wird - unabhängig davon, wofür es genutzt wird. Auch bei IPDA wird so verfahren. Wenn es darum geht, VLAN-Tagging aus- oder einzuschalten: (AMOs SIPCO oder CGWB: VLAN) ist das Tag gemeint, nicht die Funktion VLAN. Laut Standard gibt es 3 Typen von Frames:	
	• Untagged	Normale Ethernet-Frames ohne Tag
	• Priority Tagged	Ethernet-Frames mit Tag Die Prioritäts-Bits sind genutzt Die VLAN-ID ist 0.
	• VLAN Tagged	Ethernet-Frames mit Tag Die Prioritäts-Bits sind 0 Die VLAN-ID ist > 0.
	Es gibt Hersteller von IP Equipment, welche die Nutzung der Prioritätsbits nur erlauben, wenn die VLAN-ID >0 gesetzt wird. Die IPDA-Komponenten nutzen bei Einsatz des Tagging immer Priority-Tagging, erlauben es aber, eine VLAN-ID > 0 einzustellen Die Prioritätsbits werden abhängig von der Verkehrsart fest eingestellt. Die Werte sind in Tabelle 3 „TOS-Werte“ angegeben.	
TOS-Byte	Das **T**ype **O**f **S**ervice Byte ist Bestandteil des Headers aller IP-Pakete nach RFC 791. Nach RFC 791 (*Internet Protocol*) teilt sich das Byte folgendermaßen auf (höchstwertiges -> niederwertigstes Bit)	

	3 Bit für Precedence 111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 - Priority 000 - Routine	3 Bit für Priorität D-T-R **Slight delay**: 0 = Normal, 1 = Low **Throughput**: 0 = Normal, 1 = High **Reliability**: 0 = Normal, 1 = High	2 Bit reserviert für zukünftige Nutzung
	Nach RFC 2474 (*Differentiated Services*) werden die höherwertigen 6 Bits als DiffServ Code Point (DSCP) genutzt, die 2 niederwertigsten Bits sind reserviert.		
	Die einzustellenden Werte werden teilweise als 6-Bit Wert ohne die 2 reservierten Bits, teilweise als 8-Bit Wert (mit den 2 reservierten Bits = 0) angegeben. Für IPDA wird immer das gesamte TOS-Byte angegeben. Die zwei niederwertigsten Bits werden immer zu Null gesetzt. Ein reiner DiffServ Code Point muss also um 2 Bit nach links geschoben bzw. mit 4 multipliziert werden, um die TOS-Byte-Einstellung für IPDA zu erhalten.		

Tabelle 1: Beispiel: Klasse B IP-Adresse, Netzmaske und Netzadresse

IP-Adresse			
172	16	222	45
1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 0 1 1 1 1 0	0 0 1 0 1 1 0 1
Netzmaske			
255	255	240	0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0	0 0 0 0 0 0 0 0
Subnetz		1 1 0 1	
Netzadresse			
172	16	208	0
1 0 1 0 1 1 0 0	0 0 0 1 0 0 0 0	1 1 0 1 0 0 0 0	0 0 0 0 0 0 0 0

2.1.2 Fax- bzw. Modem-Übertragung und -Erkennung

Mithilfe des Leistungsmerkmals „FMoIP“ (Fax/Modem over IP) können Fax- und Modemsignale über das IP-Netzwerk übertragen werden.

Mit dem Leistungsmerkmal FMoIP stehen folgende Funktionen zur Verfügung:

- DMC (Direct Media Connection) für Fax-/Modemverbindungen. Hierdurch fällt bei Fax-/Modemverbindungen in einem lokalen HiPath-4000-/OpenScape-4000-Netzwerk maximal ein IP-Hop (zweimalige Umwandlung zwischen IP und TDM) an. DMC wird für HG 3500 / HG 3575 unterstützt. Dies stellt die wichtigste Verbesserung gegenüber der Vorgängerversion dar, wo nach der Tonerkennung eine Umschaltung zum Master Call erfolgte.
- Die DMC-Endpunkte HG 3500 und HG 3575 unterstützen G.711 F/M.
- T.38

Wichtig: Bei Anschaltung eines Faxadapters an eine HG 3500 (SIP-Subscriber) muss DMC für dieses Device abgeschaltet werden (nur so kann eine Übertragung mit T.38 stattfinden). Möchte man DMC für dieses Gerät dennoch anschalten, muss der Codec fix auf G.711 eingestellt werden (Faxübertragung mit G.711, nicht T.38).

Wichtig: T.38 Konfiguration/Nutzung erfordert eine End-to-End-DMC zwischen den OpenScape 4000-Gateways (minimierter IP-Hop) aufgrund von Timing-Anforderungen nach T.38-Standard. Im Falle von mehreren IP-Hops kann die Fax-Übertragung bei manchen Faxgeräten fehlschlagen. Eine entsprechende Liste der Faxgeräte finden Sie in der Release Note.

Wichtig: In früheren Versionen waren nur vier T.38-Verbindungen pro DSP möglich. Von HiPath 4000 V6 R2 wird diese Einschränkung aufgehoben und bis zu 60 T.38 parallele Aufrufe werden unterstützt und sind auf STMI-Baugruppen und 120 auf vSTMI-Baugruppen möglich.

---

1) Mehr Informationen darüber, welche Szenarien genau unterstützt werden, finden Sie im Dokument „T.38 Fax“, Kapitel 2, „Leistungsmerkmalbeschreibung“.

- RFC2833 und RFC2198 werden für HG 3500/75 zur Übermittlung von Fax-/Modemsignalen über IP unterstützt.
- Erweiterte DSP-Tonerkennung (mit Übermittlung von Toninformationen nach RFC2833/RFC2198) für HG 3500/75-Baugruppen. Unterstützte Töne:
- – Verbindungsaufbautöne CNG und CT (beim Anrufer)
  – Meldetöne ANS (CED), /ANS, ANSam, /ANSam (beim Gerufenen)

Einschränkungen

- Lässt sich bei DMC die Anzahl der IP-Hops für eine Verbindung nicht auf eins reduzieren, kann es bei Fax- oder Modemverbindungen aufgrund der resultierenden Verzögerungen zu Abbrüchen kommen, und zwar auch dann, wenn ein für Analogdaten optimierter G.711-Kanal verwendet wird.

- Fax-/Modemverbindung: Es wird nur die Funktion Basic Call unterstützt. Aus einer bestehenden Verbindung heraus aufgerufene Zusatzdienste wie z. B. Rückfrageverbindungen werden nicht unterstützt. Die Unterstützung für die Funktion Basic Call schließt umgeleitete Verbindungen (CFU) ein.
- Aufgrund der vielen unterschiedlichen auf dem Markt verfügbaren Modem- und Faxgerätetypen kann nicht garantiert werden, dass FMoIP in allen Anwendungsfällen absolut zuverlässig funktioniert. Unterschiedliche Funktionsweisen der verschiedenen Modem- und Faxgerätetypen (z. B. Toleranzen) sowie die typischen IP-Charakteristika (Jitter, Verzögerungen usw.) können zu Fehlern bei FMoIP-Verbindungen führen.
- Clear Channel muss mittels AMO deaktiviert werden, da es für Clear Channel keine RFC2833/RFC2198-Tonerkennung gibt. Jeder Fax-/Modem-Anruf sollte als normaler Sprachruf (G.711, G.729, ...) konfiguriert werden.

2.1.3 Codec-Standards

Um ein analoges Sprachsignals über digitale Strecken zu übertragen, muss dieses in ein Digitalsignal umgewandelt werden (und wieder zurück). Zur Realisierung dieser Codecs gibt es unterschiedliche Verfahren, welche unterschiedliche Sprachqualität bieten und unterschiedlich viel Bandbreite benötigen.

Detaillierte Informationen zu den Codec-Classmarks stehen in Tabelle 26 „Classmark-Behandlung für Codec-Typ“ im Dokument „IP Distributed Architecture (IPDA)“ zur Verfügung.

2.1.4 Sprachqualität

Bei der Übertragung von Sprache über IP-Netze kommen 3 zusätzliche Einflüsse auf die subjektiv vom Kunden empfundene Sprachqualität zum Tragen:

- **Verzögerung**
- Entsteht bei der Paketierung der Sprachdaten (siehe Bild 1 „Paketweise Sprachübertragung“) und bei der Übertragung der Pakete. Komprimierende Codecs (z. B. G.729) benötigen Verarbeitungszeit. Um Schwankungen in der Paketlaufzeit auszugleichen (Jitter) wird empfangsseitig ein Puffer eingefügt (Jitter-Buffer). Die Größe des Jitter-Buffers geht ebenfalls in die Gesamtverzögerung ein.
- **Paketverlust**
- Bei der Paketübertragung in IP-Netzen können Pakete manchmal verloren gehen. An Stelle der eigentlich benötigten Paketdaten müssen dann empfangsseitig Fülldaten eingefügt werden.
- **Jitter**
- Schwankung der Paketlaufzeit um einen Mittelwert, siehe Bild 2 „Jitter: Variation der Übertragungsverzögerung“. Der Jitter-Buffer muss diese Schwankungen abfangen. Ist die Abweichung vom Mittelwert so groß, dass sie nicht mehr vom Jitter-Buffer abgefangen werden kann, ist das Paket für

die Nutzung verloren. Das verursacht denselben Effekt wie Paketverlust im Netz.

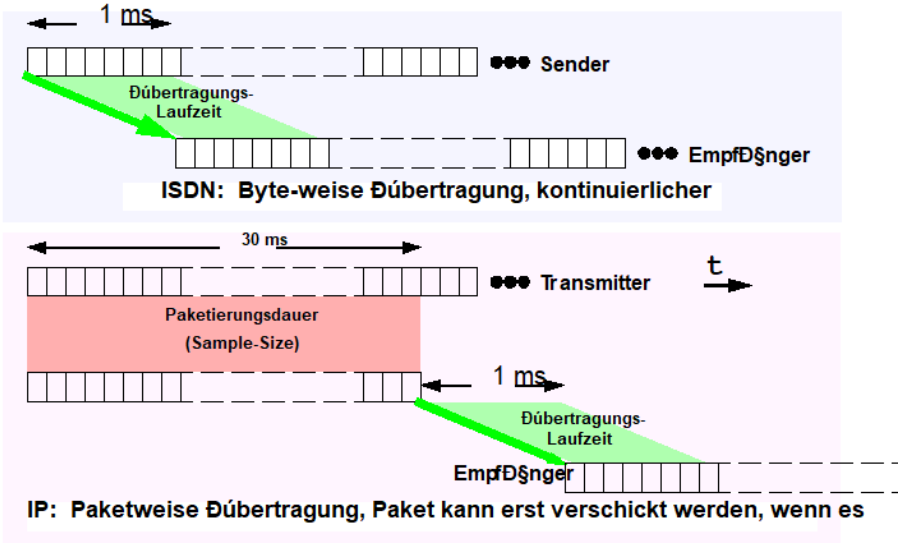


Abbildung 1: Paketweise Sprachübertragung

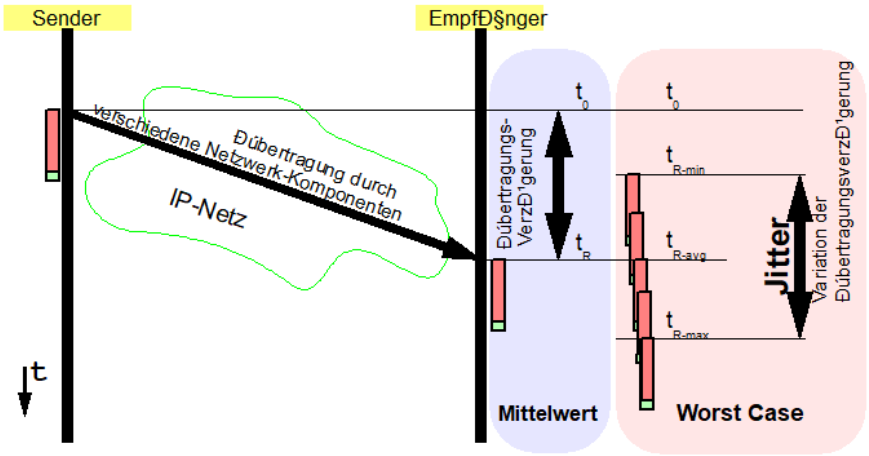


Abbildung 2: Jitter: Variation der Übertragungsverzögerung

Die Auswirkung der beiden Parameter ist zusätzlich von der Sample-Größe (wieviele Millisekunden Sprache pro Paket) und vom Codec-Typ abhängig.

Bild 3 „Sprachqualität in Abhängigkeit vom Delay“ zeigt die Beurteilung der Sprachqualität in Abhängigkeit vom Delay.

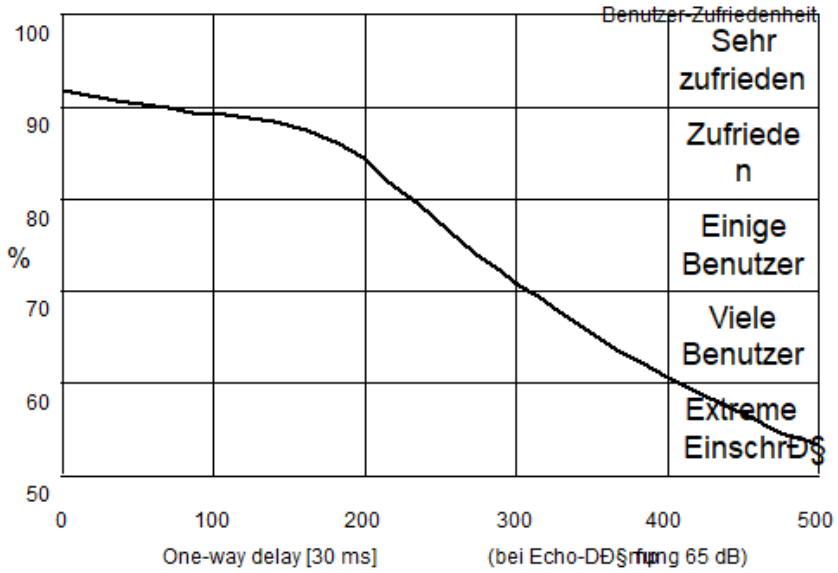


Abbildung 3: Sprachqualität in Abhängigkeit vom Delay

Tabelle 2 „Sprachqualität in Abhängigkeit von Delay und Paketverlustrate“ zeigt die Beurteilung der Sprachqualität in Abhängigkeit von Delay und Paketverlustrate.

Tabelle 2: Sprachqualität in Abhängigkeit von Delay und Paketverlustrate

Skala der Akzeptanz							
Wert	Akzeptanz						
0 - 5	sehr gut						
6 - 10	gut						
11 - 19	hinreichend						
20 und mehr	ungenügend						
Verzögerung [ms]	Paketverlustrate %						
	< 1%	1%	1,5%	2%	2,5%	3%	> 3%
50	0	4	6	8	10	12	30
100	0	4	6	8	10	12	30
150	0	4	6	8	10	12	30
200	3	7	9	11	13	15	33
250	10	14	16	18	20	22	40

300	15	19	21	23	25	27	45
350	20	24	26	28	30	32	50
400	25	29	31	33	35	37	55

Für alle Lösungen über IP, d. h. auch bei OpenScape 4000, sind Konfigurationen mit mehreren IP-TDM (bzw. TDM-IP) Wandlungen in einer Verbindung zu vermeiden, denn jede Wandlung erzeugt eine Verzögerung. Der Grund sind potentielle Einbußen bei der Sprachqualität, wenn es zu großen Verzögerungen kommt. Jede Baugruppe der HG 3500 Familie (auch HG 3575 im Access Pointe) sowie jedes direkt über FA abgesetzte Endgerät beinhaltet dabei eine IST Wandlung. Die maximale Anzahl der IP-TDM Wandlungen sollte (ohne HFA Endgeräte mit einzubeziehen) nicht höher als 2 sein.

2.1.5 Jitter-Buffer

2.1.5.1 Funktionalität des Jitter-Buffers

In TCP/IP-basierten Netzwerken können Pakete einer Übertragung mit unterschiedlicher Verzögerung eintreffen. Da sich dieser Effekt störend auswirkt, muss kontrollierend in den Datenstrom eingegriffen werden. Der Jitter-Buffer ist ein Zwischenspeicher für IP-Pakete. Er kann Verzögerungen von IP-Paketen bis zu einem gewissen Grad ausgleichen.

IP-Pakete gelangen in den Jitter-Buffer in der Reihenfolge ihres Eintreffens. Jedes Paket enthält einen Zeitstempel, der im RTP-Header des Pakets gespeichert ist. Aus den Zeitstempeln der Pakete ergibt sich deren tatsächliche Reihenfolge. Der Jitter-Buffer sorgt dafür, dass die Pakete ihn in der tatsächlichen Reihenfolge und zeitlich synchronisiert wieder verlassen. Eine Durchschnittszeit (Durchschnitts-Delay) definiert, wie lange Pakete, die zum erwarteten Zeitpunkt eintreffen, im Jitter-Buffer bleiben. Pakete, die später eintreffen als erwartet, bleiben entsprechend kürzer im Jitter-Buffer und Pakete, die früher eintreffen als erwartet, entsprechend länger. Wenn ein Paket so spät eintrifft, dass es nicht mehr eingeordnet werden kann, geht es verloren. Theoretisch können Pakete auch so früh eintreffen, dass sie nicht eingeordnet werden können. Dies ist jedoch in der Praxis kaum der Fall.

Bild 4 „Funktionalität des Jitter-Buffers“ verdeutlicht die Funktionalität des Jitter-Buffers.

Bei Sprachübertragungen ist es akzeptabel, wenn einzelne Pakete verloren gehen. Dagegen sollte die Verzögerung möglichst niedrig sein, da zu große Verzögerungen das Telefonieren beeinträchtigen.

Bei Datenübertragungen sollten so wenig Pakete wie möglich verloren gehen, um die Integrität der Daten sicher zu stellen. Dagegen spielen Verzögerungen keine so große Rolle.

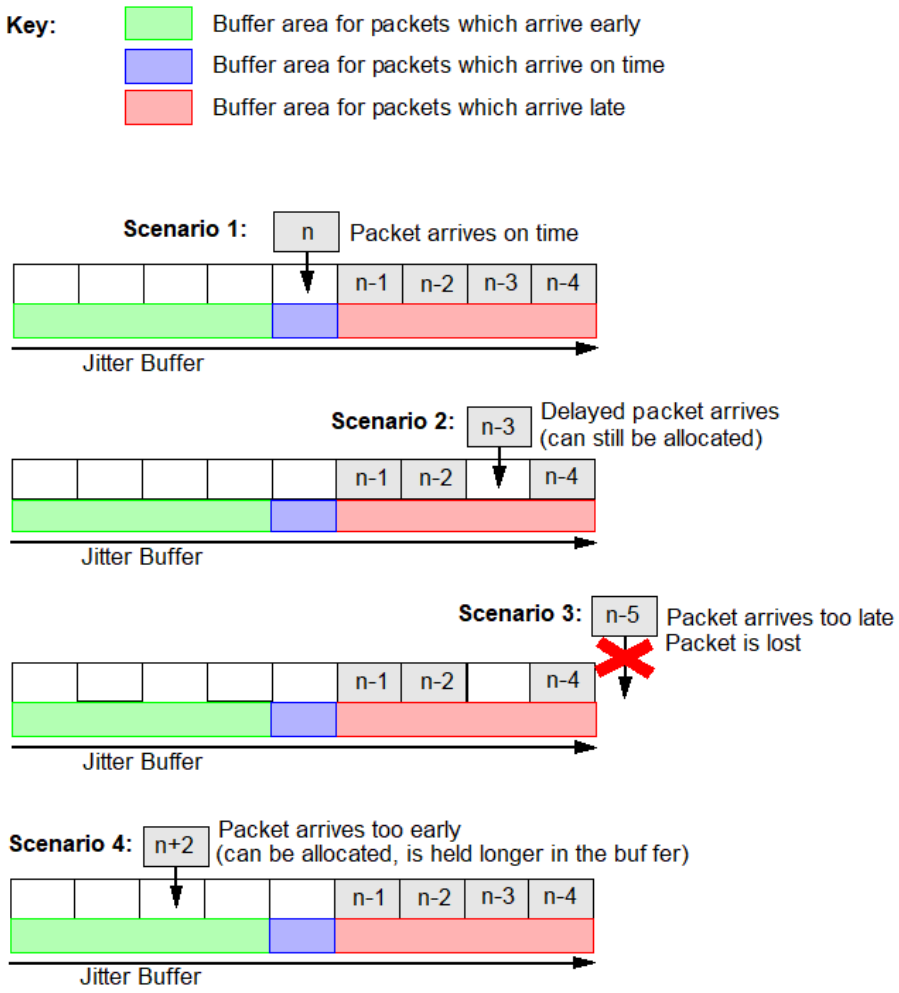


Abbildung 4: Funktionalität des Jitter-Buffers

2.1.5.2 Modes des Jitter-Buffers

Der Jitter-Buffer der Gateways HG 3500/3575 kann verbindungsabhängig in zwei verschiedenen Modi betrieben werden:

- **statischer** Jitter-Buffer
- **adaptiver** (dynamischer) Jitter-Buffer

Der adaptive Jitter-Buffer ist speziell für die Sprachübertragung gedacht. Während beim statischen Jitter-Buffer die Durchschnittsverzögerung für Pakete konstant bleibt, wird diese beim adaptiven Jitter-Buffer je nach Situation automatisch angepasst. Bild 5 „Unterschied zwischen statischem und adaptivem Jitter-Buffer“ verdeutlicht den Unterschied zwischen statischem und adaptivem Jitter-Buffer anhand einer Situation, in der vermehrt Pakete mit erhöhter Verzögerung eintreffen.

Die durchschnittliche Verzögerung ist beim adaptiven Jitter-Buffer lediglich der Startwert für die durchschnittliche Verzögerung. Diese wird während des Betriebs automatisch an die jeweiligen Emfangsverhältnisse angepasst (grüne Linie).

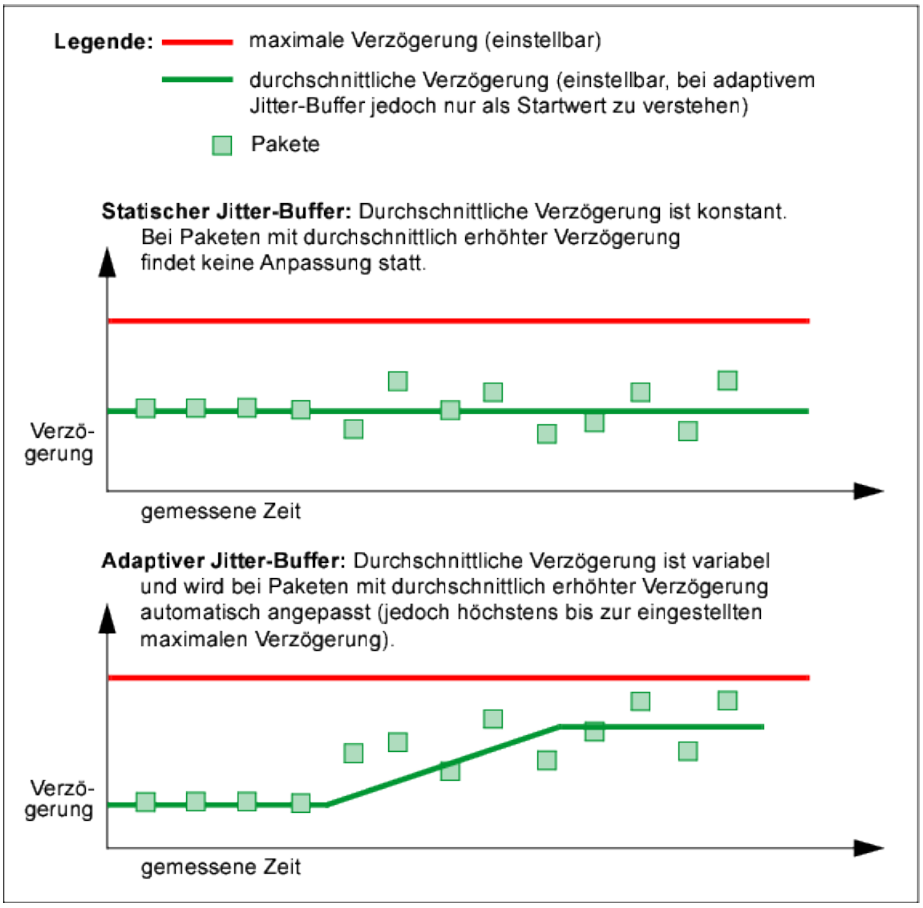


Abbildung 5: Unterschied zwischen statischem und adaptivem Jitter-Buffer

2.1.5.3 Abwägungen beim Einstellen der Verzögerung bei statischem Jitter-Buffer

Je niedriger durchschnittliche und maximale Verzögerung eingestellt werden, desto natürlicher wird von Gesprächsteilnehmern die Übertragung von Sprache empfunden. Dafür steigt die Gefahr des Paketverlusts und damit die Gefahr von Informationsverlusten und Verzerrungen. Bei höheren Werten für die Verzögerung können weniger Pakete verloren gehen, doch dafür dauert es länger, bis ein Teilnehmer das Gesprochene des anderen Teilnehmers hört, was bei zu hoher Verzögerung zu Kommunikationsschwierigkeiten führen kann. Die folgende Illustration verdeutlicht dies:

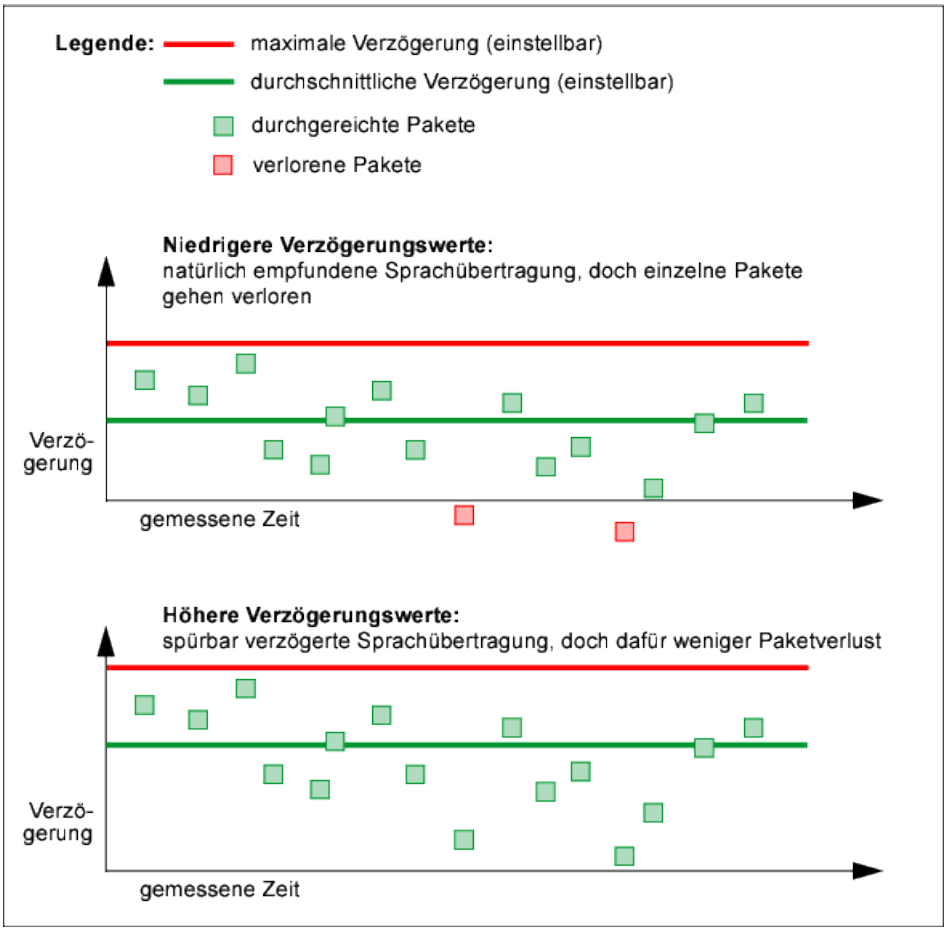


Abbildung 6: Einstellung des statischen Jitter-Buffers

Beim Generieren der HG 3500/75-Baugruppe werden großzügige Werte eingestellt, mit denen die meisten Installationen problemlos in Betrieb gehen. Diese Werte können in vielen Fällen gezielt reduziert werden.

2.1.5.4 Clock Drift bei statischem Jitter-Buffer

Bei der digitale Sprachübertragung im ISDN arbeiten alle Übertragungseinrichtungen synchron. Das heißt, die Menge an Sprachdaten pro Zeiteinheit sind beim Sender und Empfänger absolut gleich. Dazu werden die Übertragungseinrichtungen auf ein gemeinsames Taktnormal (Amtstakt) synchronisiert.

Bei der digitalen Sprachübertragung über IP arbeiten die Übertragungseinrichtungen asynchron. Ausnahme: IPDA Access Points mit digitalem Amtsanschluss können sich auf den Amtstakt synchronisieren. Diese Asynchronität führt dazu, dass auf der Sendeseite immer mehr oder weniger Pakete pro Sekunde erzeugt werden, als auf Empfängerseite erwartet werden. Diese Diskrepanz wird als Clock Drift bezeichnet.

Wenn auf Sendeseite mehr Pakete erzeugt werden, als der Empfänger erwartet, gelangen mehr Pakete in den Jitter-Buffer als vorgesehen. Das führt zu einem ständigen Anstieg der gemessenen durchschnittlichen Verzögerung. Wenn diese den eingestellten Maximalwert für Verzögerung erreicht, reguliert sich der Jitter-Buffer. Er überspringt überzählige Pakete, bis

die gemessene durchschnittliche Verzögerung wieder den eingestellten Wert für durchschnittliche Verzögerung erreicht. Der gesamte Vorgang beginnt von Neuem. Die folgende Abbildung verdeutlicht den Vorgang:

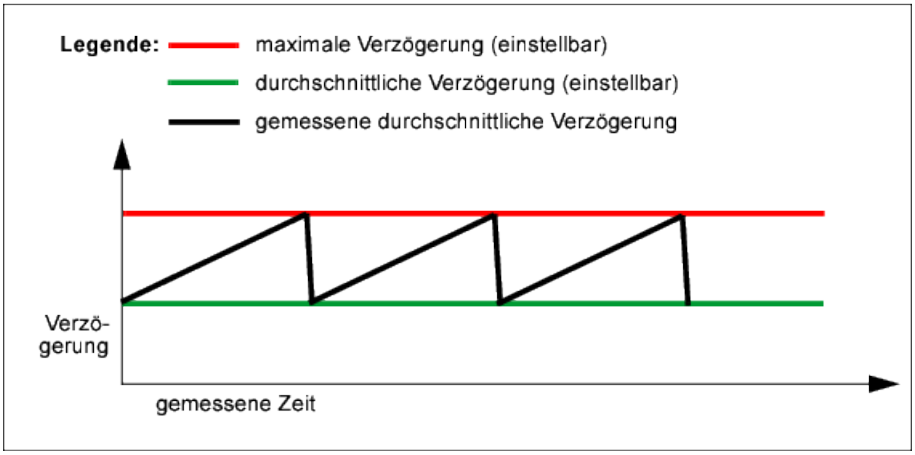


Abbildung 7: Clock Drift bei statischem Jitter-Buffer [Sender schneller als Empfänger]

Ist zum Beispiel die durchschnittliche Verzögerung auf 40 ms eingestellt und die maximale Verzögerung auf 80 ms, so bedeutet das, dass sich die gemessene Gesamtverzögerung periodisch vom Startwert um 40 ms erhöht. Die Periodendauer hängt von der Taktdifferenz der Taktgeneratoren im Zentralsystem (für alle HG 3500) bzw. auf den HG 3575-Baugruppen, sowie von den Konfigurationsdaten ab (Differenz von Maximal und Durchschnittswert). Bei der Beispielkonfiguration (40 ms Delay-Hub) liegt die Periodendauer zwischen etwa 30 und 120 Minuten.

Wenn auf der Sende weniger Pakete erzeugt werden, als der Empfänger erwartet, gelangen weniger Pakete in den Jitter-Buffer als vorgesehen. Das führt zu einer ständigen Verringerung der gemessenen durchschnittlichen Verzögerung. Wenn sich gar keine Pakete mehr im Jitter-Buffer befinden, reguliert sich der Jitter-Buffer und passt die gemessene durchschnittliche Verzögerung wieder an den eingestellten Wert für durchschnittliche Verzögerung an, in dem er Pakete einfügt. Der gesamte Vorgang beginnt von Neuem. Die folgende Abbildung verdeutlicht den Vorgang:

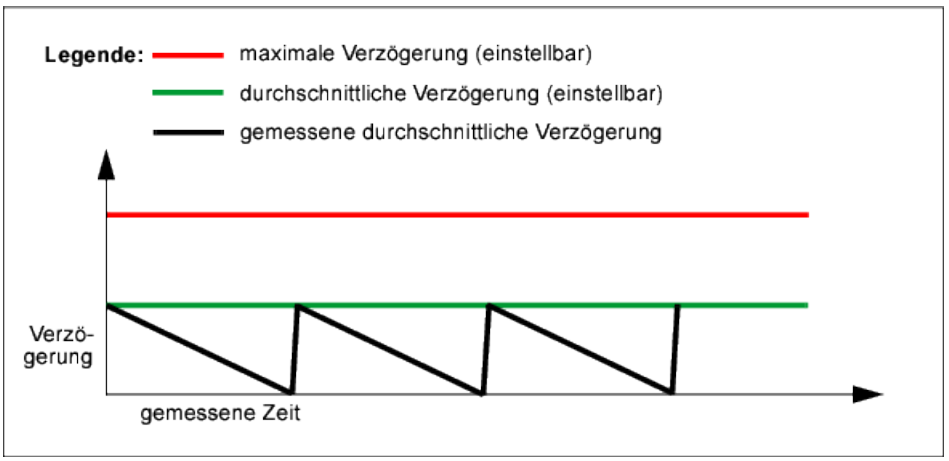


Abbildung 8: Clock Drift bei statischem Jitter-Buffer [Sender langsamer als Empfänger]

Ist die durchschnittliche Verzögerung zum Beispiel auf 40 ms eingestellt, so bedeutet das, dass sich die gemessene Gesamtverzögerung periodisch vom Startwert um 40 ms verringert. Die Periodendauer hängt von der Taktdifferenz der Taktgeneratoren im Zentralsystem (für alle HG 3500) bzw. auf den HG 3575-Baugruppen, sowie von den Konfigurationsdaten ab (Differenz von Maximal und Durchschnittswert). Bei der Beispielkonfiguration (40 ms Delay-Hub) liegt die Periodendauer zwischen etwa 30 und 120 Minuten.

Die Variation der Gesamtverzögerung durch Clockdrift kann durch Synchronisation der beteiligten Komponenten auf einen gemeinsamen Amtstakt komplett verhindert werden.

2.1.5.5 Minimalverzögerung bei adaptivem Jitter-Buffer

Im adaptiven Arbeitsmodus versucht der Jitter-Buffer, die durchschnittliche Verzögerung so gering wie möglich zu halten. In einer Situation, in der kein Jitter-Effekt auftritt, sinkt die durchschnittliche Verzögerung auf ein Minimum. Dieses Minimum ist in der HG-Baugruppe einstellbar. Die durchschnittliche Verzögerung, die auf Basis der aktuell gemessenen Verzögerung laufend angepasst wird, bewegt sich also zwischen zwei Grenzen: der einstellbaren Minimalverzögerung und der einstellbaren Maximalverzögerung. Die folgende Illustration verdeutlicht dies:

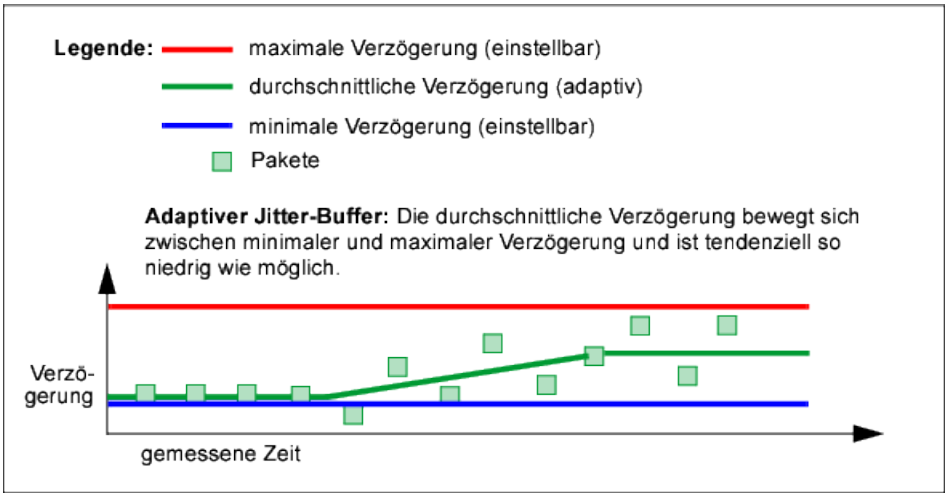


Abbildung 9: Minimalverzögerung bei adaptivem Jitter-Buffer

Die Grenzen von minimaler und maximaler Verzögerung werden auch dann eingehalten, wenn dabei Pakete verloren gehen.

2.1.5.6 Paketverlustkontrolle bei adaptivem Jitter-Buffer

Beim adaptiven JB wird die durchschnittliche Verzögerung automatisch nachgeregelt. Das Ziel dabei ist, einen möglichst guten Kompromiss zwischen möglichst kurzer durchschnittlicher Verzögerung einerseits und möglichst geringem Paketverlust andererseits zu erreichen.

Welchem dieser beiden Faktoren mehr Bedeutung beigemessen wird, ist durch einen „Präferenz-Parameter“ einstellbar. Mit Werten zwischen 0 und 8 lässt sich einstellen, ob beim Berechnen der durchschnittlichen Verzögerung tendenziell

mehr Gewicht auf die Minimierung der Verzögerung oder auf die Vermeidung von Paketverlust gelegt werden soll. Dabei bedeutet 0 „Paketverlust möglichst vermeiden“ und 8 „Durchschnittsverzögerung möglichst gering halten“. Voreingestellt ist ein mittlerer Wert (4).

Faustregel: Der Wert 0 wird ca. 10 ms höhere Durchschnittsverzögerung bewirken und der Wert 8 ca. 10 ms geringere Durchschnittsverzögerung als der mittlere Wert 4.

2.1.5.7 Parameter zur Konfiguration des Jitter-Buffers

Zum Verständnis der Delay-Parameter ist wichtig, dass sich die Werte am kompensierbaren Netzwerk-Jitter ausrichten. Wie alle IP-Gateways oder -Endpunkte schwanken auch bei HG 3500 und HG 3575 die tatsächlichen Absendezeitpunkte der Sprachpakete etwas um einen konstanten Idealwert. Diese Abweichung, der sendeseitige Eigen-Jitter, ist bereits in der Implementierung berücksichtigt.

Diese Parameter können über **AMO STMIB** (für HG3575) bzw. **AMO CGWB** (für HG 3500) eingestellt werden.

- **Jitter-Buffer-Type:** Wählen Sie aus, ob der Jitter-Buffer statisch oder adaptiv arbeiten soll. Im adaptiven Modus passt der Jitter-Buffer die Durchschnittsverzögerung entsprechend der Situation beim Datenempfang ein. Dabei wird versucht, die Verzögerung so gering wie möglich zu halten und zugleich so wenige Datenpakete wie möglich zu verlieren. Im statischen Modus bleibt die Durchschnittsverzögerung stets gleich.
- **Durchschnitts-Delay für Sprache (ms):**Mit diesem Parameter geben Sie an, wie viele Millisekunden ein IP-Paket bei IP-basierten Sprachübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. Beim Jitter-Buffer-Typ „adaptiv“ stellt der hier eingegebene Wert lediglich einen Anfangswert dar. Ein für die meisten Umgebungen empfehlenswerter Wert ist 40.
- **Maximales Delay für Sprache (ms):**Beim Jitter-Buffer-Typ „statisch“ geben Sie mit diesem Parameter an, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen bei Sprachübertragung betragen darf, bevor der Jitter-Buffer regulierend in den Datenstrom eingreift. Beim Jitter-Buffer-Typ „adaptiv“ geben Sie in diesem Feld an, wie viele Millisekunden die Durchschnittsverzögerung für Sprache maximal betragen darf. Ist die tatsächlich gemessene Verzögerung höher, gehen Pakete verloren. Bei statischem Jitter-Buffer ist 80 ein für die meisten Umgebungen empfehlenswerter Wert, bei adaptivem Jitter-Buffer beträgt der Empfehlungswert 120. Der Wert muss in jedem Fall höher sein als derjenige im Feld „Durchschnitts-Delay für Sprache (ms)“.
- **Minimales Delay für Sprache (ms):**Wenn als Jitter-Buffer-Typ „adaptiv“ ausgewählt wurde, geben Sie mit diesem Parameter an, wie viele Millisekunden die Durchschnittsverzögerung für Sprache minimal betragen darf, d. h. die Durchschnittsverzögerung wird in jedem Fall größer oder gleich sein als dieser Wert.
- **Paket-Verlust / Delay-Präferenz:**Mit diesem Parameter geben Sie im Fall von adaptivem Jitter-Buffer mit einem Wert zwischen 0 und 8 an, ob Sie im Fall von großen Paket-Verzögerungen eher den Verlust von Paketen in Kauf nehmen oder eher eine höhere Verzögerung. 0 bedeutet minimalen Paketverlust und Inkaufnahme von Verzögerungen im Sprachdatenstrom, 8 bedeutet minimale Verzögerung im Sprachdatenstrom und Inkaufnahme von

Paketverlusten. Ein für die meisten Umgebungen empfehlenswerter Wert ist 4.

- **Durchschnitts-Delay für Daten (ms):**Mit diesem Parameter geben Sie an, wie viele Millisekunden ein IP-Paket bei Datenübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. Ein für die meisten Umgebungen empfehlenswerter Wert ist 60.
- **Maximales Delay für Daten (ms):**Mit diesem Parameter geben Sie an, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen bei Datenübertragung betragen darf, bevor der Jitter-Buffer regulierend eingreift. Ein für die meisten Umgebungen empfehlenswerter Wert ist 200. Bei größeren Werten (ab ca. 200) ändert eine Parametereinstellung nichts mehr, da, sobald ein Paket im Puffer komplett empfangen wurde, dieses den Puffer sofort wieder verlässt. Werte unter 100 ms sind zwar möglich, aber in der Praxis auf keinen Fall zu empfehlen.

2.1.6 Laufzeit und dadurch bemerkbare Effekte

2.1.6.1 Allgemeine Hinweis zur Verzögerung

Man kannbei jedem IP-Hop eine Verzögerung zwischen 40-100 ms erwarten.

2.1.6.2 Verzögerung und Echo

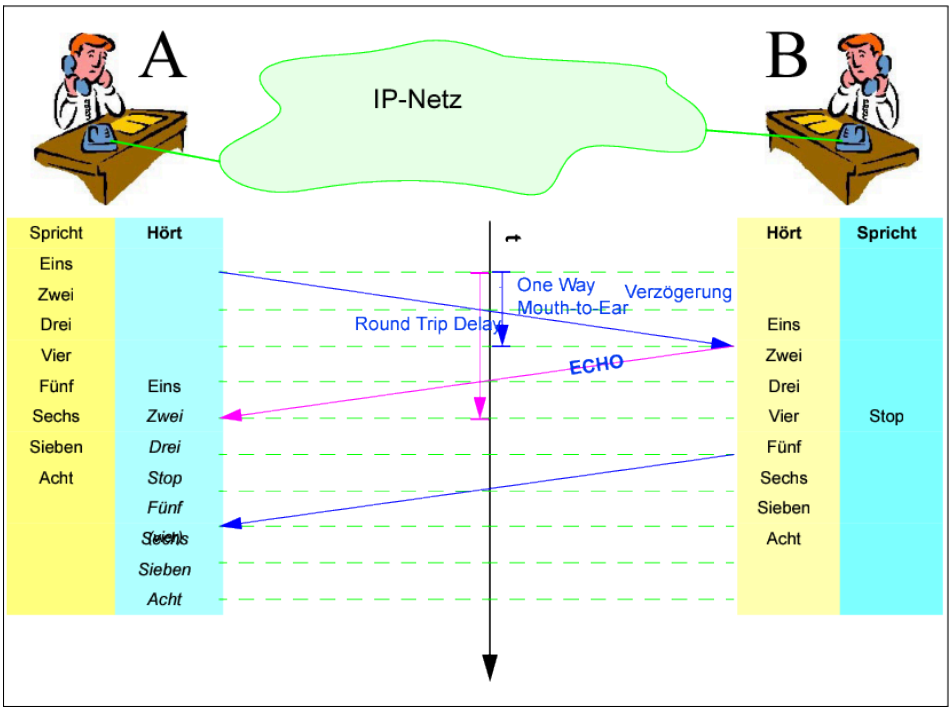


Abbildung 10: Verzögerung und Echo

Die Sprachübertragung kostet generell mehr Laufzeit, als wir es aus der klassischen Telefonie gewöhnt sind. Abbildung 10: Verzögerung und Echo auf

Seite 38 zeigt, wie sich das an einem konkreten Beispiel anhört. Hier ist das Mouth-to-Ear-Delay etwa 250 ms.

Zählt Sprecher *A* von **Eins** bis **Acht** und sagt Sprecher *B* **Stop**, nachdem er **Drei** gehört hat, so hört *A* das **Stop** während er gerade **Acht** sagt. Nun wird das Auswählen einer Zahl durch Zählen und STOP-Sagen nicht gerade sehr häufig in der Praxis vorkommen. Den Verzögerungseffekt des Round-Trip-Delays erfährt man aber trotzdem im normalen Gesprächsverlauf. Es kommt verstärkt zu *Kollisionen*, wenn der Sprecher wechselt.

Wird auf der B-Seite ein Echo erzeugt (z. B. durch das 2-Draht/4-Draht-Hybrid von analogen Endgeräten, auch Gabelübertrager genannt) so stört das den Sprecher, der gegen das anredet, was er vor z. B. einer halben Sekunde gesagt hat.

Es ist daher generell bei hohen Übertragungslaufzeiten nötig, mit echofreien Signalen auf die Übertragungsstrecke zu gehen. Bei IPDA wird das durch aktive Echo-Canceller in den HG 3500 und HG 3575-Baugruppen erreicht, welche den von A empfangenen Signalanteil im Sendesignal von B (das Echo) vor der Übertragung aus dem Sendesignal von B herausrechnen.

2.2 Architektur und Systemanforderungen

2.2.1 Voraussetzungen

Vor der Installation von IP-Gateways beim Kunden muss eine Netzwerkanalyse durchgeführt werden, um zu ermitteln, ob das IP-Netzwerk des Kunden den Betrieb von IP-Telefonen unterstützt. Hierbei werden im IP-Netzwerk Parameter wie Jitter, Paketverluste, verfügbare Bandbreite sowie unterstützte QoS-Mechanismen analysiert und es wird ermittelt, inwieweit das Netzwerk überhaupt VoIP-fähig ist.

2.2.2 Strombedarf

Beim HG 3500 Gateway handelt es sich um eine OpenScape 4000 Peripheriekarte, die in Access Points AP 3300 und AP 3700 eingebaut werden kann. Durch den Einsatz von Komponenten mit einem hohen Strombedarf (DSPs) benötigen HG 3500 Baugruppen allerdings vergleichsweise viel Energie. Infolge dieses Umstands ist die Zahl der HG 3500 Baugruppen auf insgesamt jeweils 6 pro AP 3700 IP (9 ETBs) und 10 pro AP 3700 (13 EBTs) beschränkt.

2.2.3 Netzwerk-Anforderungen

Die HG 3500 / IPDA-Komponenten stellen hohe Anforderungen an das Netzwerk, über welches sie an seine IP-Endpunkte gekoppelt werden. Voice-over-IP-Datenströme sind ebenso wie Signalisierungsverbindungen zwischen der Zentrale und den Access Points empfindlich bezüglich Paketlaufzeit, Laufzeitvarianz (Jitter) und Paketverlust.

Die Verfügbarkeit und Zuverlässigkeit eines HG 3500- / IPDA-Systems hängt entscheidend von der Qualität des benutzten IP-Netzwerkes ab.

Deshalb muss das Netzwerk vor der Installation auf Eignung für VoIP für den Einsatz von HG 3500 / IPDA geprüft werden. Genauere Informationen sind im Leitfaden HiPath-4000-/OpenScape-4000-Netzwerkanalyse zu finden.

Alle OpenScape 4000 Komponenten **müssen** an eigenen Ports von Layer 2 - Switches angeschaltet werden.

Die Verwendung von Hubs zusammen mit OpenScape 4000 kann zu Problemen führen. Daher dürfen diese in entsprechenden VoIP-Szenarien nicht eingesetzt werden. Hubs sind, falls vorhanden, durch Switche zu ersetzen.

Um hohe Dienstgüte (Sprachqualität / Echtzeitverhalten der Signalisierung) zu erreichen, ist die Unterstützung von IEEE 802.1p/q VLAN-Tagging und IETF RFC 2474 DiffServ empfehlenswert (siehe auch Abschnitt 2.4, „Netzwerkdaten“).

Wichtig: Geht die Anbindung eines Access Points über **W**ide **A**rea **N**etworks, in denen die verfügbare **Bandbreite stark eingeschränkt ist, muss eine Priorisierung** der Steuerungsinformationen (Signaling) und der Sprachdaten (Payload) für Access Points gegenüber anderen Diensten erfolgen.

Im LAN des Kunden werden häufig aus Sicherheitsgründen nur explizit bekannte TCP/IP oder UDP/IP Portnummern unterstützt. Alle anderen sind dann gesperrt. Welche Portnummern für die HG 3500 Komponenten im Netz unterstützt werden müssen, ist im Kapitel 21, „IP-Ports“ beschrieben.

IP Interface MTU

Die OpenScape 4000 IP-Schnittstellen nutzen per default eine IP Interface MTU von 1500 Bytes. Um den optimalen IP Netzwerk Durchsatz zu bekommen, wird empfohlen das IP Netzwerk sowohl für das IPDA LAN (Signaling/Media - Voice over IP) als auch das Management LAN ebenfalls mit einer MTU von 1500 Bytes zu betreiben.

Für den Fall, dass dieses nicht möglich ist, zum Beispiel aufgrund von WAN-Routern (PPPoE, IPSEC,...) mit geringerer MTU, wird empfohlen in diesen Routern das TCP - MSS Clamping einzusetzen. Diese Konfiguration im Router bewirkt, dass die OpenScape 4000 Software Komponenten die TCP Paketgröße beim nächsten TCP Three Way Handshake anpassen.

Wichtig: Dieses Verfahren gilt für TCP, aber nicht für UDP. Im Regelfall sind die UDP-Pakete (z.B. RTP-Media) aber kleiner 500 Bytes.

Ausnahme: SIP-Q via UDP

Bei Problemen besteht die Möglichkeit die IP Interface MTU für CGW-/ OpenScape 4000 SoftGate- Baugruppen über das WBM der Baugruppe zu konfigurieren. Der Wert für die IP Interface MTU sollte aber nicht kleiner als 1000 Bytes gewählt werden.

Des Weiteren reagieren die OpenScape 4000 Software Stacks in der Regel auch auf ICMP Fragmentation Needed Packets, welche dann zu adaptierten Paketgrößen führt. Dieses Verfahren kann aber erhöhte Laufzeiten hervorrufen.

2.2.4 Netzwerkdaten

Mit diesem Leistungsmerkmal werden zusätzliche Knoten/IP-Gateway im LAN des Kunden eingerichtet. Jeder Knoten/IP-Gateway benötigt Konfigurationsdaten, die mit der Netzwerkadministration des Kunden abgestimmt, dokumentiert und exakt wie abgesprochen eingerichtet werden müssen.

Für jeden neuen Knoten/IP-Gateway im LAN des Kunden müssen folgende Daten festgelegt werden:

- IP-Adresse des Knotens
- Netzmaske für das Netz, in dem der neue Knoten hinzugefügt wird
- Default-Router, über den andere Netze erreicht werden können

Zusätzlich ist für alle Netze, in welche OpenScape 4000 Komponenten eingebracht werden, zu klären, wie sie Quality of Service unterstützen. Da OpenScape 4000 IP Distributed Architecture Verfahren zur Steuerung von Quality of Service im Netz auf unterschiedlichen Protokollebenen unterstützt, ist zu klären:

- Wird IEEE 802.1 p/q VLAN-Tagging (Schicht 2) unterstützt?

  Hierfür ist es wichtig, dass alle Komponenten im Netz, mit denen eine OpenScape 4000 Komponente kommuniziert, den Standard unterstützen und entsprechend eingestellt sein müssen. Sind Knoten im Netz (insbesondere Switche und Router), welche IEEE 802.1 p/q nicht unterstützen, muss VLAN-Tagging ausgeschaltet bleiben. Die Prioritätswerte sind fest der Verkehrsart zugeordnet.
- Wird DiffServ nach RFC 2474 unterstützt, was sind die nutzbaren CodePoints?

  In den OpenScape 4000 Komponenten müssen TOS-Bytes für die folgenden Verkehrsarten auf teilweise unterschiedliche Werte eingestellt werden. Die Default-Werte gehen von DiffServ-Unterstützung im Netz aus und realisieren die Quality of Service Strategie. Mehr Informationen zum TOS-Byte finden sie im Abschnitt 2.4.1, „TOS Byte“.

Es sind auch andere Verfahren zur Priorisierung gebräuchlich, welche dann ausschließlich in den betroffenen Routern zu administrieren wären:

- Priorisierung auf Grund der IP-Adresse

  Der gesamte Verkehr aus einer Schnittstelle wird (identisch) priorisiert. Damit kann der Verkehr aus IPDA-Komponenten durch Angabe von deren IP-Adresse höher priorisiert werden als anderer Verkehr.
- Priorisierung eines Port (Socket) Bereichs

  Hier würden die IPDA-spezifischen Ports (siehe Kapitel 21, „IP-Ports“) im Netz höher priorisiert als andere Ports.

  Hier ist es unbedingt erforderlich, die **Signalisierungs**- und die Payload-Ports zu berücksichtigen. Wegen des großen Portbereichs für Payload ist dieses Verfahren nicht zu empfehlen.

- Priorisierung bestimmter Dienste (TCP, UDP)

  Die Priorisierung z.B. des UDP-Verkehrs im Netz würde zwar der Payload zu Gute kommen, aber dadurch die Signalisierung (TCP/IP) zurückdrängen. Damit ist diese Form der Priorisierung für IPDA **nicht** geeignet! Sie beeinträchtigt die Systemverfügbarkeit.

2.2.4.1 TOS Byte

Das TOS-Byte kann auf unterschiedliche Arten gelesen werden:

- Zwei 3-Bit-Werte für Precedence und Priorität
- Ein 6-Bit-Wert als Kombination der beiden 3-Bit Werte (DiffServ CP)
- Das gesamte TOS-Byte inklusive zweier Füllbits.

Für IPDA wird das gesamte TOS-Byte angegeben. Die zwei niederwertigsten Bits werden immer zu Null gesetzt. Siehe auch Abschnitt 1.1, „Schlüsselbegriffe“.

Tabelle 3: TOS-Werte

Typ	Verkehrsart	HW	TOS-Byte				IEEE 802.1p/q Priorität
	Package Handling Behavior Wie soll mit den Paketen dieser Verkehrsart umgegangen werden?		mit DiffServ CodePoint (default)		ohne DiffServ		
			binär	dez	binär	dez	
TOSPL	VoIP Payload minimales Delay geringer Paketverlust	HG 3500 HG 3575	1011 1000 (EF)	184	0001 0000	16	5
TOSSIGNL	Signalisierung zwischen OpenScape 4000 und Access Point minimaler Paketverlust geringes Delay	OpenScape 4000	0110 1000 (AF31)	104	0001 0100	20	3

TOSLAN	Signalisierung über LAN minimaler Paketverlust geringes Delay	AF	0110 1000 (AF31)	104	0001 0100	20	3
TOSMODEM	Signalisierung über Survivability-Verbindung minimaler Paketverlust geringes Delay		0111 0000 (AF 32)	112	0001 0000	16	- entfällt, da PPP-Verbindung

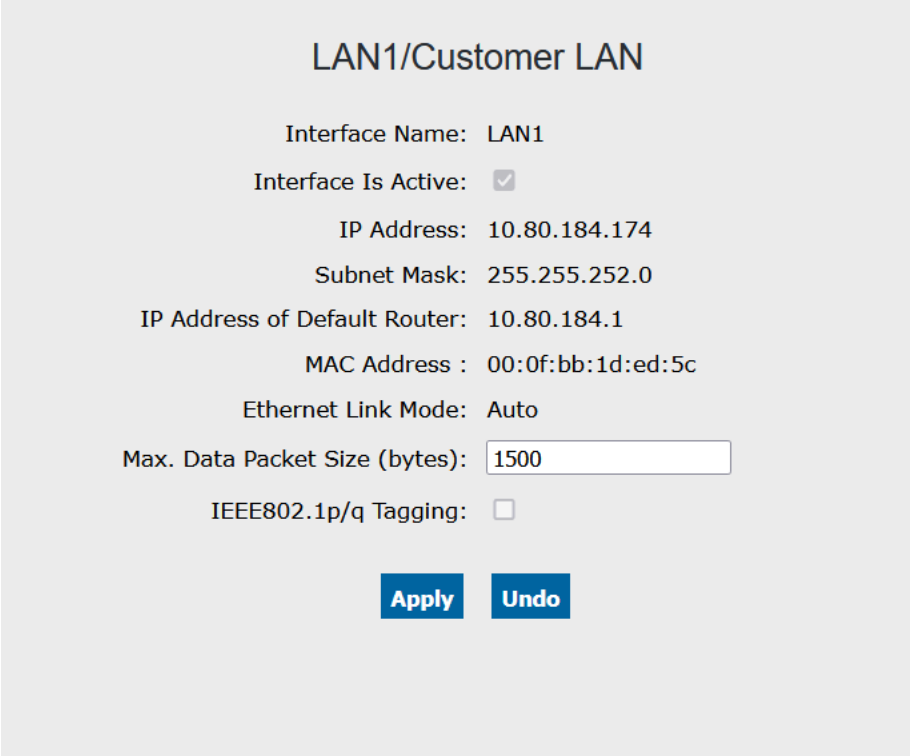
Die Werte für **TOSSIGNL** (AMO CGWB, AMO SIPCO), **TOSLAN** (AMO STMIB) und **TOSMODEM** müssen ungleich Null sein. **TOSLAN** und **TOSMODEM** müssen unterschiedlich eingestellt werden. **TOSPL** wird im AMO CGWB, AMO SIPCO und AMO STMIB eingestellt.

Wichtig ist, dass im Netz das geforderte Verhalten *(Package Handling Behavior)* erreicht wird. Die absoluten Zahlenwerte für TOS und IEEE 802.1 Priorität sind dabei unbedeutend. Sie dienen ausschließlich dazu, das geforderte Package Handling Behavior zu bezeichnen.

Die in der Tabelle angegebenen Werte sind die Default-Einstellungen der IP-Gateway Loadware (STMI/NCUI). Diese Einstellungen entsprechen den OSCAR-Spezifikationen.

Sie können die L2-Prioritätswerte aber auch ändern über

1) **WBM > Konfiguration > Netzwerk & Routing > Netzwerkschnittstellen > LAN1 (LAN1)**



Die Werte für die VLAN-Priorität (Layer 2) können über AMO nicht geändert werden. Daher ist die L2-Priorität für den Signalisierungsanschluss (CCA/CCB, AMO SIPCO) fest kodiert.

Wichtig: Wenn Sie die TOS-Werte für die **HG 3500** mit **AMO CGWB** ändern, muss danach ein Reboot der betroffenen Gateways durchgeführt werden. Wenn die TOS-Werte für die **HG 3575** mit **AMO STMIB** geändert werden, muss ein `EXEC-USSU:UPDATAP;` bzw. `RESET-USSU:LTU;` abhängig davon, welche Parameter geändert wurden. Beide Kommandos erzeugen einen Restart des Shelfs Wenn Werte mit dem **AMO SIPCO** geändert werden, muss danach ein Soft-Restart im CCA und CCB erfolgen.

Wertebereich für die TOS-Werte (0-255)

Ab HiPath 4000 V5 R1 ist der Wertebereich für die TOS-Werte (0-255) erweitert worden (siehe Tabelle 4 „TOS Byte Abhängigkeit“).

Wichtig: Die Spalte „Dezimal 8-Bit“ enthält die Werte, die für die AMO-Kommandos gebraucht werden. Die anderen Spalten dienen lediglich zu Informationszwecken.

Tabelle 4: TOS Byte Abhängigkeit

DSCP-Wert	Dezimal 6-bit	Dezimal 8-Bit	Hexadezimal 6-Bit	Hexadezimal 8-Bit
DSCP63	63	252	3F	FC
DSCP62	62	248	3E	F8
DSCP61	61	244	3D	F4
DSCP60	60	240	3C	F0
DSCP59	59	236	3B	EC
DSCP58	58	232	3A	E8
DSCP57	57	228	39	E4
CS7	56	224	38	E0
DSCP55	55	220	37	DC
DSCP54	54	216	36	D8
DSCP53	53	212	35	D4
DSCP52	52	208	34	D0
DSCP51	51	204	33	CC
DSCP50	50	200	32	C8
DSCP49	49	196	31	C4
CS6	48	192	30	C0
DSCP47	47	188	2F	BC
EF	46	184	2E	B8
DSCP45	45	180	2D	B4
DSCP44	44	176	2C	B0
DSCP43	43	172	2B	AC
DSCP42	42	168	2A	A8
DSCP41	41	164	29	A4
CS5	40	160	28	A0
DSCP39	39	156	27	9C
AF43	38	152	26	98
DSCP37	37	148	25	94
AF42	36	144	24	90

DSCP-Wert	Dezimal 6-bit	Dezimal 8-Bit	Hexadezimal 6-Bit	Hexadezimal 8-Bit
DSCP35	35	140	23	8C
AF41	34	136	22	88
DSCP33	33	132	21	84
CS4	32	128	20	80
DSCP31	31	124	1F	7C
AF33	30	120	1E	78
DSCP29	29	116	1D	74
AF32	28	112	1C	70
DSCP27	27	108	1B	6C
AF31	26	104	1A	68
DSCP2 5	25	100	19	64
CS3	24	96	18	60
DSCP23	23	92	17	5C
AF23	22	88	16	58
DSCP21	21	84	15	54
AF22	20	80	14	50
DSCP19	19	76	13	4C
AF21	18	72	12	48
DSCP17	17	68	11	44
CS2	16	64	10	40
DSCP15	15	60	F	3C
AF13	14	56	E	38
DSCP13	13	52	D	34
AF12	12	48	C	30
DSCP11	11	44	B	2C
AF11	10	40	A	28
DSCP9	9	36	9	24
CS1	8	32	8	20
DSCP7	7	28	7	1C

DSCP-Wert	Dezimal 6-bit	Dezimal 8-Bit	Hexadezimal 6-Bit	Hexadezimal 8-Bit
DSCP6	6	24	6	18
DSCP5	5	20	5	14
DSCP4	4	16	4	10
DSCP3	3	12	3	C
DSCP2	2	8	2	8
DSCP1	1	4	1	4
DF	0	0	0	0

2.2.5 Bandbreitenbedarf

Die tatsächlich erforderliche Bandbreite pro aktiver Payload-Verbindung richtet sich nach dem eingestellten Codierungsalgorithmus, der Samplingzeit und ob das Leistungsmerkmal „Signalisierungs- und Sprachverschlüsselung (SPE)“ aktiviert ist.

2.2.5.1 Codierung

Es sind z.B. folgende Codierungen einstellbar:

- G.711 (PCM) mit Unterstützung für Annex 1 (packet loss enhancements) und Annex 2 (Voice Activity Detection with Comfort Noise Generation).
- G.729A Sprachkomprimierung mit 8 kBit/s.
- G.729AB mit Voice Activity Detection.

Wichtig: Bei der Codierung von TDM-Sprachpaketen nach G.711 kommt es praktisch zu keiner Verzögerung (algorithmische Verzögerung = 0 ms).

Weitere Details zu Codecs siehe Abschnitt 1.3, „Codec-Standards“.

2.2.5.2 Samplingzeit

Bevor die Sprachsignale in IP-Pakete gepackt werden können, muss die Sprache zunächst digitalisiert werden.

Für Telefonie-Anwendungen wird die Sprache alle 125 µs mit 8 Bit gesampelt. Dabei ist es nicht sinnvoll, jedes einzelne 8-Bit-Sample in ein eigenes IP-Paket zu packen. Bei der Codierung nach G.711 werden stattdessen mindestens 240 8-Bit-Samples in einem IP-Paket zusammengefasst.

Um 240 Sprach-Samples zu erhalten, benötigt man 30 ms.

Die Samplingzeit ist dabei die Zeit, die benötigt wird, um eine festgelegte Anzahl von Sprach-Samples zu erstellen, die dann in einem IP-Paket ausgesendet werden.

Naturgemäß wird der IP-Overhead immer kleiner, je länger die Samplingzeit ist. Um den Bandbreitenbedarf so gering wie möglich zu halten, muss also die Samplingzeit erhöht werden.

Eine längere Samplingzeit führt allerdings auch zu einer größeren Gesamtverzögerung.

Wichtig: Zwischen der Verringerung von Verzögerungen und der Einsparung von Bandbreite muss jeweils ein Kompromiss gefunden werden.

Je nach Codec-Typ kann als Samplingzeit für IP-Gateways ein Wert zwischen 10 und 90 ms eingestellt werden.

2.2.5.3 IP-Overhead

Der IP-Overhead umfasst die RTP (Real Time Protocol)-, UDP (User Datagram Protocol)- und IP-Header sowie die Ethernet-Frames und zusätzliche Oktette für das QoS-Tagging. Für G.711 wäre ein typischer IP-Overhead-Wert beispielsweise 30% .

2.2.5.4 Bandbreitenbedarf pro Verbindung

Bei der Berechnung der Bandbreite wird ein Wert von 70 Byte für den Overhead zugrundegelegt, der sich wie folgt ergibt: RTP (12 Byte), UDP (8 Byte), IP (20 Byte), 802.1Q VLAN-Tagging (4 Byte), MAC (einschl. Preamble, FCS, 26 Bytes).

Wichtig: Die Bandbreitenanforderungen setzen einen **Vollduplexbetrieb** voraus! Beim Betrieb von Halbduplex wird die doppelte Bandbreite benötigt.

Bandbreite für aktive DMC-Masterverbindungen ohne SPE:

Tabelle 5: Bandbreite für aktive DMC-Masterverbindungen ohne SPE

Codec	Samplingz [ms]	Payload-Frames pro Sekunde	Payload [Bytes]	Bytes gesamt	Bandbreite [Bit/s]
G.711	10	100,00	80	150	120000
	20	50,00	160	230	92000
	30	33,33	240	310	82667
	40	25,00	320	390	78000

Codec	Samplingz [ms]	Payload-Frames pro Sekunde	Payload [Bytes]	Bytes gesamt	Bandbreite [Bit/s]
G.729AB	20	50	20	90	36000
	30	33,33	30	100	26667
	40	25,00	40	110	22000
	60	16,67	60	130	17333
G.723	30	33.33	24	94	25067
	60	16,67	48	118	15733

Bandbreite für aktive DMC-Masterverbindungen mit SPE:

Tabelle 6: Bandbreite für aktive DMC-Masterverbindungen mit SPE

Codec	Samplingz [ms]	Payload-Frames pro Sekunde	Payload [Bytes]	Bytes gesamt	Bandbreite [Bit/s]
G.711	10	100,00	90	160	128000
	20	50	170	240	96000
	30	33,33	250	320	85333
	40	25,00	330	400	80000
G.729AB	20	50	30	100	40000
	30	33,33	40	110	29333
	40	25,00	50	120	24000
	60	16,67	70	140	18667
G.723	30	33.33	34	104	27733
	60	16,67	58	128	17067

Bandbreite für stillgelegte Masterverbindungen ohne SPE:

Tabelle 7: Bandbreite für stillgelegte Masterverbindungen ohne SPE

Codec	Frame	Packets		Packegröße [Byte]		Bandbreite [kBit/s]	SID[1] relative to Active
	Länge [Byte]	Länge	Rate	Reine Daten	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	1	71	0,6	0,7%
G.729A	2	1000 ms	1,00 /s	2	72	0,6	1,6%
G.723	4	990 ms	1,01/s	4	74	0,6	2,4%

Bandbreite für stillgelegte Masterverbindungen mit SPE:

Tabelle 8: Bandbreite für nicht mehrbenutzte Master-Verbindungen (mit SPE)

Codec	Frame	Packets		Packegröße [Byte]		Bandbreite [kBit/s]	SID[2] relative to Active
	Länge [Byte]	Länge	Rate	Reine Daten	Ethernet	Ethernet	Ethernet
G.711	1	1000 ms	1,00 /s	11	81	0,6	0,8%
G.729A	2	1000 ms	1,00 /s	12	82	0,7	1,6%
G.723	4	990 ms	1,01/s	14	84	0,7	2,4%

2.2.5.5 Voice Activity Detection (VAD)

VAD sorgt dafür, dass ungenutzte Bandbreite während der Sprechpausen für andere Anwendungen im IP-Netzwerk zur Verfügung steht und kann eine Reduzierung des Bandbreitenbedarfs um 50% bis 75% bewirken (weitere Details siehe Abschnitt 4.3, „Voice Activity Detection (VAD)“).

1 Rate zwischen aktiver Masterverbindung und stillgelegter Masterverbindung

2 Rate zwischen aktiver Masterverbindung und stillgelegter Masterverbindung

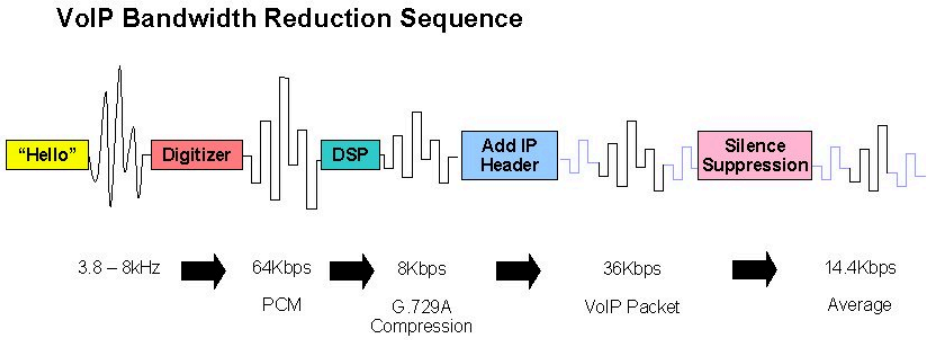


Abbildung 11: Bandbreitenreduzierung bei VoIP

2.2.5.6 Hinweise zu DMC

Beim Herstellen einer DMC-Verbindung wird immer auch eine „Master-Verbindung“ aufgebaut.

Die Master-Verbindung folgt dabei dem selben Pfad wie die Signalisierung über sämtliche Gateways zwischen den beiden IP-Clients.

Über die Master-Verbindung wird sichergestellt, dass bei Aufruf eines Leistungsmerkmals, das eine Mehrfachverbindung (z.B. eine Konferenz) zur Folge hat, jederzeit die benötigten Ressourcen zur Verfügung stehen. Der Aufruf der entsprechenden Leistungsmerkmale erfolgt außerdem verzögerungsfrei, da die Verbindung bereits aufgebaut ist.

Das Konzept der Master-Verbindung hat allerdings auch Nachteile:

- Für die Aufrechterhaltung der Master-Verbindung wird zusätzliche Bandbreite benötigt.
- Je nach Konfiguration kann es zwischen den IP-Clients zu deutlichen Verzögerungen und mehrfachen Hops kommen, wenn die Payload über die Master-Verbindung transportiert wird. Insbesondere dann, wenn IP-Endpoints auf unterschiedliche Access Points in IP-Systemen zugreifen, können Verzögerungen über das akzeptable Maß hinaus auftreten.

Bild 13 „DMC und Master-Verbindung“ zeigt eine Gesprächsverbindung mit DMC und Master-Verbindung zwischen zwei IP-Clients in zwei unterschiedlichen über IP vernetzten OpenScape 4000-Systemen.

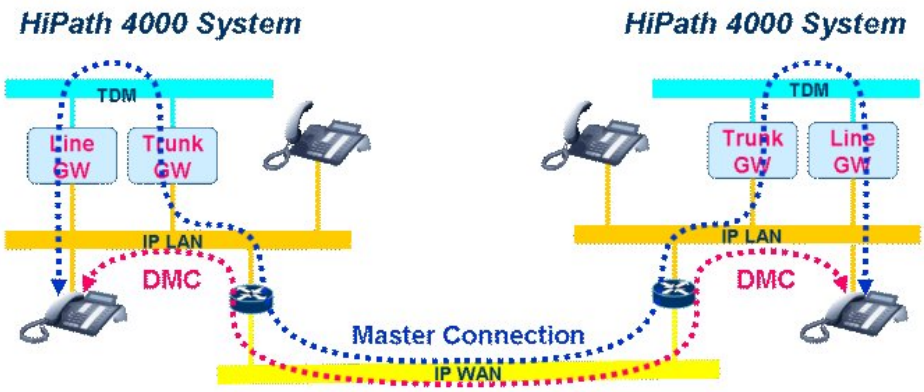


Abbildung 12: DMC und Master-Verbindung

Durch Aktivierung von VAD lässt sich der Bandbreitenbedarf auf der Master-Verbindung auf ein vernachlässigbares Maß reduzieren.

Die Verzögerungen bei den einzelnen TDM-IP-Umwandlungsschritten summieren sich. Im obigen Beispiel durchläuft die Master-Verbindung 3 Hops. Bei der Codierung nach G.711 mit einer Samplingzeit von 30 ms und einem High-Quality-Netzwerk (20 ms Verzögerung) ergibt dies über die ganze Verbindung hinweg eine Verzögerung von ca. 200 ms. Die DMC-Verbindung durchläuft nur einen einzigen Hop, wodurch die Verzögerung über die ganze Verbindung hinweg ca. 80 ms ausmacht.

Weitere Informationen finden Sie unter Abschnitt 4.1, „Direct Media Connection (DMC)“.

2.2.6 B-Kanäle

Die folgende Tabelle gibt einen Überblick über die Anzahl der zur Verfügung stehenden B-Kanäle in Abhängigkeit der aktivierten Leistungsmerkmale.

Tabelle 9: B-Kanäle in Abhängigkeit der aktivierten Leistungsmerkmale

	STMI2		NCUI2+		STMI4		NCUI4	
	2 DSP (Q2316-X)	4 DSP (Q2316-X10)	2 DSP **(Q2305-X35)**	4 DSP **(2305-X40)**	2 DSP (Q2324-X500)	5 DSP **(Q2324-X511)**	**2 DSP (Q2324-X)**	**5 DS (Q23 X11)**
Standards	60	120	60	120	60	120	60	120
QDC	56	112	56	112	60	120	60	120
SRTP	45	90	45	90	50	120	50	120
QDC+ SRTP	42	84	42	84	50	120	50	120
DMC	45	90	45	90	50	100	50	100
QDC+ DMC	42	84	42	84	50	100	50	100
DMC+ SRTP	32	63	32	63	40	100	40	100
QDC+ DMC +SRTP	30	60	30	60	40	100	40	100

Wichtige Hinweise zu QDC

QDC wird über das WBM auf dem Gateway aktiviert und benötigt Performanceresourcen.

QDC wird **bei der Kanalreduktion nicht automatisch berücksichtigt**. Daher muss die **Anzahl der Kanäle bei Aktivierung von QDC manuell** (je nach Kartentyp) an die in der Tabelle oben genannten Werte angepasst werden, wenn QDC aktiviert ist. Wenn keine Anpassung stattfindet, treten Performance-Probleme auf.

Automatische B-Kanal-Reduktion

Mit den Funktionen für Signalisierung und Nutzlastverschlüsselung (SPE) sowie DMC wird eine automatische B-Kanal-Reduktion durchgeführt, d. h. die eingestellten aktuellen Werte werden um einen festen Prozentsatz reduziert. Dieser Prozentsatz hängt von der verwendeten Hardware ab.

Wichtig: Die automatische B-Kanal-Reduktion wird mit der Funktion QDC nicht durchgeführt. Diese B-Kanal-Reduktion muss manuell unter Bezugnahme auf Tabelle 9 „B-Kanäle in Abhängigkeit der aktivierten Leistungsmerkmale“ erfolgen.

Diese Reduktion wird nicht nur auf Kartenebene, sondern auch auf Funktionsebene berechnet. Das bedeutet, dass die oben genannten Prozentwerte pro konfigurierter Funktion berechnet werden.

Beispiele für die Unterstützung von Einzelfunktionen (STMI2/STMI4):

1) DMC ist aktiviert für HG 3550 auf Q2324-X511

DMC aktiviert auf Q2324-X511: Reduzierung der b-Kanäle um 17% (= minus 20 b-Kanäle)

=> Maximale Anzahl der verfügbaren b-Kanäle: 120-20= **100**

2) SPE und DMC ist für HG 3550 auf Q2316-X aktiviert.

SPE aktiviert auf Q2316-X: Reduzierung der b-Kanäle um 25% (= minus 15 b-Kanäle)

=> 60-15= **45**

DMC zusätzlich aktiviert auf Q2316-X: Reduzierung der b-Kanäle um 25% (der maximalen Anzahl der verfügbaren b-Kanäle / abhängig von der Karte und/oder Anzahl der DSPs = minus 15 b-Kanäle)

=> Maximale Anzahl der verfügbaren b-Kanäle: 45-15= **30**

Beispiel für die Unterstützung mehrerer Funktionen (STMI2/STMI4/STMIX):

1) **DMC** wird für 2 HG 3550 Schaltungen mit 40 b-Kanälen auf Q2324-X500 aktiviert. Die restlichen 20 b-Kanäle sind für das HG 3530 konfiguriert.

SPE aktiviert auf Q2324-X500 für HG 3550: Reduzierung der b-Kanäle um 17% (von 40 b-Kanälen = minus 7 b-Kanäle)

=> Maximale Anzahl der verfügbaren b-Kanäle für HG3550: 40-7= **33**

Das Gateway HG 3530 kann nicht als DMC-Endpunkt fungieren. Daher werden die 20 b Kanäle bei HG 3530 nicht reduziert.

2) SPE wird für 2 HG 3550 Schaltungen mit 40 b-Kanälen und HG 3530 für 20 b-Kanäle auf Q2324-X500 aktiviert.

SPE aktiviert auf Q2324-X500 für HG 3550: Reduzierung der b-Kanäle um 17% (von 40 b-Kanälen = minus 7 b-Kanäle)

=> Maximale Anzahl der verfügbaren b-Kanäle für **HG3550**: 40-7= **33**

SPE aktiviert auf Q2324-X500 für HG 3530: Reduzierung der b-Kanäle um 17% (von 20 b-Kanälen = minus 3 b-Kanäle)

=> Maximale Anzahl der verfügbaren b-Kanäle für **HG3530**: 20-3= **17**

Diese reduzierten B-Kanalwerte sind die Obergrenze für die Pfadauswahl.

Die B-Kanalzahl steigt entsprechend an, wenn Funktionen deaktiviert werden.

Zusammenfassung:

Im AMO BFDAT kann nur die maximale Anzahl der B-Kanäle konfiguriert werden. Mit AMO BCSU kann die Anzahl der aktuell verfügbaren B-Kanäle angezeigt und die B-Kanäle können konfiguriert werden.

Die folgenden Tabellen geben einen Überblick über die Anzahl der zur Verfügung stehenden B-Kanäle in Abhängigkeit der aktivierten Leistungsmerkmale.

2.2.6.1 B-Kanal-Konfiguration

2.2.6.1.1 AMO BFDAT

Mit AMO BFDAT wird das Profil der Karte mit einer maximalen Anzahl von B-Kanälen definiert.

- ADD-BFDAT, Parameter **BRDBCHL**

  Der Parameter **BRDBCHL** legt fest, ob ein Block für eine Karte mit 60 oder 120 b Kanälen konfiguriert wird.
- ADD-BFDAT, Parameter **FUNCTION**

  Mit dem Parameter **FUNCTION** können Sie die Funktionen des gemeinsamen Gateways (z.B. HG 3500, HG 3530, etc.) konfigurieren.
- CHANGE-BFDAT, Parameter **BCHLCNT**

  Mit dem Parameter **BCHLCNT** können Sie die maximale Anzahl der B-Kanäle pro Funktion konfigurieren. Dieser Wert darf nicht höher sein als die maximal mögliche Anzahl von B-Kanälen für diese Funktion (siehe Abschnitt 2.6.1.2, „AMO BCSU“, Parameter **BCHLCNT**).

2.2.6.1.2 AMO BCSU

Das mit AMO BFDAT konfigurierte Profil (maximale Anzahl der B-Kanäle (**BRDBCHL**) und konfigurierte Funktionen (**FUNCTION**)) wird von AMO BCSU ausgewertet. Zusätzlich werden die aktivierten Features im System (z.B. DMC, SPE) berücksichtigt. Eine automatische b-kanalige Reduktion wird durchgeführt (siehe Abschnitt 2.6.1.2, „Bei Bandbreitenproblemen usw. muss der aktuelle Wert der B-Kanäle, die für jede konfigurierte Funktion verwendet werden können, reduziert werden. Dies kann in AMO BCSU mit den B-Kanalparametern erfolgen (**BCHL3530**, **BCHLSIP**, **BCHL3550**).“).

Mit DISPLAY-BCSU können die folgenden Informationen gefunden werden:

- Wie viele b-Kanäle stehen auf der Karte zur Verfügung (**BCHANNELS**).

- Wie viele B-Kanäle wurden mit AMO BFDAT pro Funktion konfiguriert (**BCHANNELS**).
- Wie viele b-Kanäle sind pro Funktion möglich (**BCHLCNT**). Der Parameter **BCHLCNT** hängt davon ab, welches Merkmal aktiviert wurde (siehe Abschnitt 2.6, „B-Kanäle“). Der Wert im Parameter **BCHLCNT** kann kleiner sein als die konfigurierte Anzahl von B-Kanälen für diese Funktion in AMO BFDAT. Es steht jedoch nur die Anzahl der b Kanäle des Parameters **BCHLCNT** für die Funktion zur Verfügung.

Bei Bandbreitenproblemen usw. muss der aktuelle Wert der B-Kanäle, die für jede konfigurierte Funktion verwendet werden können, reduziert werden. Dies kann in AMO BCSU mit den B-Kanalparametern erfolgen (**BCHL3530**, **BCHLSIP**, **BCHL3550**).

2.2.6.2 Anzeige der aktuell verfügbaren/konfigurierten B-Kanäle (mögliche IP-basierte Verbindungen)

Die Gesamtzahl der aktuell genutzten B-Kanäle wird wie gewohnt in AMO BCSU angezeigt. Die Anzahl der B-Kanäle wird in AMO BSCU mit dem entsprechenden B-Kanalparameter für jede Funktion konfiguriert (**BCHL3530**, **BCHLSIP**, **BCHL3550**, **BCHLWAML** and **BCHL3570**). AMO BFDAT enthält den Parameter **BRDBCHL**. Hiermit wird die maximale Anzahl der B-Kanäle für die Karte definiert (60 oder 120 B-Kanäle).

Mit AMO BCSU können Sie die Anzahl der verfügbaren B-Kanäle für die gemeinsame Gateway-Karte abfragen. Für eingerichtete HG3575-Baugruppen muss der AMO UCSU verwendet werden.

Wichtig: Die Ermittlung der B-Kanal-Werte ist bei HG 3500 und HG 3575 unterschiedlich!

Die Abfrage der genutzten Kanäle bzw. der genutzten Bandbreite ist nach entsprechender Konfiguration mit dem AMO GKTOP möglich.

Der Befehl `DISPLAY-BCSU:TAB,1,<LTU-Nummer>;` gibt drei b-Kanalwerte aus:

- Die maximale Anzahl der von der Baugruppe unterstützten B-Kanäle,
- die Anzahl der pro Funktion belegten B-Kanäle und
- die maximal mögliche Anzahl von B-Kanälen pro Funktion.

2.2.7 Verkehrsbezogene Hinweise

Vom verkehrstechnischen Standpunkt her kann ein HG 3500-IP-Gateway wie eine Verbindungsleitung mit 60 bzw. 120 Verbindungen behandelt werden. Die Anzahl der erforderlichen Verbindungen hängt dabei von der Zahl der pro HG 3500 konfigurierten IP-Telefone und deren jeweiligem Verkehrswert (CCS) ab. Mithilfe einer Standard-ErlangB-Berechnung lässt sich die Anzahl der pro Gateway erforderlichen Verbindungsleitungen/Verbindungen für eine bestimmte Konfiguration ermitteln.

Die Tools arbeiten mit einem vereinfachten Verfahren, das pro Gateway-Typ 240 Standard-Benutzer und 60/120 „High-Traffic“-Benutzer (z.B. Call Center-Agenten) erlaubt. Es ist auch ein Mischbetrieb mit Standard- und „High-Traffic“-

Benutzern möglich, wobei die Gesamtanzahl pro Gateway allerdings auf 60/120 beschränkt ist. Auf diese Weise wird sichergestellt, dass Call Center-Agenten jederzeit eine Leitung belegen können.

Kapazität

Pro HG 3500-Gateway können maximal 240 IP-Clients konfiguriert werden.

Ein für 60 Verbindungen ausgelegtes Gateway kann normalerweise 240 Benutzer mit jeweils 6 CCS bedienen. Falls die Benutzer ein höheres Verkehrsaufkommen erzeugen, wird ein Gateway für 120 Verbindungen benötigt.

Für Call Center-Agenten wird üblicherweise ein Verkehrswert von 32 CCS angesetzt, so dass am Gateway pro Agent eine Verbindung benötigt wird. Somit ist die mögliche Anzahl von Call Center-Agenten bei der HG 3500 je nach Gateway-Typ (60/120 Verbindungen) auf 60 bzw. 120 beschränkt.

Wichtig: Die Kombination von normalen Benutzern und Call Center-Agenten auf ein- und derselben Baugruppe ist möglich. Um jedoch für Call Center-Agenten jederzeit eine Verbindung bereitstellen zu können, wird für normale Benutzer ein Verkehrswert von 1 Erlang (36 CCS) angesetzt.

2.3 Unterstützte Gateways

2.3.1 HG 3500 (Common Gateway)

2.3.1.1 Allgemeine Informationen

HG 3500 wird mit den folgenden Baugruppen unterstützt:

- STMI2 (Q2316-X und Q2316-X10)
- STMI4 (Q2324-X500 und Q2324-X510)
- STMIX (Q2343-X)

Das HG 3500 ersetzt die folgenden Gateways:

- HG 3530 (HFA-Teilnehmer)
- HG 3540 (SIP-Trunking (native & SIP-Q) und SIP-Teilnehmer)
- HG 3550 (IP-Trunking)
- HG 3570(IPDA (host side) - Master und IPDA (host side) - DMC)

MIt dem HG 35000 Gateway können verschiedene Sub-Leistungsmerkmale (z.B. Trunking und IPDA) auf einer Baugruppe gleichzeitig und parallel genutzt werden (**Multiple Feature Support** (**MFS**)). Das Gateway kann aber auch weiterhin als **Single Feature Configuration** verwendet werden.

Das Konzept von HiPath Feature Access (HFA) wird auf die anderen Funktionalitäten ausgeweitet.

Wichtig: Einschränkung: Je Baugruppe kann nur jeweils ein Trunking Protokoll konfiguriert werden. Eine Mischung mit anderen Funktionalitäten ist uneingeschränkt möglich.

Konfigurationsbeispiel zu Multiple Feature Support: siehe Kapitel 15, „Multiple Feature Support Konfiguration am Common Gateway (Beispiel)“

Beispiele für die Konfiguration einzelner Features finden Sie in den Dokumenten:

- HiPath Feature Access (HFA)
- IP Distributed Architecture (IPDA)
- Access Point Emergency (APE)
- SIP Connectivity > Kapitel 6, „Konfiguration SIP-Q-Trunking / Native SIP Trunking“ oder
- H323-/H323-Annex-Trunking

2.3.1.2 Baugruppentausch

Um ein STMI-/STMI2-/STMI4-Board zu ersetzen, beachten Sie bitte Folgendes:

- „Kleines“ STMI/STMI2/STMI4 durch „kleines“ STMI/STMI2/STMI4 ersetzen: kein Problem
- „Großes“ STMI/STMI2/STMI4 durch „kleines“ STMI/STMI2/STMI4 ersetzen: kein Problem
- „Kleines“ STMI/STMI2/STMI4 durch „großes“ STMI/STMI2/STMI4 ersetzen: kein Problem
- „Großes“ STMI/STMI2/STMI4 durch „kleines“ STMI/STMI2/STMI4: funktioniert nur, wenn maximal 60 B-Kanäle verwendet werden

Vorgangsweise:

- Tauschen Sie die Baugruppe aus.
- Sie müssen hierbei nicht alle Sätze auf der Baugruppe und die Baugruppe selbst löschen, sondern es reicht aus mit AENDERN-BCSU die Sachnummer anzupassen.

```
AENDERN-
BCSU:TYP=SACHNR,LTG=<LTG>,LTU=<LTU>,EBT=<EBT>,SACHNR1=<Sachnummer
 der
auszuwechselnden Baugruppe>,SACHNR2=<Sachnummer der neuen
 Baugruppe>;
```

- Führen Sie einen Neustart der Baugruppe aus über

```
RESTART-BSSU:ADRART=LAGE,LTG=<LTG>,LTU=<LTU>,EBT=<EBT>;
```

Die Konfiguration des SIP-Profils einschließlich der Anmeldedaten für den SIP-Anbieter (sofern verwendet) wird auf dem Board/der Hardware gespeichert (d. h. STMI2/STMI4/STMIX und vSTMI auf SoftGate). Bitte beachten Sie beim Austausch von Hardware, dass ein „Factory Reset“ vom Web-Based Management durchgeführt wird, bevor Sie das Board austauschen, um sicherzustellen, dass alle privaten Daten entfernt werden.

Anmerkung: Vor diesem Schritt sollte ein HG3500 Backup durchgeführt werden, um sicherzustellen, dass die alten Daten für das neue Board zur Verfügung stehen.

2.3.1.3 Leistungsumfang

Wichtig: Informationen zum gemeinsamen Leistungsumfang von HG 3500 und HG 3575 siehe Kapitel 4, „Leistungsmerkmale und Einschränkungen“.

- Das HG 3500 Gateway ist dafür ausgelegt, 60/120 Verbindungen in Fast Ethernet-Pakete umzuwandeln und eine TDM-IP-Umwandlung für 60/120 gleichzeitige Verbindungen durchzuführen.
- HG 3500 Gateways lassen sich als **Gateways** zur Absicherung gegen Ausfälle einzelner Gateways konfigurieren.

Mehr Informationen Informationen zu Gateways

Im System können eine oder mehrere HG 3500 als IP-Gateways für den Fall eingerichtet werden, dass eines der installierten Gateways ausfällt.

Dieses Konzept ist besonders effizient und kostengünstig, da durch ein einziges Gateway gleich mehrere Gateways abgesichert werden können. Ein einzelnes Gateway bietet zwar keinen Schutz beim gleichzeitigen Ausfall mehrerer Gateways, aber dieser Fall ist höchst unwahrscheinlich.

Beim Ausfall eines Gateways programmiert das System ein Gateway mit den Parametern des ausgefallenen Gateways. Somit können sich die IP-Clients neu anmelden und normal weiterbetrieben werden.

IP-Telefone melden sich automatisch am aktivierten Gateway an, ohne dass hierfür irgendwelche Administrationsmaßnahmen notwendig sind. Beim Betrieb am Gateway bleiben den Benutzern die ursprünglichen Leistungsmerkmale und Nebenstellen erhalten.

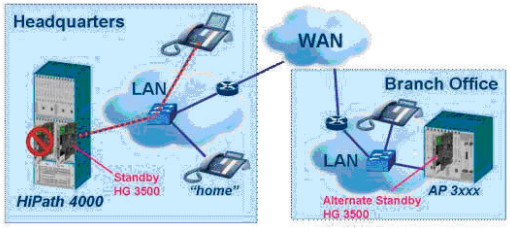


Abbildung 13: HG 3500 als Gateway

Das jeweilige Gateway kann im Host-System und/oder auf einem IP Access Point eingerichtet sein. Die einzige Vorgabe ist, dass sich sämtliche aktive und Standby-Gateways im selben lokalen IP-Subnetz befinden müssen.

Wichtig: Standby-Gateways und IP-Clients müssen sich im selben System befinden. Z.B. können von einem Standby-Gateway keine IP-Clients gesteuert werden, die sonst von einem Gateway in einem anderen System gesteuert werden. Standby-Gateways auf IP Access Points bieten IP-Benutzern im Host-System keine Absicherung beim Ausfall des Hosts, da Ausfälle auf höheren Ebenen (z.B. Shelf-, AP-, Host- oder Stromausfälle) keine automatische Umschaltung anstoßen.

Details zur Konfiguration entnehmen Sie bitte Kapitel 8, „Standby Board HG 3500“.

- Das HG 3500 Gateway unterstützt **sekundäre Gateways** und sorgt so für eine umfassende Redundanz im IP-Telefonverkehr. Über sekundäre Gateways lässt sich für IP-Clients eine volle Redundanz und somit wirksamer Schutz bei Ausfällen auf höheren Ebenen, z.B. Komplettausfällen von Access Points oder Hosts, erreichen.

Mehr Informationen Informationen zu sekundären Gateways

Zur Absicherung gegen Ausfälle auf höheren Ebenen (z.B. Access Point- oder Host-Ausfälle) können im System sekundäre Gateways eingerichtet werden. Bei dem sekundären Gateway handelt es sich um ein zusätzliches, vollständig konfiguriertes Gateway für einen IP-Client an einer beliebigen Stelle im OpenScape 4000-System. Jeder durch ein sekundäres Gateway abgesicherten IP-Benutzer hat zwei Nebenstellen, z.B. x1333 auf dem primären Gateway, und x5333 auf dem sekundären Gateway.

Falls die Verbindung mit dem primären Gateway unterbrochen wird (z.B. bei einem Shelf- oder Host-Ausfall), versucht das IP-Telefon, sich am sekundären Gateway anzumelden. Sofern das sekundäre Gateway in Betrieb ist und IP-Konnektivität besteht, werden sämtliche durch sekundäre Gateways abgesicherte Telefone am jeweiligen Sekundär-Gateway angemeldet und bleiben komplett betriebsbereit.

Während der Benutzer am sekundären Gateway angemeldet ist, stehen ihm sämtliche Leistungsmerkmale zur Verfügung, die für die Zweit-Nebenstelle aktiviert wurden. Bei der primären Nebenstelle eingehende Anrufe werden automatisch über das neue Leistungsmerkmal „Alternate Routing on Error“ auf die Zweit-Nebenstelle umgeleitet.

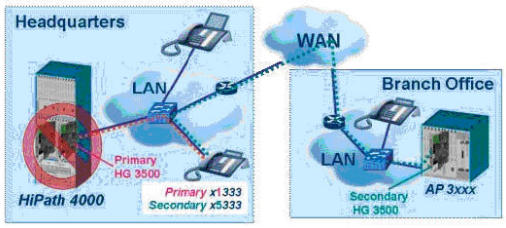


Abbildung 14: HG 3500 als sekundäres Gateway

Die Anzahl der für einen Failover-Betrieb notwendigen sekundären Gateways und Leitungen lässt sich mit Hilfe der folgenden Maßnahmen beschränken:

- Bei den sekundären Gateways lässt sich durch Einstellen einer höheren Blockierungsrate die Anzahl von IP-Benutzern beschränken, die gleichzeitig telefonieren können.
- Durch „Undertrunking“ kann die Anzahl der für die sekundären Gateways benötigten zusätzlichen Leitungen verringert werden.

Es handelt sich hierbei um optionale Maßnahmen, über deren Anwendung jeder Kunde selbst entscheiden kann. Es erscheint jedoch sinnvoll, die Ressourcen (und damit Kosten) für einen Failover-Betrieb gering zu halten, da entsprechende Ausfallszenarien äußerst selten eintreten dürften.

Wichtig: Sekundäre Gateways und IP-Clients müssen sich im selben System befinden. Sekundäre Gateways bieten IP-Benutzern eine automatische Absicherung, sofern das sekundäre Gateway in Betrieb ist und IP-Konnektivität zwischen dem IP-Client und dem Gateway besteht.

- Das HG 3500 Gateway unterstützt **QoS**. Um bei Verbindungen über IP-Netzwerke die bestmögliche Sprachqualität zu erzielen, wurden VLAN-Tagging gemäß IEEE 802.1p/q auf Schicht 2 sowie DiffServ (laut Definition in RFC 2474) auf der IP-Schicht implementiert.
- Damit die entsprechenden Mechanismen genutzt werden können, müssen sämtliche Switches und Router im IP-Netzwerk des Kunden IEEE 802.1p/q bzw. DiffServ-Priorisierung unterstützen.
- Das HG 3500 Gateway unterstützt „**sekundäre Clients**“.

Mehr Informationen zu sekundären Clients

1) Bei den sekundären Clients handelt es sich um Soft-Clients, für die dieselbe Rufnummer wie für ein reguläres IP-Telefon konfiguriert ist.

- Für sekundäre Clients wird keine ComScendo-Lizenz benötigt.
- Es wird eine Soft-Client SW-Lizenz benötigt.

  Der Standard H225-Signaling-Port ist 1720 und wird bei Soft-Clients zum Aufbau von Telefonverbindung von der Baugruppe zum Soft-Client verwendet. Es kann sein, dass der Soft-Client einen anderen Port verwenden muss. Läuft eine andere H323-Anwendung gleichzeitig mit dem Soft-Client, so kann ein anderer H225-Signaling-Port auf den Soft-Client eingerichtet werden. Der Soft-Client informiert HG 3500 bei der Anmeldung und dann verwendet HG 3500 diesen Port zum Verbindungsaufbau.

  Der Soft-Client kann als nicht-standardisierter VPN-Client verwendet werden. In dieser Einstellung überprüft HG 3500 die gelieferte IP-Adresse und die tatsächliche Adresse auf dem verbundenen CorNetTC-Socket und teilt dem Soft-Client die tatsächliche IP-Adresse mit, falls sich die 2 Adressen unterscheiden.

Vorteile von sekundären Clients:

- Über sekundäre Clients kann remote auf sämtliche OpenScape 4000-Leistungsmerkmale zugegriffen werden.
- Beim Starten des Soft-Client auf einem PC an einem beliebigen Standort wird das Büro-IP-Telefon (mit der betreffenden Rufnummer) automatisch abgemeldet. Dem Client-Benutzer stehen anschließend die selben Leistungsmerkmale und Berechtigungen wie am Büro-IP-Telefon zur Verfügung.
- Kehrt der Remote-Benutzer wieder an seinen Arbeitsplatz zurück, wird er aufgefordert, das IP-Telefon zu reaktivieren. Das IP-Telefon wird damit wieder in den normalen Betriebszustand versetzt, bis es erneut durch Aktivierung des zugehörigen Soft-Clients abgemeldet wird.

- Eine „**Überbelegung“ (Overbooking)** ist möglich, d.h. es können pro HG 3500 Gateway mehr IP-Telefone konfiguriert werden, als Verbindungen zur Verfügung stehen (maximal 240 Teilnehmer).

Mehr Informationen zu „Überbelegung“ (Overbooking)“

1) Bei „Overbooking werden immer mehr Endgeräte (**ANZSATZ**) konfiguriert als eigentlich Teilnehmer (**ANZBKAN**) da sind. Bei den B-Kanälen wird dann die eigentliche Anzahl der Teilnehmer konfiguriert.

Beispiel:

In einem Lager sind fünf Mitarbeiter beschäftigt. Das Lager ist aber so groß, dass 10 Endgeräte konfiguriert werden. Da nur fünf Mitarbeiter gleichzeitig telefonieren können, sind nur fünf B-Kanäle notwendig.

Parameter: ANZSATZ=10, ANZBKAN=5

- Bei einer STMI-Karte mit 60 (DSP) Kanälen können beispielsweise bis zu 240 IP-Teilnehmer konfiguriert, aber nicht mehr als 60 gleichzeitige Anrufe getätigt werden. Die Einschränkung der DSP-Kanäle gilt nicht für vSTMI-Karten.
- Sämtliche IP-Telefone unterstützen **DHCP** und werden über das HG 3500 Gateway im DHCP-Modus unterstützt. Dabei muss im IP-Netzwerk ein DHCP-Server eingerichtet sein. Andernfalls müssen sämtliche Clients eine statische IP-Adresse haben.
- Die **Anschaltung von analogen Geräten über ein AP 1120** Analog-Gateway wird unterstützt. Weitere Details finden Sie im E-Doku-Angebot im Intranet (http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=AP%201120&product_version_main=&product_version_sub=&search_term_type=all&ter
- Innerhalb von Einzelsystemen und vernetzten Systemen besteht für Benutzer volle **Mobilität**.
- Das HG 3500 Gateway wird an allen **IPDA Access Points** unterstützt.

2.3.1.4 Einschränkungen

- CQR Viewer
- Die Applikation CQR Viewer wird nur für HFA (**FUNCTION=HG3530**) und IPDA (**FUNCTION=HG3570**) unterstützt, nicht für Trunking (**FUNCTION=HG3550**).
- HG 3500 unterstützt nur Telefon-Adapter, die keinen eigenen B-Kanal benötigen.
- Folgende Adapter werden nicht unterstützt:
  - Telefonadapter,
  - a/b-Adapter,
  - S0-Adapter
  - V.24-Adapter
- Autoset Relocate, Teleworking V2.6 und das Workstation-Protokoll werden bei HG 3500 nicht unterstützt.
- HG 3500 Gateways arbeiten nicht mit Lastverteilung. Es erfolgt eine feste Zuordnung von IP-Telefonen zu einem HG 3500 Gateway.
- Das integrierte HG 3500 Gateway funktioniert nicht mit (H.323/H.450- oder SIP-kompatiblen) IP-Telefonen/Clients von Fremdanbietern.
- Für das integrierte HG 3500 Gateway wird eine statische IP-Adresse benötigt.
- NTP (Network Time Protocol) wird beim HG 3500 nicht unterstützt

2.3.2 HG 3575

2.3.2.1 Allgemeine Informationen

HG 3575 wird mit den folgenden Baugruppen unterstützt:

- NCUI2+ (Q2305-X35 und Q2305-X40)
- NCUI4 (Q2324-X und Q2324-X10)

Es gibt im Gegensatz zu HG 3500 kein Standby-Konzept für HG 3575.

2.3.2.2 Baugruppentausch

OpenScape 4000 - Access Point

1) Ausschalten des Shelfs
```
AUSS-USSU:LTG=1,LTU=17;
```
2) Alte Baugruppe ziehen, neue Baugruppe stecken

Wenn die neue Baugruppe die gleiche Sachnummer wie die alte Baugruppe hat, dann fahren Sie bitte direkt mit Punkt 6. “Shelf einschaltenâ fort.

3) AP löschen
```
EXEC-USSU:ART=DELAP,LTU=17;
```
4) Neue Sachnummer dem Shelf zuweisen
```
AE-UCSU:ART=AP,LTG=1,LTU=17,LTSACHNR=Q2305-X10;
```
5) AP konfigurieren
```
EXEC-USSU:ART=CONFAP,LTU=17;
```
6) Shelf einschalten
```
EINS-USSU:EINHEIT=LTG,LTG=1,LTU=17;
```

OpenScape 4000 - Switch

```
AENDERN-
STMIB:MTYPE=NCUI2,LTU=18,SLOT=99,TYPE=GLOBAL,PATTERN=213;
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=IFDATA,VLAN=NEIN,TOSLAN=72,TOSMO►
DEM=80,VLANID=0,BITRATE=100MBFD;
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=SERVIF,LOGINTRM="TRM",LOGINPPP="PPP";
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,TOSPL=48,PRIO=PRIO1,CO►
DEC=G711,VAD=NEIN,RTP="30";
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO2,CODEC=G729,VAD=NEIN,RTP="20
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NEIN,RTP="20
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO4,CODEC=NONE,VAD=NEIN,RTP="20
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO5,CODEC=NONE,VAD=NEIN,RTP="20
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO6,CODEC=NONE,VAD=NEIN,RTP="20
```

```
AENDERN-
STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO7,CODEC=NONE,VAD=NEIN,RT
AEND-
STMIB:MYTP=NCUI2,LTU=18,TYP=JB,AVGDLY=40,MAXDLYV=120,MINDLYV=20,P
LOSS=4,AVGDLYG=60,MAXDLYD=200,JBMODE=1;
AEND-STMIB:MTYP=NCUI2,LTU=18,TYP=SIGQOS,BANDW=0,MAX►
RTD=0,MINTHRPT=0,SIGPTHSW=STD,QOSSTAT=NEIN;
AEND-
STMIB:MTYP=NCUI2,LTU=18,TYP=H323,Q931T1=50,Q931T2=500,GWNAME="HG3
AEND-
STMIB:MTYP=NCUI2,LTU=18,TYP=DMCDATA,DMERL=NEIN,DMCCONN=0;
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=SNMP,CS1="public";
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=WBMDATA,LOGINWBM="HP4K-
DEVEL",ROLE=ENGR;
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=WBMDATA,LOGINWBM="HP4K-
SU",ROLE=SU;
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=WBMDATA,LOGINWBM="HP4K-
ADMIN",ROLE=ADMIN;
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=WBMDATA,LOGINWBM="HP4K-
READER",ROLE=READONLY;
AEND-STMIB:MYTP=NCUI2,LTU=18,TYP=GWSECTOR,GWSECTNR=0;
AEND-
STMIB:MYTP=NCUI2,LTU=18,TYP=DLSDATA,DLSPORT=10444,DLSACPAS=NEIN;
```

WBM Konfiguration

Weitere Einstellungen über das WBM durchführen.

CLI-Konfiguration

Damit wieder eine Verbindung zum Switch zustande kommt, müssen die IP-Adressen in der neuen Baugruppe über das CLI konfiguriert werden.

2.4 Leistungsmerkmale und Einschränkungen

Die folgenden Leistungsmerkmale werden durch HG 3500 **und** HG 3575 unterstützt. HG 3500 spezifische Leistungsmerkmale finden Sie im Abschnitt 3.1.3, „Leistungsumfang“.

2.4.1 Direct Media Connection (DMC)

Die Gateways HG 3500 und HG 3575 unterstützen **DMC** (**D**irect **M**edia **C**onnection).

Mehr Informationen zu Direct Media Connection (DMC)

Die Gateways HG 3500 und HG 3575 unterstützen DMCs (Direct Media Connections, oder Peer-to-Peer-Verbindungen) zwischen zwei IP-Telefonen oder zwischen einem IP-Telefon und einer weiteren IP-Baugruppe wie z.B. HG 3500 oder HG 3575. Die Payload-Vermittlung zwischen zwei DMC-Endpunkten (DMC-Endpunkte = IP-Telefon, HG3500/3575) erfolgt dabei komplett im IP-Netz, d.h. ohne Beteiligung des TDM-Koppelfelds. Dies gewährleistet bestmögliche Sprachqualität bei minimalen Verzögerungen, da nur ein einziger Hop (Umwandlung TDM-IP-TDM) notwendig ist.

Wichtig: Beim Aufruf von Leistungsmerkmalen, die eine Mehrfachverbindung (d.h. mit mehr als 2 Teilnehmern) zur Folge haben, wird die Payload in sämtlichen Gateways über den Payload-Pfad geroutet. Bei bestimmten Szenarien kann es hierbei zu unerwünschten Verzögerungen kommen (weitere Details siehe Abschnitt 2.5.6, „Hinweise zu DMC“).

Bei einer DMC-Verbindung wird zusätzliche Bandbreite für die Master-Verbindung benötigt. Allerdings kann der Bandbreitenbedarf für die Master-Verbindung durch die Verwendung von VAD bei den IP-Clients nahezu auf Null reduziert werden. Falls eine Aktivierung von VAD nicht möglich ist, wird die doppelte Bandbreite benötigt.

Mehr Informationen zu DMC und Bandbreitenbedarf finden Sie im Abschnitt 2.5.6, „Hinweise zu DMC“.

2.4.2 Sprachkomprimierung

Die Gateways HG 3500 und HG 3575 unterstützen die **Sprachkomprimierung** nach dem Standard G.711A mit 64 kBit/s. Darüber hinaus wird auch eine Codierung nach G.729A und G.729AB unterstützt. Weitere unterstützte Codierungen sind G.711U, G.723 (nur HG 3500), G.729 und G.729B.

Die konkreten Bandbreitenanforderungen pro Verbindung richten sich dabei auch nach dem zusätzlichen IP-Overhead und verschiedenen anderen Einstellungen (siehe hierzu Abschnitt 2.5.4, „Bandbreitenbedarf pro Verbindung“).

Wichtig: Die Umsetzung der Sprachkomprimierung sowie der Gateway-Funktionalität erfolgt in den DSP-Baugruppen.

Mehr Informationen zur Sprachkomprimierung

Sprachkomprimierung nutzt komplexe Algorithmen, um die Bandbreite des Sprachsignals, zum Beispiel G.729, auf ein Achtel der vom ursprünglichen PCM-Signal benötigten Bandbreite zu reduzieren. Die Sprachqualität wird dabei nur geringfügig verschlechtert.

Problematisch ist Sprach-Kompression, wenn sie mehrfach hintereinander angewendet wird. D.h. das ursprüngliche PCM-Signal wird nach einem Verfahren komprimiert, übertragen und wieder zu einem Standard-PCM-Signal expandiert. Danach wiederholt sich das Ganze auf einem weiteren Streckenabschnitt. Schlimmstenfalls mit einem anderen Verfahren. Die mehrfache Anwendung insbesondere unterschiedlicher Kompressionsverfahren beeinträchtigt die Sprachverständlichkeit sehr, im schlimmsten Fall bis zur Unverständlichkeit.

Verkettung von komprimierten Übertragungsabschnitten - insbesondere nach unterschiedlichen Verfahren - muss daher möglichst vermieden werden.

Da auch alle digitalen Sprachspeichersysteme für Ansagen, VoiceMail etc. die Sprache komprimiert speichern, müssen solche Geräte im Zusammenhang mit komprimierten Übertragungsstrecken besonders beachtet werden.

Innerhalb des OpenScape 4000 Systems werden Verbindungen zu Ansage- /Musikeinspielungs-Geräten sowie zu Konferenzeinrichtungen

grundsätzlich unkomprimiert geschaltet, um verzerrungsfreie Musik bzw. gute Sprachverständlichkeit bei Konferenzen zu garantieren.

Die im Zusammenhang mit Sprach-Kompression angegebenen Faktoren, wie z.B. Kompression auf ein Achtel der ursprünglich (unkomprimiert) benötigten Bandbreite, beziehen sich immer ausschließlich auf die Sprachdaten selber. Werden diese Daten mittels IP übertragen, so muss die IP-Verpackung, der „Protokoll-Overhead“, mit berücksichtigt werden. Die zu übertragenden Sprachdaten werden durch die Kompression um den angegebenen Faktor reduziert, der Overhead bleibt aber gleich groß. Damit sinkt die im IP-Netz benötigte Bandbreite nie um den angegebenen Kompressionsfaktor, sondern immer wesentlich weniger. Berücksichtigen Sie bei der Dimensionierung der Bandbreite immer die Werte aus Kapitel 3, „Lastkalkulation“ im Dokument „IP Distributed Architecture (IPDA)“.

2.4.3 Voice Activity Detection (VAD)

Die Gateways HG 3500 und HG 3575 unterstützen **VAD** (**V**oice **A**ctivity **D**etection, Sprachpausenerkennung).

Mehr Informationen zu Voice Activity Detection (VAD)

Die Sprach-Aktivitätserkennung (VAD) sorgt dafür, dass ungenutzte Bandbreite während der Sprechpausen für andere Anwendungen im IP-Netzwerk zur Verfügung steht.

Da bei einem Telefongespräch normalerweise immer nur einer der Teilnehmer spricht und der andere zuhört, wird die belegte Bandbreite im Prinzip nur in einer Richtung (vom Sprecher zum Zuhörer) genutzt. In der anderen Richtung (Zuhörer -> Sprecher) werden lediglich Umgebungsgeräusche und „Stille“ übertragen. Bei VAD-Funktion macht man sich diese Erkenntnis zunutze, indem die Übertragung unterbrochen wird, sobald eine Sprechpause eintritt, und so die Datenrate ganz erheblich reduziert wird. Sobald Sprachsignale erkannt werden, wird die Übertragung in der entsprechenden Richtung sofort wieder aufgenommen (mit voller Bandbreite).

Wird in einer Richtung wirklich NICHTS mehr übertragen, so empfindet die Empfängerseite das Ausbleiben von Hintergrundgeräuschen meist als Leitungsstörung und damit als unangenehm. Deshalb wird - in Abhängigkeit vom verwendeten Codec - manchmal ein extrem komprimiertes Hintergrundgeräusch übertragen oder Rauschen eingespeist.

Das Problem bei VAD ist es, zwischen übertragungswerten *Geräuschen* und *Stille* zu unterscheiden. Nebengeräusche im Raum sollten unter *Stille* fallen, leise gesprochene Worte aber unter *Sprache*. Im Übergangsbereich ist es unvermeidlich, dass Anfänge bzw. Enden von Sprachaktivität beeinträchtigt (im schlimmsten Fall abgeschnitten) werden.

Auch bei VAD ist die Kettung problematisch. Bei mehreren Übertragungsstrecken, die in Folge VAD anwenden, verstärken sich die Nebeneffekte. Die Kettung von Übertragungsstrecken mit VAD muss daher vermieden werden.

Die eingesparte Bandbreite beläuft sich auf 50 bis 75 Prozent.

Die Berechtigung VAD ist standardmäßig deaktiviert, kann für Sprachverbindungen aber jederzeit aktiviert werden.

Wichtig: VAD darf bei Fax-, Modem- oder Datenverbindungen nicht aktiviert sein.

2.4.4 Comfort Noise Generation (CNG)

Die Gateways HG 3500 und HG 3575 unterstützen **CNG** (**C**omfort **N**oise **G**eneration).

Ist VAD aktiv, emuliert der DSP auf der Zielseite das Hintergrundrauschen von der Ausgangsseite, damit nicht der Eindruck entsteht, dass die Verbindung getrennt wurde.

2.4.5 Echo-Cancellation

Die Gateways HG 3500 und HG 3575 unterstützen **Echo-Cancellation** (Echokompensation) (Umsetzung in den On-Board-DSP-Baugruppen) gemäß ITU-T-Standard G.168.

Mehr Informationen zu Echo-Cancellation (Echokompensation)

Echo entsteht an allen analogen 2-Draht/4-Draht-Hybriden, z.B. im Gabelübertrager eines analogen Telefons, sowie durch die akustische Überkopplung von Lautsprecher und Mikrofon im Telefonhörer beim Empfänger.

Ist die Laufzeit zwischen dem Erzeugen eines Tons und dem Eintreffen des Echos beim Sprecher (Round Trip Delay) sehr gering, so stört das Echo nicht weiter. Je größer diese Laufzeit aber wird, um so störender wird das Echo. Die Laufzeiten bei IP-Übertragung sind sehr groß. Damit werden Echos immer als extrem störend wahrgenommen. Deshalb ist es wichtig, dass alle Signale echofrei sind, bevor sie im IP-Netz übertragen werden. In Abschnitt 1.6.2, „Verzögerung und Echo“ sind die resultierenden Effekte durch Verzögerung und Echo ausführlich dargestellt.

Die Echo-Cancellation unterdrückt das Echo, indem sie es aus dem Datenstrom herausfiltert. Echo-Cancellation soll immer möglichst nahe an der Quelle des Echos eingesetzt werden.

Ein Beispiel soll das erläutern:

- Teilnehmer A ist über eine IP-Strecke mit Teilnehmer B verbunden.
- Das Endgerät des Teilnehmers B erzeugt ein Echo des Signals von Teilnehmer A.
- Das Echo soll nun nahe an der Quelle, d.h. im Bereich des Teilnehmers B unterdrückt werden, so dass das Signal von B nach A echofrei ist, bevor es auf die IP-Strecke geht.

Die Echo-Cancellation (Echounterdrückung) ist ein sehr komplexer Vorgang in der digitalen Signalverarbeitung, der das übertragene Nutzsignal (ohne Echoanteil) geringfügig beeinträchtigen kann.

Echo-Cancellation wird für alle Sätze automatisch eingerichtet, ist aber abschaltbar.

Datenübertragung mit Analogmodems und Fax nutzt komplizierte Phasenmodulationsverfahren, die durch Echo-Cancellation gestört werden.

2.4.6 Redundante LAN-Schnittstelle

Das im Dokument „IP Distributed Architecture (IPDA)“, Kapitel 6, „Hinweise für Netzwerkadministratoren“ beschriebene Leistungsmerkmal “Redundante LAN-Schnittstelle“ wird grundsätzlich unterstützt. Nur wenn als Funktion WAML konfiguriert ist, wird dieses Leistungsmerkmal nicht unterstützt.

2.4.7 Security

2.4.7.1 Administrationszugriff

Der Zugriff für Administrationszwecke ist durch entsprechende Authentifizierungsverfahren abgesichert.

Zum Schutz sämtlicher Dateien und Debug-Daten in der HG 3500 ist der Zugriff nur über https und SSH möglich.

2.4.7.2 Zugriff auf SNMP

Der Zugriff auf SNMP ist durch Community-Strings für lesenden und schreibenden Zugriff beschränkt. Diese Community-Strings können im **WBM > Wartung > SNMP > Communities** konfiguriert werden.

2.4.7.3 Sicherheit bei der CorNetTC Registrierung

Die Anmeldung der IP-Telefone an HG 3500 ist über SHA1 abgesichert. Bei Payload- und Signalisierungsverbindungen findet keine Verschlüsselung statt.

2.4.7.4 Anschaltung der IP-Gateways im Internet bzw. über externe Provider

Eine Anbindung der IP-Gateways an das Internet bzw. externe Provider stellt eine Sicherheitslücke dar („unischeres“ LAN/WAN). Deshalb müssen in diesem Fall IP- bzw. MAC-Adress-Filter gesetzt werden. Dies kann über das WBM der Baugruppe durchgeführt werden.

WBM > Explorer > Sicherheit > MAC-Adress-Filter bzw. **WBM > Explorer > Sicherheit > IP-Adress-Filter**.

Für eine detailierte Beschreibung siehe „OpenScape 4000 V, Gateways HG 3500 und HG 3575, Administratordokumentation“ ().

2.4.8 Ressource Manager (RM)

Wichtig: Der Einsatz des Ressource Manager wird für stand alone Systeme mit HFA und IPDA freigegeben.

In einem komplexen IP-Netzwerk steht normalerweise nicht in allen Segmenten die gleiche Bandbreite zur Verfügung.

Mit dem Ressource Manager (RM) lässt sich die Bandbreite im jeweiligen IP-Netzwerk für bis zu 800 Segmente verwalten und überwachen.

Der RM aktualisiert jedesmal beim Auf- oder Abbau einer Verbindung eine Cluster-Matrix. Anhand dieser Matrix kann ermittelt werden, ob in einem der beteiligten Segmente ein Ressourcenengpass besteht. Abhängig von der konfigurierten und der tatsächlich vorhandenen Bandbreite werden neue Verbindungen entweder zugelassen oder abgewiesen.

Der RM berechnet die tatsächliche Bandbreite, wobei Komprimierungseinstellungen, DMC, FAX und andere Faktoren berücksichtigt werden.

Mehr Informationen zum Ressource Manager finden Sie im Kapitel 17, „Ressource Manager Funktionalität“.

2.4.9 Einschränkungen

2.4.9.1 Loadware-Update oder Reset der Baugruppe

Problembeschreibung:

Eine HG 3500 ist als SIP-Trunking-Gateway konfiguriert. Um eine fehlerfreie Funktionalität der Baugruppe zu gewährleisten, müssen die Parameter für die Verbindung zum Web Based Management der Baugruppe (AMO CGWB, Parameter **MGNTIP** und **MGNTPN**) und den Backup-Server (AMO CGWB, Parameter **BUSIP** und **BUSPN**) konfiguriert sein.

Nach einem Reset der Baurguppe oder nach einem Loadware Update werden zwar die IP-Adressen (**MGNTIP** und **BUSIP**) wieder hergestellt nicht aber die Port-Nummern (**MGNTPN** und **BUSPN**). Diese werden mit den Default-Werten (in beiden Fällen „0“) versehen. Dadurch kann keine Verbindung mehr zum Backup-Server hergestellt werden. Die nötigen Konfigurationsdaten für die SIP-Trunking-Verbindung, die im WBM eingestellt und auf dem Backup-Server gesichert waren, können nicht geladen werden. Die SIP-Trunking-Verbindung kann nicht wieder hergestellt werden.

Lösung:

Parameter im AMO CGWB prüfen und gegebenenfalls neu einrichten:

```
AEN-CGWB:MTYP=CGW,LTU=<number>, EBT=<number>,
 TYP=MGNTDATA, MGNTPN=8000,BUSPN=443;
```

Oder bei der Einrichtung der Baugruppe die Konfigurationsdaten aus dem WBM im Flash-Memory der Baugruppe sichern:

WBM > Wartung > Aktionen > Automatische Aktionen > Lokale Konfiguration für Upgrade speichern

Für eine detailierte Beschreibung siehe „OpenScape 4000 V, Gateways HG 3500 und HG 3575, Administrator Dokumentation“ ().

2.4.9.2 Mögliche IP-Hops

Wichtig: Bei mehr als 3 IP-Hops kann es in einem Voice over IP-System zu Einschränkungen kommen, d.h. das Delay kann zu hoch werden und die Folge sind schlechte Sprachqualität oder fehlschlagende Leistunsgmerkmale.

2.5 Ladekonzept der Gateway-Baugruppen

2.5.1 Wichtige Hinweise

- Dieses Kapitel beschreibt nur den Loadware-Update der Gateway-Baugruppen.
- Den Update des gesamten Systems führen Sie wie gewohnt mit den OpenScape 4000 Assisant Funktionen Software Transfer und Software Aktivierung durch.
- Um die Ausfallzeiten des Systems zu minimieren, können Sie die Gateway-Karten zunächst mit dem in den folgenden Abschnitten beschriebenen Ladekonzept und anschließend mit den Funktionen Softwaretransfer und Softwareaktivierung aktualisieren.
- Die Softwareversorgung des STMIX Hardwareboards erfolgt ausschließlich über HTTPS.

2.5.2 Hinweise zur Loadware der IP-Gateways

- Das IP Gateway HG3575 kann zwei Loadware-Images speichern, allerdings ist nur eine Loadware die „Golden Load“, die nach einem Kaltstart (Power Off) geladen wird.
- Loadware-ID-Check
- Bei jedem Hochlauf der HG3575 wird ein sogenannter LW-ID-Check durchgeführt, bei dem die aktuell geladenen Loadware der Baugruppe mit der Loadware-Version auf der Harddisk (:PDS:APSP/LTG/LGA0/PZKNCI40) verglichen wird.

  Sollte der Check negativ sein, also eine unterschiedliche Loadware auf der HD gespeichert sein, so wird die Loadware von der HD auf die NCUI mittels FTP transferiert und anschliessend installiert/neu gestartet.
- Installation NCUI-Loadware (PZKNCUI40)
- Eine im Hintergrund geladene/transferierte NCUI-Loadware (PZKNCUI40) wird mittels Warmboot installiert.

  Dieser Warmboot kann durch folgende Aktionen/Ereignisse gestartet werden:

  – Gezieltes Deaktivieren/Aktivieren über AMO USSU (`AUSS-USSU`/`EINS-USSU`).
  – Gezieltes Restarten des Access Points mittels `EXEC-USSU:UPDATAP,<AP-Nummer>;`. Dadurch werden neue

Konfigurationsdaten zum Access Point geladen und ein Warmboot angestoßen.
  - Gezieltes Neustarten nach LW-Transfer (initiert durch negativen LW ID Check während des Startup).
  - nach Verbindungsverlust im TCP (**ALVTIME**).
- Golden-Loadware-Check
- Bei der HG3575 heisst die aktuell zu ladende Loadware „Golden Loadware“ (auch im Auslieferungszustand ist eine Loadware auf der NCUI2+/NCUI4-Baugruppe auf dem Flash enthalten).

  Der Golden-Loadware-Check wird immer nach dem Laden/Neustarten einer neuen Loadware (Loadware Hochrüstung/Loadware-ID-Check negativ) durchgeführt . Wenn dieser Check erfolgreich war, wird der Ladepointer entsprechend umgeschrieben, so dass die Golden Loadware der neuen Loadware entspricht.

2.5.3 Ladekonzepte

Ladekonzept für HG 3500/HG 3575

- Die Loadware für HG 3500/HG 3575 wird über HTTPS geladen (siehe Abschnitt 5.4, „Update der Loadware mit Hilfe des Web Based Managements“ und Abschnitt 5.5, „Update der Loadware mit Hilfe des LW Update Manager“).
- Das Laden der Loadware kann während des Normalbetriebs im Hintergrund erfolgen, d.h. Die Aktivierung der neuen Loadware kann zu einem späteren Zeitpunkt (verkehrsschwächere Zeit) erfolgen. Die Aktivierung sollte dennoch möglichst zeitnah geschehen, um Probleme zu vermeiden.
- Optimiertes Laden für HG 3500 Gateways
- Da mit der Common Gateway Entwicklung nun die Software aller bisherigen Gateways, also HG 3530, HG 3540, HG 3550 und HG 3570, zu einem Software-Packet zusammengefasst wurden, hat sich die Software-/Loadware-Größe entsprechend erhöht. Dies hat eine Ladezeit von ca. 15 Minuten zur Folge. Aus diesem Grunde wurde das Laden der STMI-Loadware optimiert.

  Es gibt zwei CGW-STMI2-Baugruppen und zwei CGW-STMI4-Baugruppen. Das optimierte Handling für CGW-STMI-Baugruppen erlaubt es, dass das Loadware-File nur einmal für diese Baugruppen geladen wird, selbst wenn die HW-ID unterschiedlich ist.

  Daraus ergeben sich folgende Anwendungsfälle:

  - Beide STMI4-Typen und ein STMI2-Typ vorhanden => Loadware-File wird nur einmal übertragen und dann an alle entsprechenden Baugruppen verteilt.
  - Beide STMI2-Typen vorhanden => Loadware-File muss zweimal übertragen werden, weil die STMI2-Firmware nicht mehr geändert werden kann.

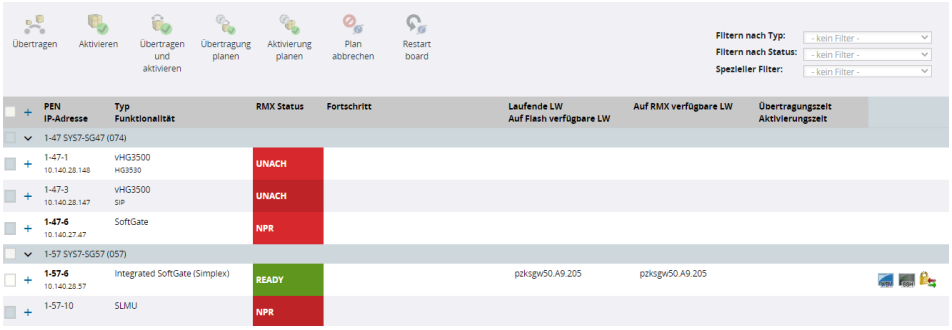
  STMI4-Baugruppen müssen mindestens Firmware **STMI4_FW_070725** haben, um das optimierte Ladekonzept für die verschiedenen CGW-STMI-Baugruppen verwenden zu können.

Wichtig: Ab V10R0 wird die Unterstützung für STMI2 nicht mehr angeboten. Der Ersatz für STMI2 ist STMIX.

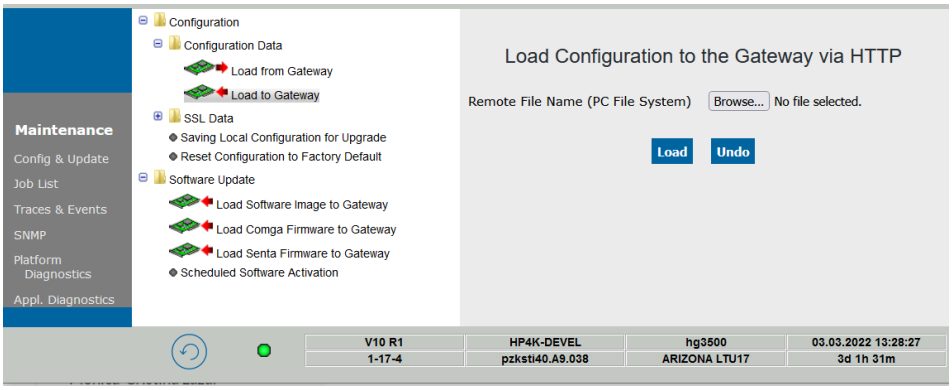
2.5.4 Update der Loadware mit Hilfe des Web Based Managements

Wichtig: Nachteil Es kann nur jeweils eine IP-Gateway-Baugruppe hochgerüstet werden!

- Melden Sie sich hierfür am OpenScape 4000 Assistant an und wählen Sie **Expertenmodus > Gateway Manager**.

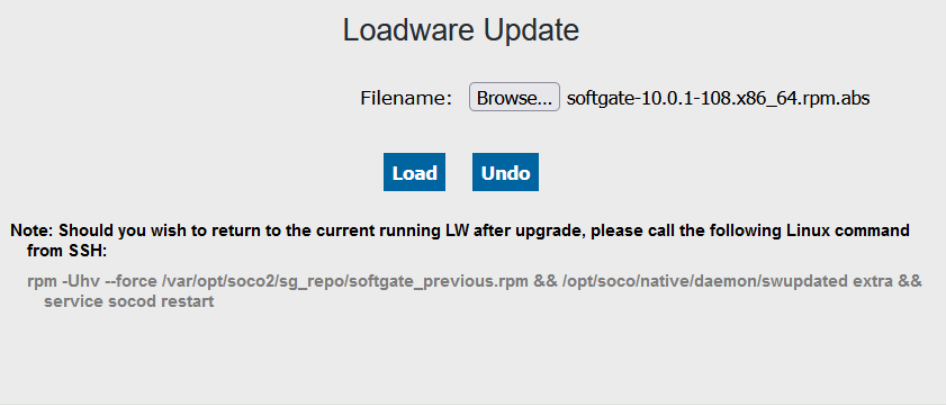


- Wählen Sie nun die gewünschte Baugruppe aus und klicken Sie auf den Link **WBM**. Es öffnet sich nun das HG 35xx WBM.
- Wählen Sie nun **Wartung > Software-Image > Laden zum Gateway**.
- Wählen Sie **Laden über http** aus.



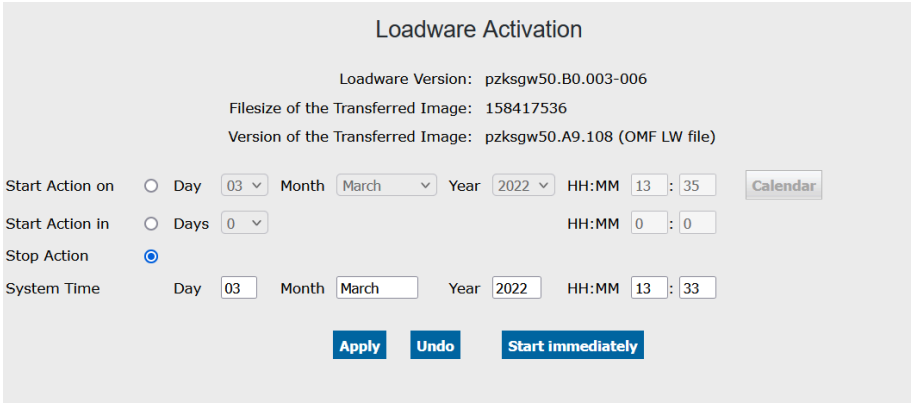
- Im Feld **Remote-Dateiname (PC-Dateisystem)** müssen Sie die zuvor auf Ihrem PC gespeicherte Software (Loadware) eintragen. Dies erfolgt über die Schaltfläche **Durchsuchen**.
- Wählen Sie nun die Schaltfläche **Laden**, um den Ladevorgang zu starten. Der Ladevorgang kann bis zu 5 Minuten dauern. Die Loadware wird im Flashspeicher der Baugruppe abgespeichert.

Wichtig: Während des Ladevorganges muss das LAN vorhanden sein und die IP-Gateways dürfen nicht rebootet (AMO USSU, AMO BSSU) werden!



- Aktivieren (entpacken und installieren) der Loadware
- Der Aktivierungsvorgang (Loadware entpacken und installieren) benötigt nun weniger als 5 Minuten.

  Sie können die Software (Loadware) **Sofort aktivieren** oder über die Schaltfläche **Termin festlegen** an einem bestimmten Tag zeitgesteuert aktivieren.



2.5.5 Update der Loadware mit Hilfe des „LW Update Manager“

Wichtig: Vorteil Es können mehrere IP-Gateway-Baugruppen auf einmal hochgerüstet werden!

Die wichtigsten Funktionen des „LW Update Managers“

- Mit der Funktion „LW Update Manager“ können einzelne Baugruppen oder alle unterstützten Baugruppen aktualisiert werden.
- Der LW-Update besteht aus zwei Teilen: Loadware-Transfer und Loadware-Aktivierung.
- Die Aktualisierung der Loadware kann unmittelbar, also sofort, oder zeitgesteuert, also mit dem Zeitplaner/Scheduler, durchgeführt werden.

Aufruf des „LW Update Managers“

Melden Sie sich hierfür am OpenScape 4000 Assistant an und wählen Sie **Expertenmodus > LW Update Manager**.

Mehr Informationen finden Sie in der Online-Hilfe des „LW Update Managers“ oder im Intranet „OpenScape 4000 Assistant V, Loadware Update Manager, Administratordokumentation“ (http://apps.g-dms.com:8081/techdoc/de/P31003H3440M1450176A9/index.htm).

2.5.6 Allgemeine Hinweise zum Ladevorgang

Ladegeschwindigkeit

Die Zeit zum Laden einer CGW-STMI-Baugruppe beträgt ungefähr 8.5 Minuten (ohne andere Restore-Zeiten mit einzuberechnen). Wenn es sich um einen Access Point mit einer langsamen IP-Verbindung handelt, verringert sich die Geschwindigkeit um den entsprechenden Faktor (siehe auch „Flusssteuerung (TCP)“).

Flusssteuerung (TCP)

Es gibt eine Flusssteuerung. Wenn die benötigte Bandbreite (Quality of Service) nicht zur Verfügung steht, kommt es zur Verlangsamung des Prozesses, d.h. auch dass der langsamste Access Point die Ladegeschwindigkeit für alle gleichzeitg zu ladenden Access Points bestimmt.

2.6 Konfigurationsdaten im lokalen Flash speichern (local Backup & Restore)

2.6.1 Überblick

Es gibt Kundenszenarien in denen die Gateway-Baugruppen und der OpenScape 4000 Assistant in verschiedenen IP-Netzwerken sind (kein Routing zwischen diesen beiden Netzwerken). Damit ist die Backup- und Restore-Funktionalität des OpenScape 4000 Assistant nicht möglich. In diesen Fällen können die WBM-Konfigurationsdaten/Zertifikate im lokalen Flash der Baugruppe gespeichert werden. Dann ist eine Sicherung und Wiederherstellung immer noch möglich, wenn die Verbindung zum Backup-Server des OpenScape 4000 Assistant fehlt oder der Backup-Server nicht erreichbar ist.

2.6.2 Leistungsmerkmalbeschreibung

Wenn „Konfigurationsdaten im lokalen Flash speichern“ aktiviert ist, wird zur eingestellten Tageszeit (Standard 03:00 Uhr) eine Sicherungsdatei auf dem lokalen Flash erstellt.

Wenn „Konfigurationsdaten im lokalen Flash speichern“ aktiviert wurde, dann wird jedesmal, wenn im WBM die Daten gespeichert wurden, eine Backup-Datei im lokalen Flash angelegt. Somit verliert man beim Loadware-Update über HDLC praktisch keine Daten mehr.

Diese Backup-Datei wird nur im Falle eines Loadware-Upgrades, der per HDLC (bei einer STMI) bzw. FTP (bei einer NCUI) erfolgt, verwendet. Wird ein solcher Upgrade angestoßen, dann wird beim Starten der neuen Loadware-Version (noch im Hochlauf - vor Gateway-Status „System-Ready“) der Restore

mit der vorhandenen Backup-Datei durchgeführt. Anschließend wird geprüft ob der OpenScape 4000 Assistant „Backup und Restore“ erreichbar ist und eventuell ein aktuelleres Backup vorliegt. Dies ist der Fall, wenn zwischen 3:00 Uhr und dem aktuellen Zeitpunkt ein manuelles/oder automatisches Backup der Baugruppe angelegt wurde. Wenn auf dem OpenScape 4000 Assistant „Backup und Restore“ Server ein aktuelleres Backup liegt und der Backup-Server erreichbar ist, dann wird dieser zweite Restore gemacht.

Wenn der Loadware-Upgrade über den Loadware-Manager des Assistant gemacht wird, dann wird die Backup-Datei im lokalen Flash (03:00Uhr) nicht benutzt. In diesem Fall wird noch vor der Aktivierung der neuen SW-Version mit der alten Load ein aktuelles Backup im lokalen Flash angelegt. Anschließend wird die neue Loadware-Version geladen und gestartet. Noch im Hochlauf wird das kurz vorher angelegte Backup importiert. Somit ist hier sichergestellt, dass dieser Upgrade mit lokalen Backup/Restore immer die aktuellsten Konfigurationsdaten beinhaltet. Der OpenScape 4000 Assistant „Backup und Restore“ muss trotzdem kontakiert wird, um die Backup-Datei zu prüfen. Dies ist wichtig im Falle von HFA-Standby: Hier wird es ein Backup auf dem OpenScape 4000 Assistant „Backup und Restore“ mit gleicher IP-Adresse aber alter MAC-Adresse geben, dass dann importiert werden muss.

Hinweise zum Reboot

- Erfolgt der Backup vom OpenScape 4000 Assistant „Backup und Restore“ noch vor dem Status „System-Ready“ der Baugruppe, dann ist kein zusätzlicher Reboot dabei. Erfolgt der Restore nach „System-Ready“, weil z. B. der OpenScape 4000 Assistant „Backup und Restore“ nicht gleich erreichbar ist, dann wird im Falle von SPE (wegen Zertifikaten bzw. MEK) ein automatischer Reboot der Baugruppe durchgeführt.
- Der Restore des lokalen Backups erfolgt während der Hochlaufphase (bevor die Baugruppe in Betrieb genommen wird) und daher ist nur in Ausnahmefällen (z. B. SPE-Zertifikate vorhanden) ein zusätzlicher automatischer Gateway-Reboot notwendig.
- Sollte zusätzlich auch ein OpenScape 4000 Assistant „Backup und Restore“-Server konfiguriert/vorhanden sein, so entscheidet letztendlich die Aktualität des Backups über die Übernahme in die Boarddaten, d. h. Restore vom local Backup oder vom OpenScape 4000 Assistant „Backup und Restore“ Backup. Sollte der OpenScape 4000 Assistant „Backup und Restore“ Backup aktueller sein, so kann dies unter Umständen zu einem zusätzlichen Reboot führen.

2.6.3 Hochlauf-Szenarien

Normaler Restart

Überprüfen Sie, ob der Backup-Server konfiguriert und erreichbar ist.

- Der Backup-Server ist **konfiguriert**, **erreichbar** und der Backup der Konfigurationsdaten hat eine **neuere Version** als der Backup, der sich im lokalen Flash befindet:
- -> Konfigurationsdaten werden vom Backup-Server geladen. Das ist der normale Fall, wenn über HDLC hochgerüstet wird oder dei baugruppen ausgetausct wurden.
- Der Backup-Server ist **konfiguriert** und **erreichbar**, aber es ist **kein Backup** mit Konfigurationsdaten gespeichertut bzw. es wird keiner gefunden:

- Das Gateway läuft mit seinen Standard-Konfigurationsdaten hoch. Es wird kein erneuter Versuch unternommen den Backup-Server zu erreichen.
- Der Backup-Server ist **konfiguriert** aber **ist nicht erreichbar**:
- Es wird ein erneuter Versuch unternommen den Backup-Server zu erreichen.
- Der Backup-Server ist **nicht konfiguriert**.
- Das Gateway läuft mit seinen Standard-Konfigurationsdaten hoch. Es wird kein erneuter Versuch unternommen den Backup-Server zu erreichen.

  Loadware-Update über HDLC

  Gleiche Vorgehensweise wie beim normalen Neustart. Beim Upgrade über HDLC kann die Baugruppe die aktuellen Konfigurationsdaten nicht im lokalen Flash (TFFS) gespeichert haben.

  Konfigurationsdaten gehen bei einem Loadware-Update über HDLC nicht mehr verloren, da beim Speichern von Daten im WBM eine Backup-Datei auf dem lokalen Flash erstellt wird.

  Loadware-Update über OpenScape 4000 Assistant / WBM

  Nach der Aktivierung der neuen Loadware wird automatisch ein Reboot der Baugruppe durchgeführt. Die neue Gateway-Loadware wird geladen. Das neue Loadware-Image lädt die zuvor gespeicherten Konfigurationsdaten. Die Daten auf dem Backup-Server können nicht neuer sein, deshalb werden sie nicht in Betracht gezogen.

  Mehr Informationen zum Loadware-Update über OpenScape 4000 Assistant / WBM finden Sie im Kapitel 5, „Ladekonzept der Gateway-Baugruppen“.

  Loadware-Update über OpenScape 4000 Assistant / WBM: Backup-Server nicht konfiguriert

  Wie „Loadware-Update über OpenScape 4000 Assistant / WBM“.

  Loadware-Update über OpenScape 4000 Assistant / WBM: Backup-Server konfiguriert aber nicth erreichbar (über IP)

  Wie „Loadware-Update über OpenScape 4000 Assistant / WBM“.

  Loadware-Update über OpenScape 4000 Assistant / WBM: Backup-Server konfiguriert und erreichbar, aber es ist kein Backup mit Konfigurationsdaten gespeichertut bzw. es wird keiner gefunden

  Wie „Loadware-Update über OpenScape 4000 Assistant / WBM“.

  Loadware-Update über OpenScape 4000 Assistant / WBM: Backup-Server konfiguriert und erreichbar, aber auf dem Backup-Server wird eine ältere Version gefunden als die aktuelle

  Wie „Loadware-Update über OpenScape 4000 Assistant / WBM“.

2.6.4 Konfiguration

Das Leistungsmerkmal wird mit Hilfe des WBM der Baugruppe eingerichtet.

WBM > Wartung > Aktionen > Automatische Aktionen > Konfigurationsdateien im lokalen Flash speichern

2.6.5 Besonderheiten

- Baugruppentausch
- Die Ersatz-Baugruppe hat bereits einen Backup im lokalen Flash gesichert (allerdings mit einer anderen Funktionalität als die zu tauschende Baugruppe).

  Nachdem es einen Backup im lokalen Flash gibt, wird dieser auch für den Restore der Daten verwendet. Aber durch den Tausch hat sich die MAC-Adresse der Baugruppe geändert. Dadurch wird der Backup und Restore kontaktiert um einen Restore über den Backup-Server durchzuführen. Nachdem Restore durch den Backup-Server sind wieder die korrekten Daten on der Baugruppe vorhanden. Es muss aber dafür gesorgt werden, dass der Backup-Server erreicht werden kann, sonst hat die Baugruppe die verkehrten Konfigurationsdaten geladen.

  Nachdem Restore sollte der Backup im lokalen Flash der Baugruppe mit den korrekten Konfigurationsdaten aktualisiert werden.
- Default-Konfiguration (leere Datenbasis)
- Eine leere Datenbasis kann wie folgt erzeugt werden:

  WBM > Wartung > Konfiguration & Update > Konfiguration > SSL-Daten > Konfiguration auf Werkseinstellung zurücksetzen ...

  Bei Auswahl dieser Option wird die Baugruppe automatisch zurückgesetzt. Während der Inbetriebnahme der Baugruppe werden die über AMO konfigurierten Parameter geladen. Die WBM-Parameter werden auf ihre Default-Werte zurückgesetzt.

2.7 Nachladbarkeit des FPGA auf der STMI4-/NCUI4- Baugruppe

Der FPGA-Code kann auf die Gateway-Baugruppen STMI4 und NCUI4 nachzuladen.

In der Regel wird der FPGA-Code mit einem LW-Hotfix (oder über Fix Release, Minor Release, Hotfix) ausgeliefert. Es gibt drei Dateien:

- Die SENTA-Datei,
- die COMGA-Datei für STMI4 und
- die COMGA-Datei für NCUI4.

Wichtig: Die Aktualisierung der SENTA-/COMGA-Firmware (FPGA-Code) kann nicht remote erfolgen!

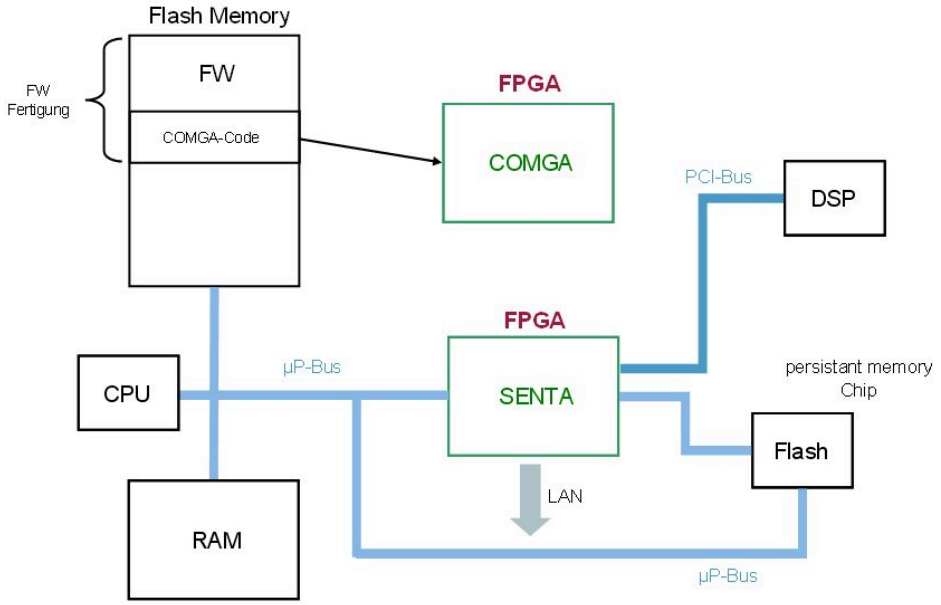


Abbildung 15: FPGA - beteiligte Hardwarekomponenten

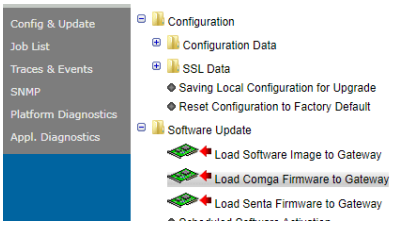
Voraussetzung:

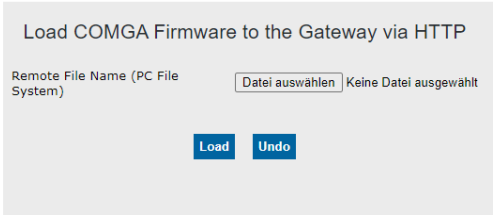
Die Loadware für SENTA /COMGA muss per PCHI-Tool / ftp-Transfer (**binär**) auf einen PC gespeichert werden. Bevor der Update durchgeführt werden kann, muss die Loadware auf einen PC übertragen werden, der sich im Kundennetz befindet und Zugang zum WBM der Baugruppen hat (WBM-Client).

Aktualisierung:

Die Aktualisierung der SENTA- und der COMGA-Loadware erfolgt über WBM. Der Bereich **Maintenance > Config and Update > Software Update** bietet zwei Möglichkeiten:

- **Load COMGA-Firmware via HTTP** (COMGA-Firmware über HTTP hochladen) oder
- **Load SENTA-Firmware via HTTP** (SENTA-Firmware über HTTP hochladen).

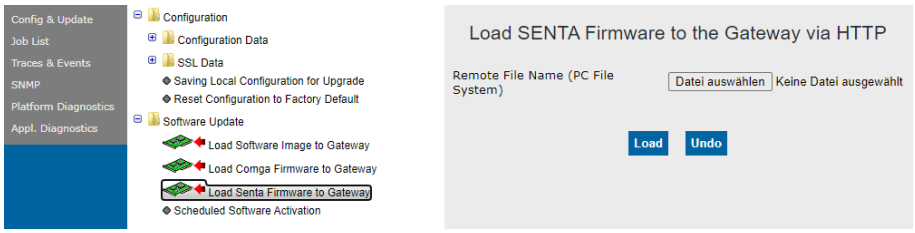




Wichtig: Die folgende Beschreibung der Firmware-Aktualisierung bezieht sich auf die SENTA-Loadware. Für die COMGA-Firmware gilt dieselbe Anleitung, außer dass Sie im Menü **Load COMGA-Firmware via HTTP** (COMGA-Firmware über HTTP hochladen) auswählen.

1) Wählen Sie im Menü die Option **Load SENTA-Firmware via HTTP** (SENTA-Firmware über HTTP hochladen).

2) Wählen Sie die Datei mit der neuen SENTA-Loadware auf Ihrem lokalen PC aus, indem Sie auf die Schaltfläche **Browse** (Durchsuchen) klicken.



3) Klicken Sie auf die Schaltfläche **Load** (Hochladen), um die Loadware in den Flash-Speicher der Baugruppe zu laden.

4) Der Hochladevorgang ist beendet, wenn der folgende Bildschirm angezeigt wird.

   Bestätigen Sie mit **OK**.

5) Aktivieren Sie die neue SENTA-Firmware, indem Sie auf die Schaltfläche **Activate now** (Jetzt aktivieren) klicken.

Wichtig: Sobald der Aktivierungsvorgang abgeschlossen ist, wird das Gateway automatisch neu gestartet.

---

6) Klicken Sie auf **OK**, um den Aktivierungsvorgang zu bestätigen.

   Die neue SENTA-Firmware wird aktualisiert und aktiviert, und das Gateway wird neu gestartet.

Trace:

Der gesamte Vorgang kann mit aktiviertem Trace SWCONF, Ebene 9, überwacht werden.

Herunterladen der SENTA-Firmware

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.688177"
 cswconfigsvc03.cpp 175)
Creating Job! Type=0x1f001b, ID=3
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.701594"
 cswconfigsvc03.cpp 377)
Created Job 3
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.702931"
 cswconfjob02.cpp 3357)
Firmware type: SENTA
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.759732"
 cswconfjob02.cpp 3419)
First block. Retrieving image header.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.760800"
 cswconfjob02.cpp 3429)
 offset |  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
 |
--------+------------------------------------------------
+-----------------
00000000| B2 00 00 00 04 30 37 2F  31 30 2F 30 38 31 33 3A
 | .....07/10/0813:
00000010| 30 36 3A 35 34 17 45 4C  46 3E 49 33 38 36 50 5A
 | 06:54.ELF>I386PZ
00000020| 4B 53 45 4E 30 31 2E 4F  31 2E 30 31 32 00 00 00
 | KSEN01.O1.012...
```

```
00000030| 00 00 30 00 99 78 70 7A  6B 73 65 6E 30 31 00 00
 | ..0..xpzksen01..
00000040| 00 00 00 00 00 00 00 00  00 00 00 00 68 00 00 00
 | ............h...
00000050| 00 00 00 00 50 D9 10 00  00 00 00 00 00 00 00 00
 | ....P...........
00000060| 00 00 00 00 00 00 00 00
 | ........
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:43.761791"
 cswconfjob02.cpp 3652)
Transfer status for job 3 is 1% (11540/1092718)
(SWCONF tBackupTask 0x30622e8 "08/25/2008 15:43:43.774272"
 cswconfigsvc01.cpp 43
9)
Execute Job in Queue:
    ID = 3, Action=0x1f001b
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.120524"
 cswconfjob02.cpp 3652)
Transfer status for job 3 is 47% (515348/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.497264"
 cswconfjob02.cpp 3652)
Transfer status for job 3 is 93% (1019156/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:44.590766"
 cswconfjob02.cpp 3522)
Writing block of 1104096 bytes, remaining 1 bytes
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.465757"
 cswconfjob02.cpp 3532)
Writing block finished OK.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.467342"
 cswconfjob02.cpp 3652)
Transfer status for job 3 is 101% (1104209/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474411"
 cswconfjob02.cpp 3543)
Got last part of the buffer
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.474737"
 cswconfjob02.cpp 3552)
Writing remaining buffer: 0 bytes
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.480742"
 cswconfjob02.cpp 3614)
 offset |  0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
 |
--------+-------------------------------------------------
+-----------------
00000000| 70 7A 6B 73 65 6E 30 31  17 45 4C 46 3E 49 33 38
 | pzksen01.ELF>I38
00000010| 36 50 5A 4B 53 45 4E 30  31 2E 4F 31 2E 30 31 32
 | 6PZKSEN01.O1.012
00000020| 00 00 00 00 00 30 00 00  00 99 78 30 37 2F 31 30
 | .....0....x07/10
00000030| 2F 30 38 20 20 31 33 3A  30 36 3A 35 34
 | /08  13:06:54
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481125"
 cswconfjob02.cpp 3641)
Writing loadware ID finished OK.
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.481718"
 cswconfjob02.cpp 3652)
```

```
Transfer status for job 3 is 101% (1104209/1092718)
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:50.492219"
 cswconfigsvc02.cpp 1010)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:51.596658"
cswconfigsvc02.cpp 1010)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:55.651796"
 cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:43:57.721041"
 cswconfigsvc02.cpp 845)
Progress Response:
    Transferred File Size=1104209
    Complete File Size=1092718
The second phase of the process:
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:22.147227"
 cswconfjob07.cpp 422)
File info: compressed size: 1104096, uncompressed size:
 12491489
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.146807"
 cswconfjob07.cpp 446)
Uncompression successful
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:23.147303"
 util.c 4765)
... writing SENTA FPGA code to SENTA flash
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:33.140242"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:43.140240"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:44:53.140241"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:03.140241"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:13.140241"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:23.140242"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:33.140478"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:43.140469"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
```

```
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:45:53.140444"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:03.140352"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:13.140249"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:23.140241"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:33.140242"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:43.140244"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:46:53.140248"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:03.140247"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:13.140245"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:23.140242"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:33.140246"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:43.140245"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:47:53.140244"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:03.140245"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:13.140245"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:23.140245"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:33.140242"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:43.140240"
 util.c 4769)
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140243"
 util.c 4769)
```

```
writting SENTA FPGA code to SENTA flash is still running
(SWCONF tEmWeb 0x353c4c0 "08/25/2008 15:48:53.140552"
 util.c 4771)
programming SENTA flash finished
.....
(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.050407"
 util.c 3928)
active SENTA version on revision 1: 12
(SWCONF tEmWeb 0x440e168 "08/29/2008 10:43:37.056302"
 cswconfjob07.cpp 539)
!!! Initializing reboot !!!
(EVTLOG tEvtLogTask 0x36de430 "08/29/2008 10:43:37.058440"
 cevtlogsvc01.cpp 942)
EventLogEntry from SYSTEM (tEmWeb "08/29/2008
 10:43:37.056510" cswconfjob07.cpp
544):
  EventType: Information
  EventCode: MSG_ADMIN_REBOOT
  EventText: Reboot initiated by Admin (Firmware
 Activation)
Executing Shutdown and Reboot for EvtCode 100
 (MSG_ADMIN_REBOOT)
Exiting Security Task*** Shutdown.
Fehler:
Im Falle eines Fehlers wird im WBM ein Fenster mit einem
 Fehlercode eingeblen►
det.
(SWCONF tFPGAWrite 0x4e39e88 "08/28/2008 15:06:53.579613"
 util.c 3666)
call of xsvfExecute returned error:2
Die Loadware wird nicht aktiviert, und es erfolgt kein
 Neustart des Gateways.
```

2.8 Standby Board HG 3500

Die Funktion „Standby Board HG 3500“ wird für alle gängigen Gateway-Karten unterstützt. Ungeachtet ob sie im Single-Feature-Mode oder im Multiple-Feature-Support (MFS) konfiguriert sind.

Wichtig: Einschränkung Im Fall von MFS kann nur die gesamte Baugruppe auf die Standby-Baugruppe übertragen werden!

2.8.1 Leistungsmerkmalbeschreibung

Dieses Leistungsmerkmal wurde entwickelt, um die Verfügbarkeit von IP-Terminals (HFA/SIP), IP-Kanalleitungen (HG3550) und IPDA-Funktionskarten (HG3570) im Falle eines Kartenausfalls oder LAN-Kabeldefekts zu erhöhen. Alle diese Leistungsmerkmale werden für die Standby-Board-Funktion unterstützt, entweder im Single-Feature-Modus oder mit Multi-Feature-Unterstützung (MFS). Grundsätzlich übernimmt das Standby Board im Fehlerfall alle konfigurierten Features von der Normal-Karte.

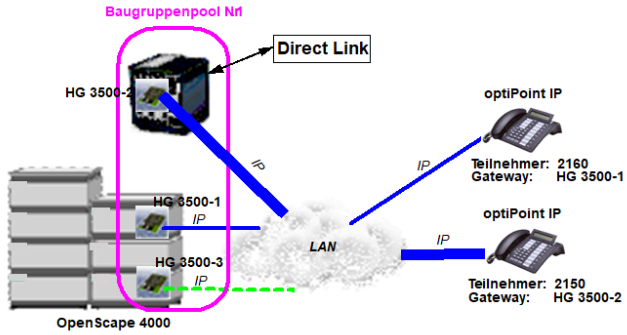


Abbildung 16: HFA Infrastruktur

Anmerkung: Die Verwendung des „Standby-Board HG3500“-Leistungsmerkmals zwischen STMI2/4-Boards und STMIX-Boards ist nur eingeschränkt kompatibel. Wird das StandBy Feature (ein BPOOL) zwischen STMI2/4 <-> STMIX verwendet und werden Konfigurationsdaten wie SIP-Profileinstellungen, SPE-Zertifikate, etc. auf der z. B. STMI2/4-Karte gespeichert, können diese nicht in den STMIX ausgetauscht werden (und umgekehrt). In der Regel verwendet das Standby Feature den Assistenten HBR HG3500M Backup & Restore Mechanismus (Backup-Sets), um die Daten im Fehlerfall auf das Standby Board zu verteilen. Da die Backup-Sets zwischen STMI2/4 und STMIX nicht kompatibel sind, betrifft dies die Standby-Funktion für diese Daten. Hintergrundinformationen: StandBy Board überprüft, empfängt und importiert das Assistant HBR-Set bei der Inbetriebnahme, falls es in CGGWB konfiguriert ist und ein vorhandenes Backup-Set verfügbar ist. Wenn Sie gemischte Gateways (STMI2/4 mit STMIX) verwenden wollen und Sie den Assistenten HBR für Daten verwenden, die nicht im AMO gespeichert sind (z.B. Trunk-Profile, SPE cert, etc.), müssen Sie eine manuelle WBM-Konfigurationssynchronisierung durchführen, um die Konsistenz der Konfiguration zu gewährleisten. Optimale Lösung: Verwenden Sie einen BPOOL, der nur aus STMI2/4-Boards besteht, und einen weiteren BPOOL, der nur aus STMIX-Boards besteht.

Dies geschieht durch die Einführung von Reserve-Baugruppen, den sogenannten „Standby Boards“. Diese Standby Boards können im Fall eines Baugruppen- oder LAN-Kabel-Defekts einer in Betrieb befindlichen Baugruppe deren IP-Teilnehmer, IP-Trunking-Strecken usw. übernehmen. Dies geschieht, falls es entsprechend vorkonfiguriert wurde, automatisch, d.h. ohne manuellen Eingriff und ohne AMO-Aufruf. Dies wird im folgenden am Beispiel eines Common Gateways mit HFA-Teilnehmern beschrieben.

Im Beispiel in Bild 17HFA Infrastruktur ist die Reserve-Baugruppe die HG 3500-3. Wird beispielsweise HG 3500-1 defekt, wird das IP Phone 2160 auf HG 3500-3 umkonfiguriert und geht mit der neuen Baugruppe in Betrieb.

Dieses automatische Umschalten erfolgt, falls das Leistungsmerkmal vorkonfiguriert wurde (siehe unten) bei folgenden Ereignissen:

- Ziehen der Baugruppe ohne vorherige Außerbetriebnahme

- Fehler auf dem LAN Anschlusskabel. Hier ist zu beachten, dass LAN Fehler, die „hinter“ Routern, Hubs oder IP-Switches lokalisiert sind, ebenso wie IP Endgeräte-Fehler nicht zu einem Umschalten führen. Nur ein signalisierter Layer 1 Fehler, d.h. im allgemeinen ein Kabelfehler initiiert den Umschaltemechanismus.
- Fehler, die von der Sicherheitstechnik erkannt werden und die zum DC-Zustand „DEF“ der Baugruppe führen, z.B. „Message not transmittable“. Ausnahme: Ein Statistiküberlauf führt nicht zu einem Umschalten.

Das automatische Umschalten wird nicht ausgelöst, falls entweder die Baugruppe oder die übergeordnete Hierarchie (LTU, LTG) betriebstechnisch gesperrt sind.

Die IP Endgeräte gehen während des Umschaltevorgangs außer Betrieb und werden nach erfolgreichem Umschalten automatisch wieder in Betrieb genommen. Die Dauer des Umschaltevorgangs wird von der Ladezeit der Baugruppendaten und von Timern auf der Baugruppe und im Endgerät bestimmt. Sie beträgt im allgemeinen ein bis zwei Minuten.

Dabei ist anzumerken, dass die Baugruppe beim Hochlauf nach dem Umschalten einen sog. „gratuitous ARP“ -Request (Gratis-Address Resolution Protocol) ins LAN sendet, damit die zur IP-Adresse gehörende MAC-Adresse (diese hat sich ja mit der Baugruppe geändert) sofort und nicht erst nach Ablauf des Aging Timers bei den LAN-Komponenten aktualisiert wird. Hier muss auf der LAN-Seite beachtet werden, dass der ARP-Request in evt. involvierten Routern nicht abgeblockt wird.

Das automatische Umschalten wird am Service-Terminal signalisiert. SYSDEP-NMC erhält ebenfalls eine Meldung, dass umgeschaltet wurde. Dafür ist der neue NMC Alarm 36 (PER-BOARD SWITCHOVER) eingeführt worden. Die Meldung am Service-Terminal sieht folgendermaßen aus:

```
F5880 M4 N0542 NO ACT   BPA   BOARD    RECONFIGURATION
    06-11-09 10:13:30
      ALARM CLASS:CENTRAL:036
        P101 :LTG1 :LTU3 :055:  0-239:90 Q2316-X10  STMI2/1
    BST:01  PLS:-06
      FORMAT:43
      REASON:00H  BOARD RECONFIGURATION OK
      SOURCE BOARD      : P117:LTG1 :LTU17:097:
      DESTINATION BOARD : P101:LTG1 :LTU3 :055:
```

Wird die defekte Baugruppe, an der die IP Teilnehmer ursprünglich konfiguriert waren, vom Servicepersonal durch eine intakte Baugruppe ersetzt, so können die IP Teilnehmer wieder bei der manuellen Inbetriebnahme zurückkonfiguriert werden. Dann wird aus der zwischenzeitlich benutzten Baugruppe wieder eine Reserve-Baugruppe, die bei künftigen Defekten die Teilnehmer übernehmen kann.

Neben der automatischen Umschaltung der IP Teilnehmer auf eine Reserve-Baugruppe im Falle eines Defekts, umfasst dieses Leistungsmerkmal auch die manuelle Umschaltemöglichkeiten, die mittels AMO BSSU ausgeführt werden kann. Dabei können die IP Teilnehmer in ihren Gruppenbeziehungen verbleiben, das bedeutet, es ist keine Teilnehmer-Umkonfiguration mittels AMO SBCSU, AMO AUN etc. notwendig.

Damit das Leistungsmerkmal funktionieren kann, muss es vorkonfiguriert werden. Dazu müssen folgende Schritte beachtet werden (AMO Details siehe Abschnitt 8.4, „Generierung“):

- Common Gateway-Baugruppen einrichten: Sowohl die normalen Baugruppen (d.h. an der die IP Teilnehmer konfiguriert werden) als auch die Reserve-Baugruppen werden wie bisher mit dem AMO BFDAT und AMO BCSU eingerichtet. Es wird hier noch nicht zwischen den beiden Funktionalitäten unterschieden.
- Common Gateway-Baugruppendaten einrichten: Hier werden normalerweise mit dem AMO CGWB die Common Gateway-Baugruppen parametrisiert. Hier erfolgt die Unterscheidung, ob die Baugruppe (als normale Baugruppe) mit IP Teilnehmern oder als Reserve-Baugruppe vorgesehen ist. Die normalen Baugruppen müssen mit einer IP-Adresse versorgt werden (wie bisher), die „Standby Boards“ werden ohne IP-Adresse und ohne weitere Parameter versorgt.
- Alle Common Gateway-Baugruppen, die das Leistungsmerkmal nutzen wollen, müssen in einem Baugruppen-Pool mittels AMO BPOOL zusammengefasst werden. Ein Baugruppen-Pool wird über eine Pool-Nummer verwaltet und muss sowohl die normalen Baugruppen als auch die Reserve-Baugruppen enthalten. Nur dann kann im Falle eines Defekts von einer normalen auf eine Reserve-Baugruppe umgeschaltet werden. Dabei ist zu beachten, dass eine automatische Umschaltung bei Defekt nur von einer Baugruppe im Pool zu einer Reserve-Baugruppe in demselben Pool erfolgen kann. Eine manuelle Umschaltung per AMO ist auch pool-übergreifend möglich, beide beteiligten Baugruppen müssen jedoch (irgendeinem) Pool angehören.
- Die IP Teilnehmer werden wie bisher an den normalen Baugruppen mit dem AMO SBCSU konfiguriert und in Betrieb genommen. An einer Reserve-Baugruppe können keine Teilnehmer konfiguriert werden.

Neben der oben beschriebenen Funktionalität unfasst das Leistungsmerkmal ausserdem:

- Pool-individuelle Einstellung von folgenden Attributen:
  - SINGLE / MULTI

    Damit kann man einstellen, ob ein automatisches Umschalten einmalig (SINGLE) oder mehrmalig, z.B. bei weiteren Defekten erfolgen soll.

    - **SINGLE** Ist einmaliges automatisches Umschalten konfiguriert, führen weitere Defekte nicht zu einem Weiterschalten, auch wenn noch Reserve-Baugruppen im Pool verfügbar sind. Diese Einstellung ermöglicht beim manuellen Zurückschalten nach dem Ersetzen der defekten Baugruppe, dass die Teilnehmer zurückgeschaltet werden ohne Angabe, wo sich die Teilnehmer aktuell befinden.
    - **MULTI** Ist mehrmaliges automatisches Umschalten konfiguriert, führen Defekte solange zum Weiterschalten, bis keine Reserve-Baugruppe aus dem Pool mehr zur Verfügung steht. Beim manuellen Zurückschalten müssen Sie angeben, von welchen Karten und auf welche die Stationen geschaltet werden sollen. Mit anderen Worten, Sie müssen das Quellboard und das Zielboard kennen oder herausfinden.
  - Info

    Dies dient lediglich dazu, die Übersichtlichkeit bei mehreren Pools zu verbessern. Hier kann ein Name einem Pool zugeordnet werden.

- Pool-History verfolgen

  Für jede Baugruppe im Pool gibt es ein History-Feld. Hier können folgende Informationen mit dem AMO BPOOL eingegeben und ausgelesen werden:

  – Baugruppe (LTU, Einbauteilung), von der die aktuell konfigurierten Teilnehmer hergeschaltet wurden
  – Baugruppe (LTU, Einbauteilung), wohin die ehemals konfigurierten Teilnehmer geschaltet wurden
  – Datum und Zeit der Her- bzw. Weg-Schaltung der IP Teilnehmer
  – Zähler, wie oft die aktuell konfigurierten Teilnehmer bereits umgeschaltet wurden

    Diese Informationen gibt es getrennt für das automatische Umschalten (nach Defekt) und für das manuelle Umschalten. Mit dem AMO BPOOL können die History Daten rückgesetzt werden, jedoch nur alle Daten gemeinsam.

    Die History protokolliert nur das jeweils letzte Umschalten. Lediglich die Zähler werden über alle Umschalte-Stufen gepflegt.

Wichtig: Damit das automatische Umschalten der IP Teilnehmer wirksam wird, müssen die Baugruppen zum Zeitpunkt des Defekts in Betrieb gewesen sein (DC-Zustand „Ready“). Die Funktion wird nicht implementiert, wenn bei der Inbetriebnahme der Karte oder des Systems ein Fehler festgestellt wird; in diesem Fall wird ein automatischer Neustart durchgeführt. Dies ist aus Gründen der Systemstabilität notwendig. **Ausnahme**: Ein abgetrenntes LAN-Kabel führt zu einem erfolgreichen Start; die spätere Erkennung des LAN-Kabelausfalls aktiviert die automatische Umschaltung, solange eine Karte vorhanden ist.

2.8.2 Benutzeroberfläche

Keine besonderen Konsequenzen für die Telefonbenutzer. Während der Umschaltephase ist das Telefon „tot“; die Anzeige ist gelöscht und erscheint wieder, sobald das Telefon an der neuen Baugruppe betriebsbereit ist. Vor diesem Zeitpunkt können auf dem Display noch temporär weitere Meldungen erscheinen (z.B. PBX NOT FOUND).

2.8.3 Serviceinformationen

Das Umschalten der IP Teilnehmer ist wie eine Umkonfiguration zu sehen. Dies bedeutet, dass die Umkonfiguration nach einem Reload der Anlage nicht mehr wirksam ist, es sei denn es wurden die statischen Daten mit EXEC-UPDAT:BP,ALL; auf die Hard Disk geschrieben.

Wichtig: Erfolgt nach einem Umschalten der IP Teilnehmer auf eine Reserve-Baugruppe ein Anlagen-Reload bevor die Datenbasis mit dem AMO UPDAT auf die HD gesichert wurde, sind die IP Teilnehmer nach dem Reload wieder an ihrer

alten Baugruppe konfiguriert. Ist diese alte Baugruppe immer noch defekt oder gezogen, erfolgt kein Umschalten, da die Bedingung, dass die Baugruppe vor dem Defekt in Betrieb gewesen sein mußte, nicht erfüllt ist (Ausnahme: ein defektes LAN-Kabel kann erst erkannt werden, wenn die Baugruppe in Betrieb ist. In diesem Fall wird erfolgt ein Umschalten).

Im Rahmen dieses Leistungsmerkmals wurde im AMO CGWB die Typverzweigung nach **SMODE** eingeführt. **SMODE** bezeichnet den Standby Mode einer Common Gateway-Baugruppe. Der Standby Mode legt fest, ob eine Baugruppe als normale Baugruppe mit IP Teilnehmern, IP Adresse etc. konfiguriert ist, oder ob es sich um eine Reserve-Baugruppe (Standby Board) handelt.

Ein Standby Mode kann zwei Ausprägungen haben:

STBYRDY: Bedeutet „Standby Ready“ und bezeichnet eine Reserve-Baugruppe, die bereit ist, Teilnehmer zu übernehmen. Üblicherweise ist eine solche Baugruppe im DC-Zustand „Ready“, da die Baugruppe den Standby Mode auswertet und bei STBYRDY eine positive Ladequittung ans System sendet. Der LAN-Status kann „Ready“ oder „DEF“ sein. Um als Reserve-Baugruppe zu dienen, muss sowohl der DC-Status der Baugruppe, als auch der LAN-Status „Ready“ sein.

STBYDEF: Bedeutet „Standby Defect“ und bezeichnet eine Baugruppe, von der wegen eines Defekts die IP Teilnehmer weggeschaltet wurden. Solch eine Baugruppe kann nicht als Reserve-Baugruppe dienen, da deren DC Zielzustand „DEF“ ist. Üblicherweise Ist eine solche Baugruppe im DC-Zustand „DEF“ bzw. „NL“, falls die Baugruppe gesteckt ist oder „NPR“, falls die Baugruppe gezogen ist. Die LW, die den Standby Mode auswertet sendet bei STBYDEF eine negative Ladequittung ans System (DEF ON REQUEST).

Baugruppen, die sich in einem Standby Mode befinden, haben weder eine eigene IP Adresse, noch irgendwelche Baugruppendaten. Erst beim Umschalten der IP Engeräte auf eine solche Baugruppe werden alle Baugruppendaten von der (defekt gewordenen) Ursprungsbaugruppe komplett übernommen, also inklusive der IP Adresse. Die Ursprungsbaugruppe wird nach dem Umschalten zu einer Standby Baugruppe (z.B. STBYDEF), hat also keine IP Adresse mehr. Physikalisch ist eine Standby Baugruppe jedoch an das LAN angeschlossen, d.h. der Layer 1 bleibt in Betrieb, die höheren Layer sind abgeschaltet. Ein Zugriff über LAN, z.B. über FTP, Telnet oder SNMP, ist daher bei einer Standby Baugruppe nicht möglich.

Wichtig: Beachten Sie, dass auch die in den Baugruppendaten konfigurierte Ethernet Bitrate von der Ursprungs- auf die Standby Baugruppe übernommen wird. Daher muss das LAN-Segment, an das die Standby Baugruppe angeschlossen ist, dieselbe Bitrate haben wie das LAN-Segment der Urprungsbaugruppe.

Das Leistungsmerkmal ist nicht systemübergreifend möglich, es ist auf eine Anlage beschränkt.

Es ist jedoch möglich, die IPDA Architektur zu nutzen, so dass die Common Gateway-Baugruppen und die Reserve-Baugruppen beliebig im OpenScape 4000 Host System oder im AP (Access Point) verteilt werden können, wobei

aber alle Baugruppen an das LAN angeschlossen werden müssen. In diesem Fall müssen alle Karten mit dem LAN verbunden sein.

Wichtig: Es ist zu beachten, dass die LAN-basierte Verfügbarkeit gewährleistet ist, sodass nicht nur das aktive Board, sondern auch das Board die IP-Stationen erreichen kann und umgekehrt. Zusätzlich ist zu beachten, dass es notwendig ist, die geänderte Zuordnung IP-Adresse zu MAC-Adresse mittels des erwähnten ARP-Requests in den LAN-Komponenten anzustoßen. Dieser „gratuitous ARP“-Request darf nicht blockiert werden (z.B. in der Router-Konfiguration).

Es ist ratsam, bei der Erstinbetriebnahme die automatische Umschaltung zu testen, so dass im Ernstfall die Umschaltung gewährleistet ist.

Da bei manuellem und automatischem Umschalten der Teilnehmer die Baugruppendaten mit umgezogen werden, ergeben sich Einschränkungen, falls die Umschaltung zwischen vollausgebauten (z.B. Q2316-X10) und teilausgebauten Baugruppen (z.B. Q2316-X) erfolgt. In diesem Fall ergeben sich folgende Besonderheiten:

- Werden nur gleichartige Baugruppen, d.h. Baugruppen die dieselben DSP Resourcen und damit dieselbe Anzahl von aktiven Verbindungen besitzen in einen Pool gebracht, gibt es keine Einschränkungen.
- Wird von einer teilausgebauten auf eine vollausgebaute Baugruppe umgeschaltet, so ist auf der vollausgebauten Baugruppe nach dem Umschalten nur die gleiche Anzahl von aktiven Verbindungen wie bei der teilausgebauten Baugruppe möglich. Um alle Resourcen der vollausgebauten Baugruppe nutzen zu können ist der UDP Portbereich zu erhöhen. Dabei ist zu beachten, dass eventuell Firewalls an den neuen UDP-Bereich angepasst werden müssen.
- Wird von einer vollausgebauten auf eine teilausgebaute Baugruppe umgeschaltet, so ist auf der neuen Baugruppe nach dem Umschalten nur eine reduzierte Anzahl von aktiven Verbindungen, nämlich die der teilausgebauten Baugruppe, möglich. Bei sehr vielen Teilnehmern mit hoher Vermittlungslast kann es dann häufiger zu Blockierungen kommen.

Werden die IP Teilnehmer manuell von einer Ursprungs-Baugruppe auf eine Ziel-Baugruppe umgeschaltet (Kommando: RESTART-BSSU:...,CGWSA=UMSCH,...;, so gilt es folgende Punkte zu beachten:

- Die Zielbaugruppe muss im Standby Mode **STBYRDY** sein, der DC-Zustand muss „Ready“ sein (z.B. nicht per AMO gesperrt) und das LAN-Kabel muss gesteckt sein.
- Die Ursprungs-Baugruppe darf sich nicht in einem Standby Mode befinden, d.h. es muss der **SMODE = NORMAL** eingestellt sein. Ansonsten kann die Baugruppe jeden DC-Zustand besitzen, also auch per AMO gesperrt sein. Ist dies der Fall, wird die manuelle Sperre auf die Ziel-Baugruppe übertragen. Ist der DC-Zustand oder der Zustand der LAN-Verbindung der Ursprungs-Baugruppe vor dem Umschalten „DEF“, ist nach dem Umschalten der **SMODE=STBYDEF** eingetragen. In allen anderen Fällen ist der **SMODE=STBYRDY** gesetzt, d.h. diese Baugruppe kann wieder als Reserve-Baugruppe dienen.

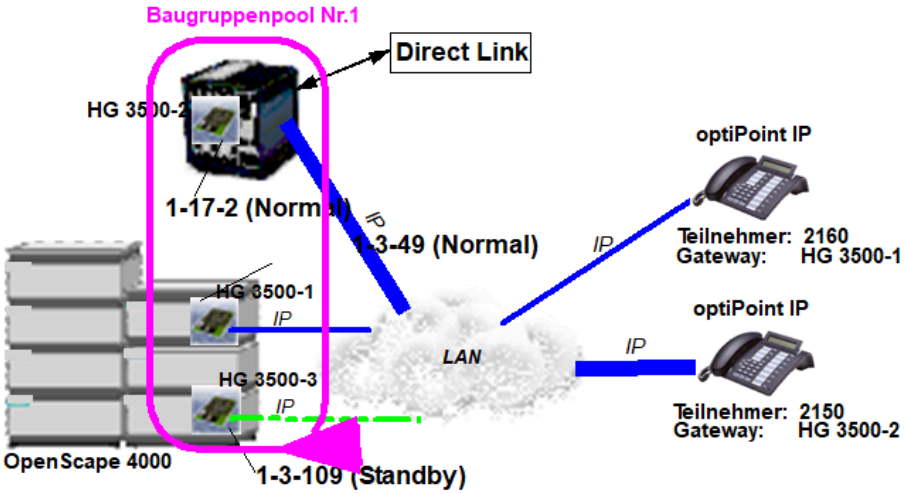
Wichtig: Der Zustand der LAN-Verbindung (Layer 1) kann, soweit es für das Umschalten eine Rolle spielt, auch mit dem

AMO BPOOL abgefragt werden. Selbstverständlich können Sie auch wie bisher den AMO SDSU benutzen.

Wichtig: Um ein SW-Update über den GW-Manager durchzuführen, benötigt auch das STMIX StandBy Board eine Management IP-Adresse (CGWB) und eine laufende Schnittstelle.

Für Software-Management-Funktionen wie LW und OS-Update aus dem Assistenten ist es wichtig, den STMIX mit einer Management-IP-Adresse (CGWB) zu konfigurieren, wie unter Kapitel , „Separate LAN-Konnektivität für Administration und VoIP“ beschrieben.

2.8.4 Generierung



Die allgemeine Konfiguration von WABE, LTU etc. wird aus Übersichtsgründen hier nicht dargestellt; es werden jedoch alle Common Gateway-spezifischen Kommandos aufgelistet: Es wird jedoch eine Liste aller gängigen Gateway-spezifischen Befehle bereitgestellt:

Einrichten des DIMSU-Speichers für die Common Gateway-Baugruppen:

```
EINR-DIMSU:TYP=SYSTEM,CGW=4;
```

Common Gateway-Baugruppen einrichten:

FCTBLK=1 : HG 3500-1

```
EINR-BFDAT:FCTBLK=1,FUNCTION=HG3530,BGBKAN=BKAN60;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3530,ANZSATZ=60,ANZBKAN=3
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANSW=JA;
```

FCTBLK=2 : HG 3500-2

```
AENDERN-BFDAT:FCTBLK=2,FUNCTION=HG3530,BRDBCHL=BCHL120;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=2,FUNCTION=HG3530,ANZSATZ=120,ANZBKAN=
AENDERN-BFDAT:CONFIG=OK,FCTBLK=2,ANSW=JA;
```

FCTBLK=3 : HG 3500-3 (Reserve-Baugruppe)

```
ADD-BFDAT:FCTBLK=3,FUNCTION=STANDBY,BRDBCHL=BCHL60&BCHL120;
```

Zuordnung von Funktionsblöcken auf Baugruppen:

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=49,SACHNR=Q2316-
X,FCTID=1,FCTBLK=1; /*HG
3500-1
EINR-BCSU:TYP=IPGW,LTG=1,LTU=17,EBT=2,SACHNR=Q2316-
X10,FCTID=1,FCTBLK=2; /*HG
3500-2
EINR-BCSU:TYP=IPGW,LTU=3,EBT=109,SACHNR=Q2316-
X,FCTID=1,FCTBLK=3; /*Standby-Bau►
gruppe HG 3500-3
```

Allgemeine und globale Leistungsmerkmal-Baugruppendaten der Common Gateway-Baugruppe einrichten. In diesem Beispiel werden 2 normale Baugruppen und eine Reserve-Baugruppe konfiguriert:

```
EINR-
CGWB:LTU=3,EBT=49,SMODE=NORMAL,IPADR=192.16.16.12,NETMASK=255.255.255.
*HG 3500-1
EINR-
CGWB:LTU=17,EBT=2,SMODE=NORMAL,IPADR=192.16.16.10,NETMASK=255.255.255.
*HG 3500-2
```

EINR-CGWB:LTU=3,EBT=109,SMODE=STBYRDY; /* Standby-Baugruppe HG 3500-3

Baugruppendaten auf die Baugruppen laden:

```
RESTART-BSSU:ADRART=LAGE,LTU=17,EBT=2,WZEIT=10;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=109,WZEIT=10;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=49,WZEIT=10;
```

Einrichten eines Baugruppen-Pools mit allen Baugruppen einschließlich Reserve-Baugruppe(n):

```
EINR-
BPOOL:MTYP=CGW,LTU=17,EBT=2,POOLNR=1,HOPAUT=SINGLE,INFO="TEST1";
EINR-BPOOL:MTYP=CGW,LTU=3,EBT=109,POOLNR=1; /* Standby-
Baugruppe */
EINR-BPOOL:MTYP=CGW,LTU=3,EBT=49,POOLNR=1;
```

Einrichten der IP Teilnehmer:

```
EINR-SBCSU:TLNNU=2150,ART=OPTI,ANSCHL=IP2,LAGE=1-17-2-29,
 GERKON=OP►
TIIP,COS1=5,COS2=6,LCOSS1=11,LCOSS2=12,LCOSD1=21,LCOSD2=22;
EINR-SBCSU:TLNNU=2160,ART=OPTI,ANSCHL=IP2,LAGE=1-3-49-0,
 GERKON=OP►
TIIP,COS1=5,COS2=6,LCOSS1=11,
 LCOSS2=12,LCOSD1=21,LCOSD2=22;
```

Zurücksetzen des FUNSU-Bits zum Verkürzen der Reload-Zeit der STMI2-Baugruppe

```
AENDERN-FUNSU:PIT=FLASH,SACHNR=âQ2316-
Xâ,FCTID=3,AKTION=RESET;
```

1) Automatisches Umschalten: Dies wird nicht über AMO gesteuert, sondern dadurch, dass eine Baugruppe, die sich im Betrieb befindet, außer Betrieb geht.

2) Beispiel vor dem automatischen Umschalten:

```
AB-BPOOL;
H500:  AMO BPOOL GESTARTET
```

```
+-------------------------------------------------------------
+
| POOLNR = 1                        MTYP = CGW
     HOPAUT = SINGLE    |
| INFO = TEST1
                         |
+-------------------------------------------------------------
+
| LTU = 3   EBT = 49                HOP-AUT-CNT = 0
     HOP-MAN-CNT = 0    |
| DC-STATUS = READY                LAN_VERB = READY
   SMODE = NORMAL       |
+-------------------------------------------------------------
+
| LTU = 3   EBT = 109               HOP-AUT-CNT = 0
     HOP-MAN-CNT = 0    |
| DC-STATUS = READY                LAN_VERB = READY
   SMODE = STBYRDY      |
+-------------------------------------------------------------
+
| LTU = 17   EBT = 2                HOP-AUT-CNT = 0
     HOP-MAN-CNT = 0    |
| DC-STATUS = READY                LAN_VERB = READY
   SMODE = NORMAL       |
+-------------------------------------------------------------
+
```

Wird jetzt die Baugruppe 1-3-49 defekt, werden alle Baugruppendaten und alle IP Teilnehmer auf die Reserve-Baugruppe 1-3-109 umgeschaltet. Damit ergibt sich nach dem Umschalten folgende AMO BPOOL Ausgabe:

```
AB-BPOOL;
H500:  AMO BPOOL GESTARTET
+-------------------------------------------------------------
+
| POOLNO = 1                       MTYPE = CGW
       HOPAUT = SINGLE |
| INFO = TEST1
                         |
+-------------------------------------------------------------
+
| LTU = 3   EBT = 49                HOP-AUT-CNT = 0
     HOP-MAN-CNT = 0    |
| DC-STATUS = NPR                  LAN_VERB =
   SMODE = STBYDEF      |
| SWITCHED AUTTO BRD LTU = 3     EBT = 109    DATUM/
UHRZEIT : 2003-09-25 18:07 |
+-------------------------------------------------------------
+
| LTU = 3   EBT = 109               HOP-AUT-CNT = 1
     HOP-MAN-CNT = 0    |
| DC-STATUS = READY                LAN_VERB = READY
   SMODE = NORMAL       |
| SWITCHED AUTFR BRD LTU = 3 EBT = 49         DATUM/
UHRZEIT : 2003-09-25 18:07 |
+-------------------------------------------------------------
+
```

```
| LTU = 17   EBT = 2          HOP-AUT-CNT = 0
 HOP-MAN-CNT = 0        |
| DC-STATUS = READY              LAN_VERB = READY
   SMODE = NORMAL       |
+-------------------------------------------------------------------
+
```

Erklärung wichtiger Abkürzungen in der Ausgabe:

HOPAUT: Automatisches Umschalten zwischen Baugruppen in diesem Pool ist nur einmal (SINGLE) oder mehrfach (MULTI) erlaubt.

SMODE: Standby Mode (siehe Abschnitt 8.3, „Serviceinformationen“

HOP-AUT-CNT: Anzahl der automatischen Umschaltungen

HOP-MAN-CNT: Anzahl der manuellen Umschaltungen

DC-STATUS: DC-Status der Baugruppe (siehe auch AMO SDSU)

LAN_VERB: Status der LAN-Verbindung; READY bedeutet i.a. „LAN-Kabel gesteckt“, DEF bedeutet i.a. „LAN-Kabel gezogen oder defekt“. Ist das Feld leer, hat die LAN-Verbindung einen DC-Zustand, der vom AMO BPOOL nicht interpretiert wird. In diesem Fall spielt der LAN-Status keine Rolle für das Umschalten. Bei Interesse können Sie den AMO SDSU benutzen.

Die folgenden Historie-Daten werden nur nach einem Umschalten angezeigt:

SWITCHED AUTFR BRD: Von dieser Baugruppe wurden (z.B. wegen eines Defekts) die IP Teilnehmer automatisch weggeschaltet (siehe auch **DATUM/ UHRZEIT**)

SWITCHED AUTTO BRD: Zu dieser Baugruppe wurden (z.B. wegen eines Defekts einer anderen Baugruppe) die IP Teilnehmer automatisch hingeschaltet (siehe auch **DATUM/UHRZEIT**)

SWITCHED MANFR BRD: Von dieser Baugruppe wurden (mit AMO BSSU) die IP Teilnehmer manuell weggeschaltet (siehe auch **DATUM/UHRZEIT**)

SWITCHED MANTO BRD: Zu dieser Baugruppe wurden (mit AMO BSSU) die IP Teilnehmer manuell hingeschaltet (siehe auch **DATUM/UHRZEIT**)

Die History-Daten können mit folgendem AMO-Befehl zurückgesetzt werden:

AENDERN-BPOOL:MTYP=CGW,ART=HISTRES,LTU=3,EBT=109;

Die Baugruppe 1-3-109 hat jetzt alle Funktionen der Baugruppe 1-3-49 übernommen, inklusive der IP Adresse der Baugruppe und sämtlicher IP Teilnehmer. Aus den Zusatzangaben kann man die Historie des letzten Schaltvorgangs ersehen. In diesem Beispiel erkennt man, dass am 25.9.2003 von 1-3-49 auf 1-3-103 umgeschaltet wurde, weil die Baugruppe 1-3-49 gezogen wurde (DC-Zustand NPR).

Die Zähler HOP-AUT-CNT und HOP-MAN-CNT sind für die Baugruppen, die sich im SMODE=NORMAL befinden, eingestellt. Bei Standby-Baugruppen sind alle Historie-Daten gelöscht.

3) Manuelles Umschalten per AMO BSSU:

   a) Es sollen die wegen eines Baugruppendefekts von 1-3-49 weggeschalteten Teilnehmer nach der Reparatur von 1-3-49 wieder bei der Inbetriebnahme zurückgeschaltet werden:
   `RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=49,CGWSA=IPSTNBCK;`

   oder
   `EINSCHALTEN-BSSU:LTU=3,EBT=49,CGWSA=IPSTNBCK;`

   Es sollen sämtliche IP Teilnehmer der Baugruppe 1-3-49 auf die Reserve-Baugruppe 1-3-109 umgeschaltet werden:
   `RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=49,CGWSA=UMSCH, LTU2=3,EBT2=109`

   Hier gilt es, zu beachten, dass eine evt. AMO-Sperre auf die Ziel-Baugruppe übernommen wird (siehe auch Abschnitt 8.3, „Serviceinformationen“)

   Es soll eine Baugruppe, die sich im Standby Mode **STBYDEF** befindet, z.B. wegen eines Defekts und weil die IP Teilnehmer weggeschaltet wurden, wieder als Reserve-Baugruppe dienen. Dies ist üblicherweise nach Reparatur bzw. Austausch der Baugruppe der Fall. Dafür ist folgendes Kommando einzugeben:
   `RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=49,,CGWSA=STBYRDY;`

4) Reload-Zeit der Common Gateway-Baugruppe verkürzen

   AENDERN-FUNSU:PIT=FLASH,SACHNR="Q2316-X",FCTID=1,AKTION=RESET;

2.8.5 Service-Aktionen nach automatischer Umschaltung

Nach einer Umschaltung im Fehlerfall können zwei Abläufe unterschieden werden:

1) Die umgeschalteten Teilnehmer sollen wieder ihre Ursprungslagen erhalten.
2) In diesem Fall muss der Baugruppen-Pool mit **HOPAUT=SINGLE** definiert sein!

   - Defekte Baugruppe tauschen bzw. LAN-Verbindung wieder herstellen.
   - Teilnehmer mit AMO-Befehl zurückschalten

   RESTART-BSSU:ADRART=LABE,LTU=xx,EBT=xx,CGWSA=CGWSWBCK;

   (xx -> Lage der Baugruppe mit Status **STDBYDEF**)

   - History-Daten des Baugruppen-Pools rücksetzen:

   `AENDERN-BPOOL:MTYP=CGW, TYP=HISTRES, LTU=j, EBT=zz;`
3) Die umgeschalteten Teilnehmer sollen auf den neuen Lagen verbleiben.
4) In diesem Fall muss der Baugruppen-Pool mit **HOPOUT=MULTI** definiert sein!

   - Defekte Baugruppe tauschen bzw. LAN-Verbindung wieder herstellen.
   - STDBYDEF-Baugruppe mit AMO-Befehl auf **STDBYRDY** schalten:
     `RESTART-BSSU:ADRART=LAGE, LTU=xx,EBT=xx, CGWSA=STBYRDY;`

2.8.6 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanaele fuer die HG3530 Funktion
	BCHL3530	e	Number of b-channels for HG3530 function
	FCTID	d	Function Id (muss immer 1 sein)
	FCTID	e	Function id (must always be set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Index to loadware block for the t1 board
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part number (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	ontinue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BPOOL	ART	d	Art der Pool-Daten: ALLE = Alle Pools löschen ATTR = Pool-Attribut ändern BAUGR = Baugruppe aus Pool löschen HISTRES = Historie der Baugruppe rücksetzen POOL = Einen bestimmten Pool löschen
	TYPE	e	Type of pool data: ALL = Delete all Pools ATTR = Change pool attribute BOARD = Delete board from pool HISTRES = Reset history for a board POOL = Delete a specific pool
	EBT	d	Einbauteilung
	SLOT	e	Slot
	HOPAUT	d	Pool-Attribut für die Hop-Kontrolle beim automatischen Umschalten: SINGLE = nur automatisches einmaliges Umschalten erlaubt MULTI = mehrfaches automatisches Umschalten erlaubt
	HOPAUT	e	Pool attribute for the hop control for automatic switchover: SINGLE = Automatic switchover is allowed only once MULTI = Automatic switchover is allowed several times
	Info	d	Pool-Attribut: Informationstext
	Info	e	Pool attribute: Information text
	LTU	d	Line Trunk Unit
	LTU	e	Line Trunk Unit
	MTYP	d	Modultyp, derzeit nur CGW möglich
	MTYPE	e	Module Type, currently onl CGW possible
	POOLNR	d	Nummer des Baugruppen-Rekonfigurations-Pools

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	POOLNO	e	Number of the Board Reconfiguration Pool
BSSU	CGWSA	d	CGW Schaltauftrag: CGWSWBCK: Rückschalten aller automatisch weggeschalteter IP Teilnehmer auf die Original-CGW-Baugruppe KEIN: Kein CGW bezogener Schaltauftrag STBYRDY: Verwendung als CGW Standby-Baugruppe (Reserve-Baugruppe) UMSCH: Umschalten der IP Teilnehmer der CGW-Baugruppe auf eine andere Baugruppe
	CGWSW	e	CGW switching activity: CGWSWBCK: Switch IP stations back to original CGW board NONE: No CGW specific activities STBYRDY: Act as CGW standby board SWITCH: Switchover IP stations of CGW board to another board
	LTG2	d	Line Trunk Group der Zielbaugruppe bei CGWSA=UMSCH
	LTG2	e	Line Trunk Group of the destination board of CGWSW=SWITCH
	LTU2	d	Line Trunk Unit der Zielbaugruppe bei CGWSA=UMSCH
	LTU2	e	Line Trunk Unit of the destination board of CGWSW=SWITCH
	EBT2	d	Einbauteilung der Zielbaugruppe bei CGWSA=UMSCH
	SLOT2	e	Slot of the destination board of CGWSW=SWITCH

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	SMODE	d	Standby Mode oder Normal Mode **Normal**: Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. **STDBYRDY**: Eine Baugruppe im Standby Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. **STDBYDEF**: Eine Baugruppe im Standby Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE	e	Standby Mode or Normal Mode **NORMAL**: A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. **STDBYRDY**: A board in Standby Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. **STDBYDEF**: A board in Standby Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network addresss part but different host address parts (also the Default Router must fulfill this requirement)
FUNSU	AKTION	d	Ladeart der Baugruppe: Damit der LW Code nicht bei jedem Baugruppen-Reset geladen wird, sollte RESET eingestellt sein.
	ACTION	e	Action set or reset loadware on board: In order to avoid loading of the LW code, it is recommended to set this parameter to RESET.

2.9 DLS-Client-Bootstrapping

Ehe DLS-Server und Gateway Konfigurationsdaten miteinander austauschen können, ist einmalig das sogenannte DLS Client Bootstrapping erforderlich. Dabei wird für das Gateway ein individuelles (DLS-)Zertifikat erzeugt und an das Gateway übertragen. Anhand der Zertifikate können sich Gateway und DLS anschließend eindeutig wechselseitig autentifizieren.

2.9.1 Bootstrapping mit PIN Modus „Keine PIN“

Variante A:

1) Virtuelles IP-Gerät im DLS unter **IP Devices > IP Device Verwaltung > IP Device Konfiguration** anlegen.
2) Gateway mittels Funktion **IP Devices > IP Device Interaktion > IP Devices scannen** im DLS kontaktieren. Hierbei ist im **Register „IP Bereiche“** im Feld **Port 8084** einzutragen.

Wenn alles korrekt funktioniert hat, wird im DLS unter **IP Devices > IP Device Vewrwaltung > IP Device Konfiguration > Register „DLS Verbindung“** im Feld **Security Status:** der Wert **Sicher** angezeigt.

Variante B:

1) Virtuelles IP-Gerät im DLS unter **IP Devices > IP Device Verwaltung > IP Device Konfiguration** anlegen.
2) Am Gateway mit CLI-Kommando `set dls ip_address` die IP-Adresse des DLS-Servers eintragen. Der Port ist üblicherweise 18443.
3) Am Gateway das CLI-Kommando `contact DLS` eingeben.

2.9.2 Bootstrapping mit PIN Modus „Standard PIN“ oder „Individuelle PIN“

Variante A:

1) Virtuelles IP-Gerät im DLS unter **IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „DLS Verbindung“** anlegen und dabei gewünschten PIN Modus wählen.
2) Gateway mittels Funktion **IP Devices > IP Device Interaktion > IP Devices scannen** im DLS kontaktieren. Hierbei ist im **Register „IP Bereiche“** im Feld **Port 8084** einzutragen.
3) Am Gateway CLI-Kommando `activate dls pin <pin>` mit der unter 1. angezeigten PIN eingeben.

Variante B:

1) Virtuelles IP-Gerät im DLS unter **IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „DLS Verbindung“** anlegen und dabei gewünschten PIN Modus wählen.
2) Am Gateway mit CLI-Kommando `set dls ip_address` die IP-Adresse des DLS-Servers eintragen. Der Port ist üblicherweise 18443.
3) Am Gateway das CLI-Kommando `contact DLS` eingeben.
4) Am Gateway CLI-Kommando `activate dls pin <pin>` mit der unter 1. angezeigten PIN eingeben.

2.10 Zurücksetzen einer NCUI-Baugruppe

2.10.1 Gründe für das Zurücksetzen der NCUI

- Die Anmeldedaten für die Baugruppe sind unbekannt und entsprechen nicht den Standardeinstellungen.
- Die Baugruppe wird nicht vollständig gestartet, aber das Boot-Menü ist noch erreichbar.
- Die Baugruppe muss formatiert werden.

2.10.2 Methoden zur Übertragung der Loadware

Es gibt zwei Methoden zur Übertragung der Loadware:

- Methode 1: Mit einem PC auf dem LAN mit TFTP-Server
- Methode 2: Mit einem FTP-Server (hierfür kann die OpenScape 4000 selbst verwendet werden)

2.10.3 Wichtige Hinweise

- Die NCUI-Baugruppe wird über die Anwendung **OpenScape 4000 Expert Access** (auch bekannt als ComWin) zurückgesetzt.
- Verwenden Sie den Telnet-Terminalbildschirm, da im normalen Dialog die NCUI-Eingabeaufforderungen nicht korrekt angezeigt werden. Die Einstellungen sind 38400, 8, none, 1. Stellen Sie sicher, dass „End Of

Command“ (unter **TeInet > Parameter > Edit**) auf **CR** und nicht auf **ETX** eingestellt ist. Natürlich können auch andere Terminalprogramme verwendet werden.

- Beachten Sie bei der Eingabe von Befehlen an die NCUI-Baugruppe die Groß- und Kleinschreibung. Mit dem Kleinbuchstaben „w“ wird ein Software-Image über FTP geladen und an TFFS kopiert, wohingegen mit dem Großbuchstaben „W“ eine Datei über FTP geladen und an TFFS kopiert wird.

Die Ausgaben der NCUI-Baugruppe sind in der Schriftart `Courier` und die manuellen Aktionen oder Texteingaben sind blau dargestellt.

2.10.4 Verfahren

So rufen Sie das Boot-Menü auf:

Verbinden Sie ComWin mit der v24-Schnittstelle mit den obigen Einstellungen.

Drücken Sie die Reset-Taste. Die folgenden Eingabeaufforderungen werden angezeigt.

```
RS232 initialized for Output: 38400,8,n,1
loading FPGA: Load O.K.
testing Checksum Firmware: Test O.K.
testing Data-Bus DRAM: Test O.K.
testing Address-Bus DRAM: Test O.K.
testing Pattern 0x55555555: Test O.K.
testing Pattern 0xAAAAAAAA: Test O.K.
```

Drücken Sie bei der Eingabeaufforderung „stop auto-boot“ eine beliebige Taste und geben Sie das richtige Passwort ein:

```
Total TFFS size: 31846400 bytes / free: 17645568 bytes
SW_IMAGE.001 10/18/07 10:03:31
SW_IMAGE.002 05/16/06 13:27:14
Press any key to stop auto-boot...
Boot password: HIPATH4000
[NCUI2 Boot CLI]:
```

So formatieren Sie die NCUI-Baugruppe:

(Optional, es seid denn, die Anmeldedaten für die Baugruppe sind nicht bekannt!)

(Lowlevel-Formatierung ist ebenfalls optional!)

```
[NCUI2 Boot CLI]: y
Format the flash file system, all files will be deleted.
Do you want to format the flash file system y/[n]? y
Do you want to low-level format the flash file system y/
[n]?
n
Formatting the flash file system!
Format ok!
[NCUI2 Boot CLI]:
```

Hochladen der Software – Methode 1: Mit einem PC auf dem LAN mit TFTP-Server

Sie benötigen eine Kopie der NCUI-Loadware und müssen sie auf diesem TFTP-Server bereitstellen, da die NCUI-Karte auf diese Weise ihre Loadware erhält. Die Loadware finden Sie auf dem System unter:

`:PDS:APSP/LTG/LGA0/PZKNCUI20` (NCUI2) oder

`:PDS:APSP/LTG/LGA0/PZKNCUI40` (NCUI2+/NCUI4) je nach Baugruppe.

Wichtig: Natürlich können in SWS neuere Versionen vorhanden sein.

- Geben Sie den Kleinbuchstaben c ein, um die folgenden Einstellungen aufzurufen (IP-Adressen bei Bedarf anpassen):

```
[NCUI2 Boot CLI]: c
'.' = clear field;  '-' = go to previous field;  ^D =
 quit
boot device          : tffs/0 emac
processor number     : 0
host name            :
file name            : SW_IMAGE.002 PZKNCI40
inet on ethernet (e) : 192.168.112.65:ffffff00 */ Bei
 Bedarf
ändern
inet on backplane (b):
host inet (h)        : 192.168.111.134
gateway inet (g)     :
user (u)             :
ftp password (pw) (blank = use rsh):
flags (f)            : 0x1000 0x80
target name (tn)     :
startup script (s)   :
other (o)            : emac
```

- Optional: Geben Sie z ein, um die Parameter für weitere Aufrufe zu speichern:

```
[NCUI2 Boot CLI]: z
Copy content of /tffs/bootline.act into /tffs/
bootline.bck.
Write /tffs/bootline.act ok!
```

- Geben Sie w ein, um das neue Image zu laden. Geben Sie außerdem das Suffix-Image 001 ein:

```
[NCUI2 Boot CLI]: w
SW_IMAGE.001  11/28/13 02:29:13
SW_IMAGE.002  11/22/13 08:21:30
Input a new suffix SW_IMAGE.x: 001
Nun sollten Sie sehen, dass die LW übertragen wird:
Attached TCP/IP interface to emac0.
Attaching network interface lo0... done.
Loading...
1448 bytes
.
.
10270624 bytes
Loading ok.
```

- Beantworten Sie die Frage, ob beim nächsten Booten dieses Image verwendet werden soll, mit „y“:
  ```
  Change bootline to the loaded image
  and write bootline to TFFS (y/n)? y
  ```
- Weisen Sie die Karte schließlich mit @ an, neu zu starten:
  ```
  [NCUI2 Boot CLI]: @
  ```

Aktualisieren der Software – Methode 2: Mit einem FTP-Server

Anmerkung: Die OpenScape 4000 lässt sich wie im unten stehenden Beispiel dargestellt selbst als FTP-Server einsetzen.

Es kann ein beliebiger FTP-Server verwendet werden. Sie benötigen einen gültigen FTP-Server mit der Loadware in dem Root-Verzeichnis, mit dem sich der FTP-Client verbindet. Die Loadware finden Sie auf dem System unter:

`:PDS:APSP/LTG/LGA0/PZKNCUI20` (NCUI2) oder

`:PDS:APSP/LTG/LGA0/PZKNCUI40` (NCUI2+/NCUI4) je nach Baugruppe.

Wichtig: Natürlich können in SWS neuere Versionen vorhanden sein.

Wichtig: Wenn Sie die OpenScape 4000 verwenden, muss die Loadware in das Root-Verzeichnis des Bereichs :PDS: kopiert werden. Die IP „host inet“ muss dann die IP des aktiven CC (also CCA oder CCB) sein.

- Geben Sie den Kleinbuchstaben c ein, um die folgenden Einstellungen aufzurufen (IP-Adressen bei Bedarf anpassen):

```
[NCUI2 Boot CLI]: c
'.' = clear field;  '-' = go to previous field;  ^D =
 quit
boot device          : tffs/0 emac
processor number     : 0
host name            :
file name            : SW_IMAGE.002 PZKNCI40
inet on ethernet (e) : 192.168.112.65:ffffff00 */ Bei
 Bedarf
ändern
inet on backplane (b):
host inet (h)        : 192.168.111.134
gateway inet (g)     : 192.168.112.254 */ Für Direct-
Link AP
nicht benötigt
user (u)             : hicom */ Standard-Benutzer für 4K
ftp password (pw) (blank = use rsh): hipath */ Standard-
Passwort für 4K
flags (f)            : 0x1000 0
target name (tn)     :
startup script (s)   :
other (o)            : emac
```

- Optional: Geben Sie z ein, um die Parameter für weitere Aufrufe zu speichern:
```
[NCUI2 Boot CLI]: z
Copy content of /tffs/bootline.act into /tffs/
bootline.bck.
Write /tffs/bootline.act ok!
```
- Geben Sie w ein, um das neue Image zu laden. Geben Sie außerdem das Suffix-Image 001 ein:
```
[NCUI2 Boot CLI]: w
SW_IMAGE.001  11/28/13 02:29:13
SW_IMAGE.002  11/22/13 08:21:30
Input a new suffix SW_IMAGE.x: 001
```
- Nun sollten Sie sehen, dass die Loadware übertragen wird:
- Beantworten Sie die Frage, ob beim nächsten Booten dieses Image verwendet werden soll, mit y:
```
Change bootline to the loaded image
and write bootline to TFFS (y/n)? y
```
- Weisen Sie die Karte schließlich mit @ an, neu zu starten:
```
[NCUI2 Boot CLI]: @
```

2.11 Zurücksetzen einer STMIX-Baugruppe

2.11.1 Allgemeine Beschreibung

STMIX kann neu geflasht werden, falls die Baugruppe nicht bootet oder in RMX nicht READY wird.

Das Verfahren kann auch zum Zurücksetzen einer STMIX-Baugruppe auf die Werkseinstellungen verwendet werden. Alle vom Kunden gespeicherten Daten werden von der Baugruppe gelöscht.

Hardware- und Verkabelungsvoraussetzungen

- PC oder Notebook mit Windows-Betriebssystem: Es muss eine Verbindung zwischen dem PC/Notebook und der STMIX-Baugruppe über ein an STMIX LAN1 angeschlossenes LAN-Kabel hergestellt werden.

  In dem in diesem Dokument aufgeführten Beispiel verwendet STMIX die IP-Adresse 192.0.2.101. Es wird dringend empfohlen, für den PC **192.0.2.100** mit der Netzmaske 255.255.255.0 zu verwenden. Konfigurieren Sie KEINE andere IP-Adresse auf derselben Schnittstelle, um Probleme zu vermeiden.

  INFO: Es ist möglich, eine zweite PC-Netzwerkschnittstelle zu verwenden, falls vorhanden.

- USB-Kabel, Typ A auf Typ B (z. B. USB-Druckerkabel): Schließen Sie den Windows-PC über USB (Typ A) und den STMIX über USB (Typ B) an.
- STMIX in OpenScape 4000, beliebiger Rahmentyp: AP37009, AP370013, LTUW usw.

Software-Voraussetzungen

- DHCP-Server + TFTPD-Server: z. B. tftpd64.exe von https://tftpd64.software.informer.com/download/

  INFO: Verwenden Sie die 32-Bit-Version, wenn Sie ein 32-Bit-Windows-Betriebssystem verwenden.

- HTTP-Dateiserver: z. B. HFS.exe von https://www.rejetto.com/hfs/?f=dl
- Dekomprimierungstool, das das Entpacken von .exe- und .gz-Dateien unterstützt: z. B. 7zip.
- SSH-Client (z. B. Putty) für den SSH-Zugang zu OpenScape 4000 und für den COM-Port-Zugang zu STMIX über den USB-Port.
- SFTP-Client (z. B. WinSCP) zum Herunterladen von Dateien von der OpenScape 4000-Plattform.
- STMIX USB-Treiber aus OS4K-Installations-ISO: z. B. OS4K_V10_R0.28.0_InstallImage.iso\DriversAndTools \STMIX_USB_Serial_Console_Driver\
- JeOS-Image für STMIX, erstellt auf der OS4K-Linux-Plattform.

  NOTICE: Mindestens erforderliche OS4K-PLT-Version: V8 R2.22.9 oder V10 R0.28.5.

2.11.2 Vorbereiten der erforderlichen Dateien

1) Erstellen Sie einen Arbeitsordner auf dem PC (z. B. D:\stmix-image-repo) und kopieren Sie den HTTP-Fileserver (hfs.exe) und den TFTPD/DHCP-Server (tftpd64.exe).

   NOTICE: Die Datei tftpd64.exe kann entweder installiert oder aus dem Installationsprogramm (mit 7-Zip) extrahiert und in den Arbeitsordner kopiert werden. Die hfs.exe muss nicht installiert werden.

2) Verbinden Sie sich per SSH mit der Linux-Plattform eines beliebigen OS4K-Einsatzmodells (Simplex, Duplex, Survivable, Standalone usw.) und erzeugen Sie das STMIX-Image mit dem folgenden Befehl:
   `bash /opt/yaps/create_stmix_PXE_boot_image.sh`

   Das Ergebnis wird auf der OpenScape 4000-Plattform Linux unter folgenden Pfad gespeichert: /stmix-image-repo.
3) Die generierten Dateien müssen per SFTP-Client in den auf dem PC erstellten Arbeitsordner (D:\stmix-image-repo) kopiert werden.
4) Wählen Sie die Datei .pxeboot aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie dann die 7-Zip-Option "Archiv öffnen". Doppelklicken Sie nun auf die angezeigte .tar.gz-Datei und öffnen Sie sie.
5) Extrahieren Sie den Inhalt mit der Option "Extrahieren" (oder ziehen Sie den Inhalt des Ordners per Drag&Drop) in den Arbeitsordner (D:\stmix-image-repo).
6) Der Arbeitsordner sollte nun die folgenden Dateien enthalten:
   `STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz`
   `STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.md5`
   `STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.pxeboot`

```
pxelinux.cfg\default
initrd
menu.c32
pxelinux.0
vmlinuz
hfs.exe
tftpd64.exe
```

INFO: Es kann auch ein Ordner mit Paxheaders erzeugt werden, der aber ignoriert werden kann.

NOTICE: Die Datei "D:/stmix-image-repo/pxelinux.cfg/default" ist für das Netzwerk 192.0.2.0/24 vorkonfiguriert. Wenn die Standardwerte nicht verwendet werden, muss die Datei bearbeitet werden, um sie an die IP-Konfiguration anzupassen.

2.11.3 Tool-Konfiguration für das Flashen

NOTICE: Es wird empfohlen, die Tools als Administrator auszuführen. Andernfalls werden die Einstellungen möglicherweise nicht gespeichert.

Tool-Konfiguration:

1) Führen Sie die Datei hfs.exe des Webservers aus:

Menü -> Dateien hinzufügen

Wählen Sie die folgenden Dateien aus dem Ordner "D:/stmix-image-repo" aus und öffnen Sie sie:
`STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz`
`STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz.md5`

Menü -> IP-Adresse

Wählen Sie die IP-Adresse, die auf der mit dem STMIX LAN-Port verbundenen Schnittstelle verwendet wird (z. B. 192.0.2.100).

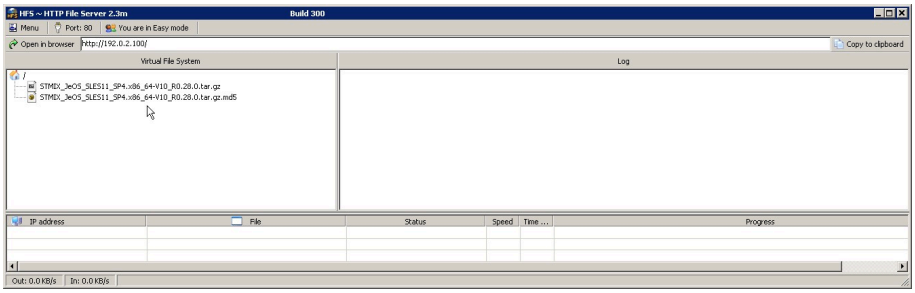


Figure 17: IP-Einstellungen für hfs.exe

2) Führen Sie die Datei tftpd64.exe aus. Stellen Sie sicher, dass die folgenden Einstellungen vorhanden sind:

- **Aktuelles Verzeichnis**: D:/stmix-image-repo

  Server-Schnittstellen: Wählen Sie die mit STMIX verbundene Schnittstelle

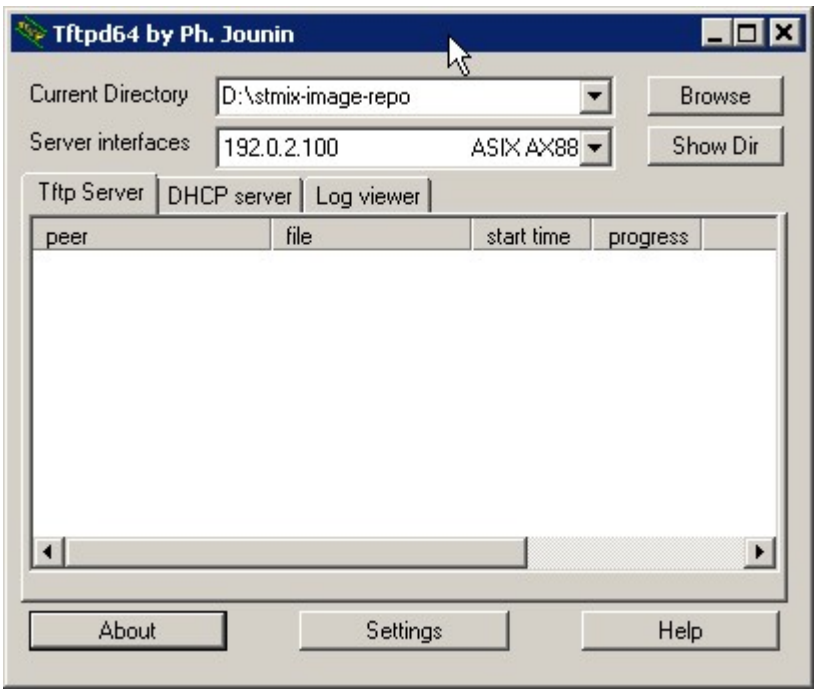


Figure 18: Einstellungen für tftpd64.exe

- **Sorgen Sie unter der Registerkarte GLOBAL für Folgendes:**
  - Das Kästchen "TFTP-Server" ist aktiviert.
  - Das Kästchen "DHCP-Server" ist aktiviert.

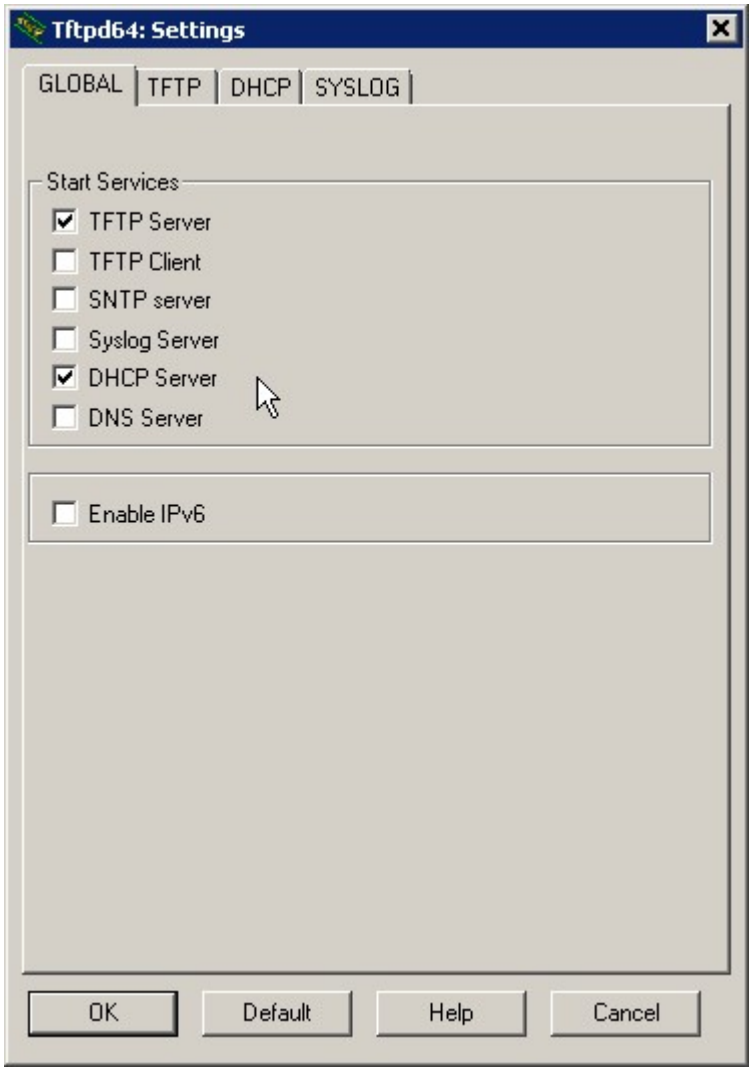


Figure 19: GLOBAL-Einstellungen für tftpd64.exe

- **Sorgen Sie unter der Registerkarte TFTP für Folgendes:**
  - Das Basisverzeichnis ist auf "D:/stmix-image-repo" festgelegt.
  - Das Kästchen "PXE-Kompatibilität" ist aktiviert.
  - Das Kästchen "TFTP binden" ist aktiviert und die IP-Adresse der mit STMIX verbundenen Windows-PC-LAN-Schnittstelle wird aus dem Dropdownmenü ausgewählt.

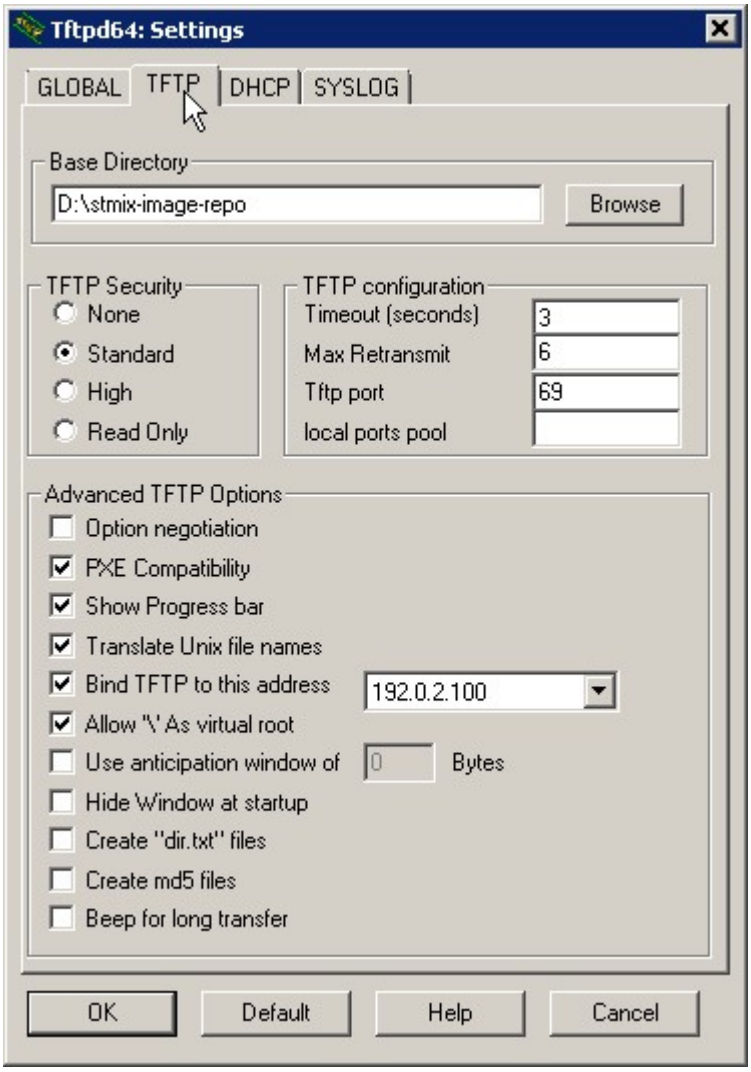


Figure 20: TFTP-Einstellungen für tftpd64.exe

- **Sorgen Sie unter der Registerkarte DHCP für Folgendes:**
  - IP-Pool-Startadresse: IP-Adresse von STMIX (z. B. 192.0.2.101)
  - Größe des Pools: 1
  - Boot-Datei: pxelinux.0
  - Maske: 255.255.255.0
  - Permanente Leases: Das Kästchen darf nicht aktiviert sein.
  - Binden Sie DHCP an diese Adresse: IP der LAN-Schnittstelle des Windows-PCs, der mit STMIX verbunden ist (z. B. 192.0.2.100)

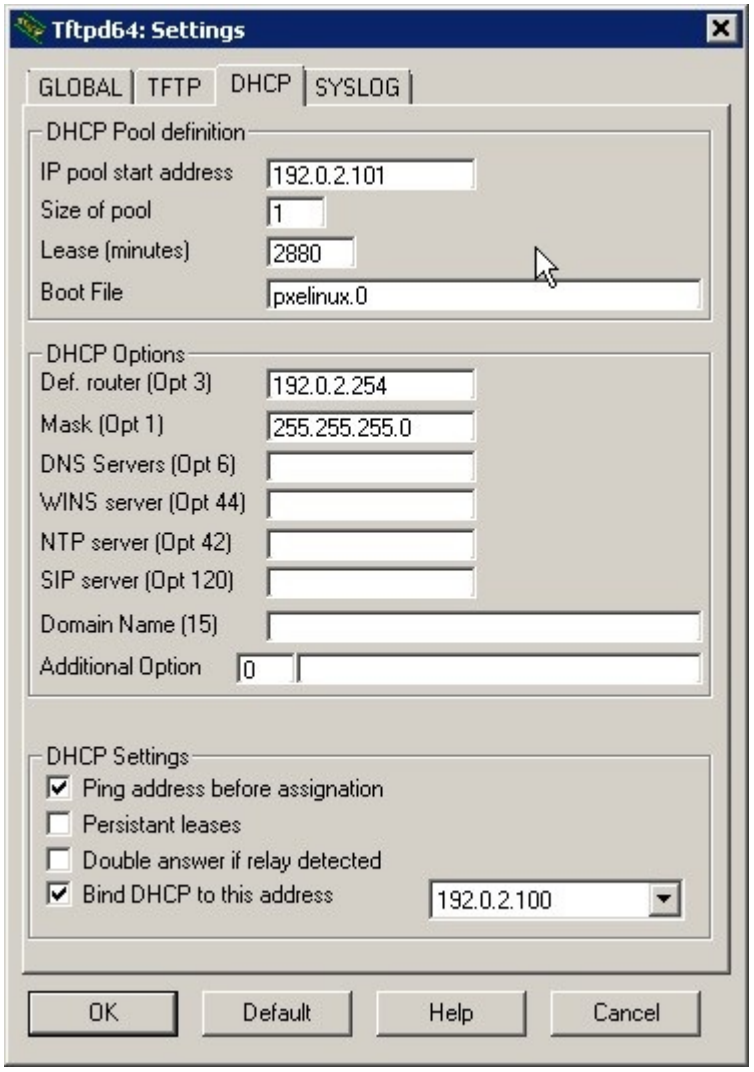


Figure 21: DHCP-Einstellungen für tftpd64.exe

IMPORTANT: Nachdem Sie die obigen Schritte ausgeführt haben, beenden Sie das Programm tfdtp64 und starten Sie es neu, um die konfigurierten Einstellungen zu initialisieren.

2.11.4 STMIX USB-Konfiguration

USB-Terminal

Installieren Sie den STMIX USB-Treiber auf dem Windows-PC.

Wenn das USB-Kabel angeschlossen und die STMIX-Baugruppe eingeschaltet ist, identifizieren Sie den STMIX zugewiesenen COM-Port im Geräte-Manager des Windows PC:

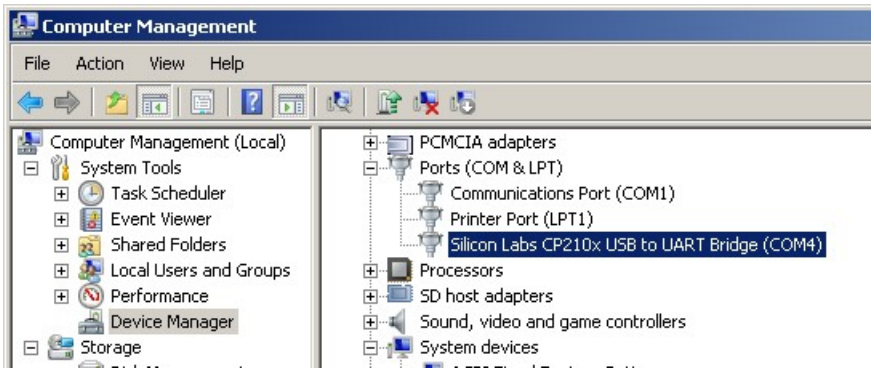


Figure 22: Geräte-Manager, COM-Anschluss

Konfigurieren Sie in Putty eine neue Verbindung für den identifizierten COM-Port. Die serielle Schnittstelle sollte mit den Werten "115200", "8", "1", "Keine", "Keine" konfiguriert werden.

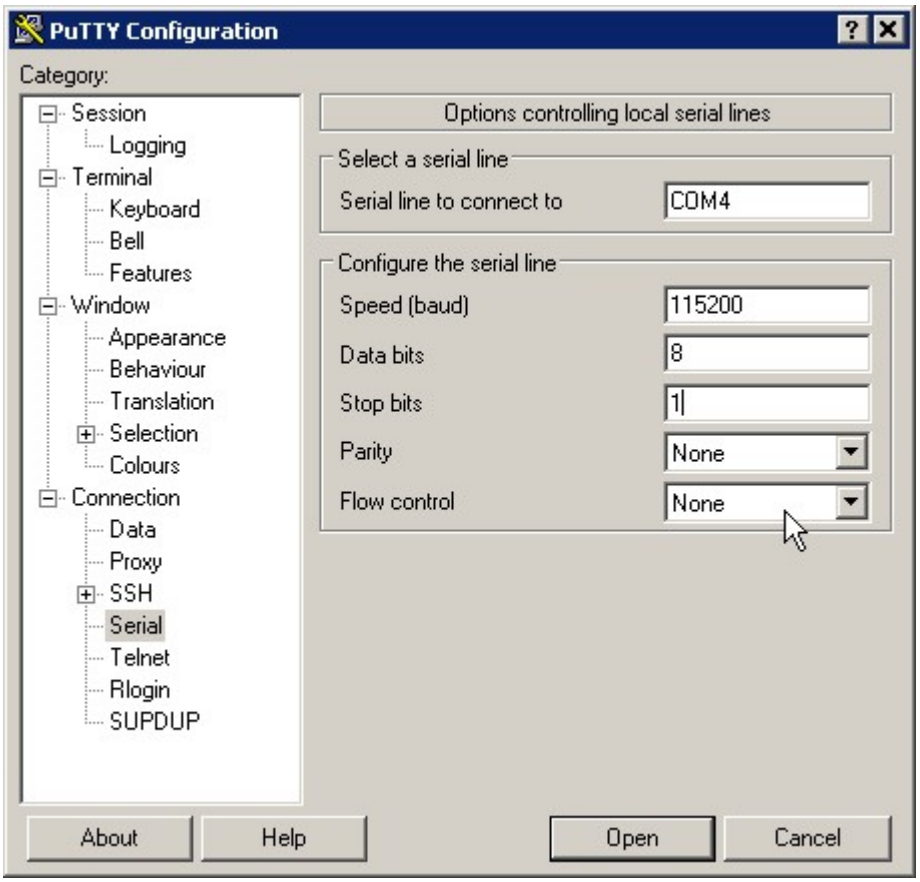


Figure 23: PuTTY-Konfiguration

Die Tastatur sollte auf den Typ "Linux" eingestellt sein, wie unter "Funktionstasten und Tastenfeld" gezeigt.

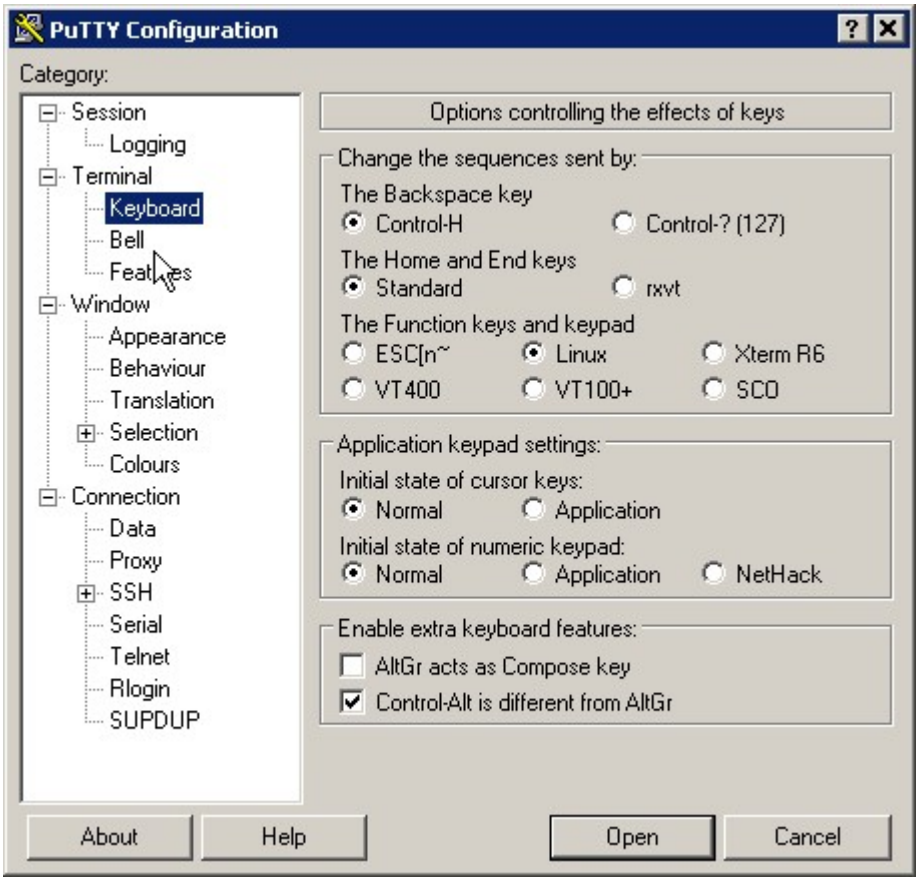


Figure 24: Einstellungen für die Tastatur

Speichern Sie die Sitzung. Sie können nun eine Verbindung mit STMIX USB-COM herstellen. Der Benutzername ist TRM und das Kennwort ist wie in AMO CGWB konfiguriert.

2.11.5 STMIX-Reflash

1) Starten Sie STMIX per SSH neu oder schalten Sie die Baugruppe durch erneutes Anschließen aus und wieder ein.

2) Achten Sie auf die STMIX-BIOS-Einstellungen.

Im Terminal sehen Sie den Bootvorgang von STMIX. Drücken Sie sofort Esc oder Entf, um das BIOS-Setup aufzurufen.

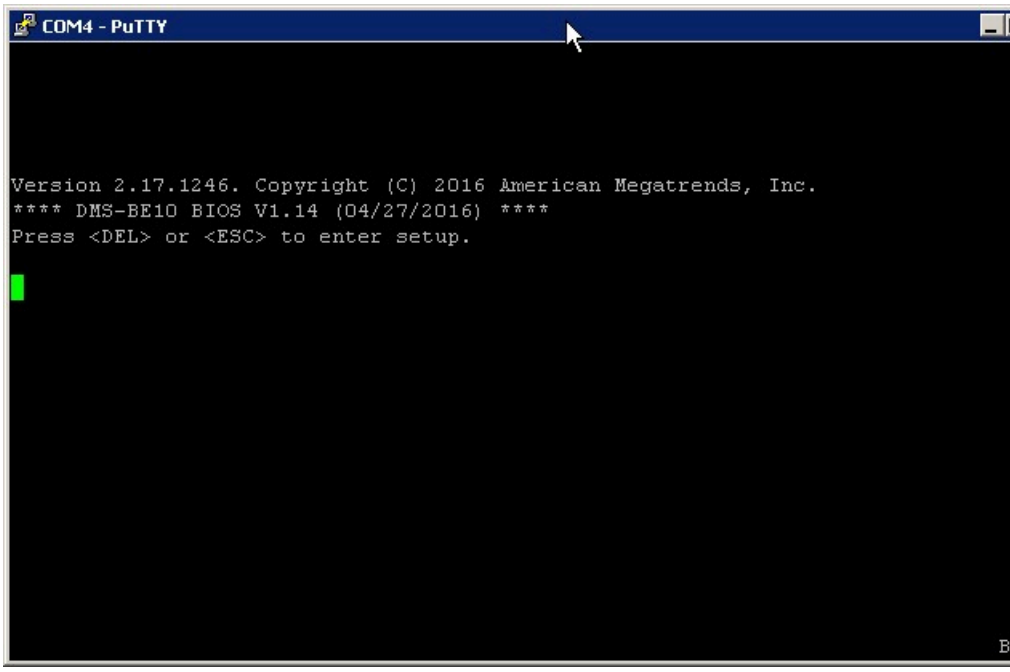


Figure 25: STMIX über PuTTY zurücksetzen

Wählen Sie im Bereich „Speichern & Beenden“ die Bootoption "Realtek PXE" und drücken Sie die Eingabetaste.

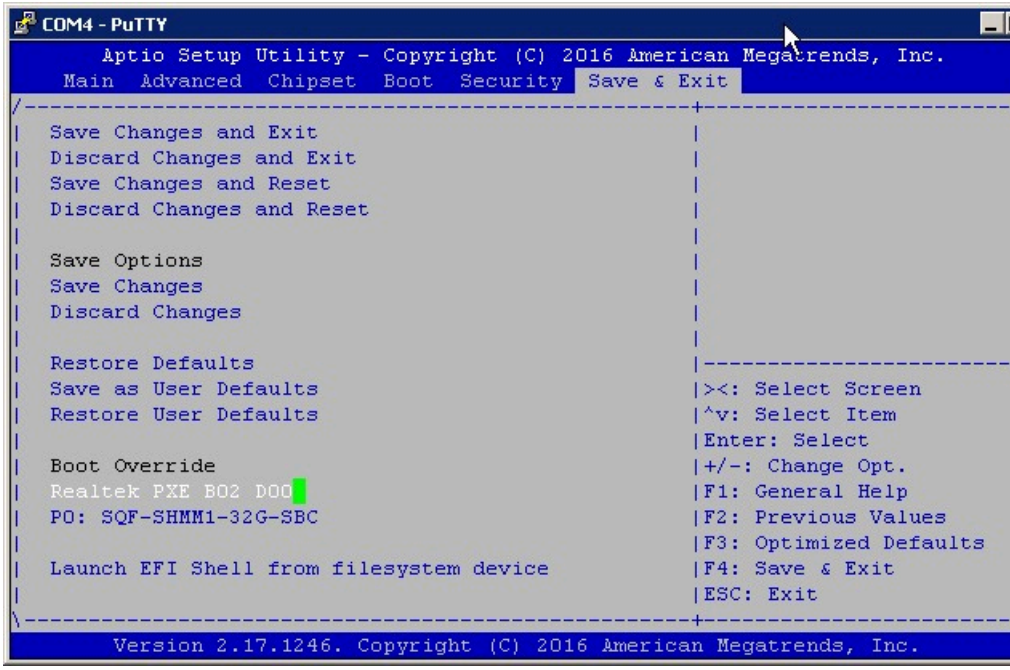


Figure 26: STMIX-Bootvorgang

NOTICE: Wenn es keine Bootoption für "Realtek PXE" gibt, aktivieren Sie diese zunächst unter **Chipsatz -> South**

Bridge -> Lan1 Option-ROM -> Aktivieren -> Speichern.
Beenden Sie den Vorgang und beginnen Sie von vorne.

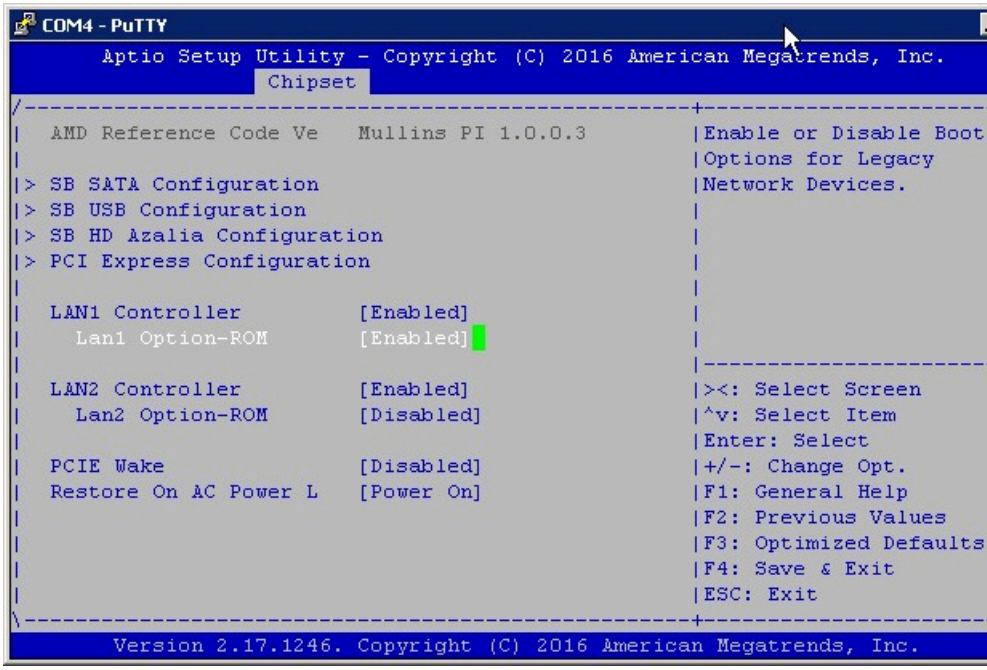


Figure 27: Lan1 Option-ROM aktivieren

3) Beim Booten sehen Sie den STMIX PXE-Bootvorgang im Terminal.



Figure 28: STMIX PXE-Boot-Bildschirm

Sie sollten nun im dhcp/tftpd-Programm Popup-Meldungen mit der zugewiesenen IP-Adresse und den in STMIX geladenen Dateien sehen.

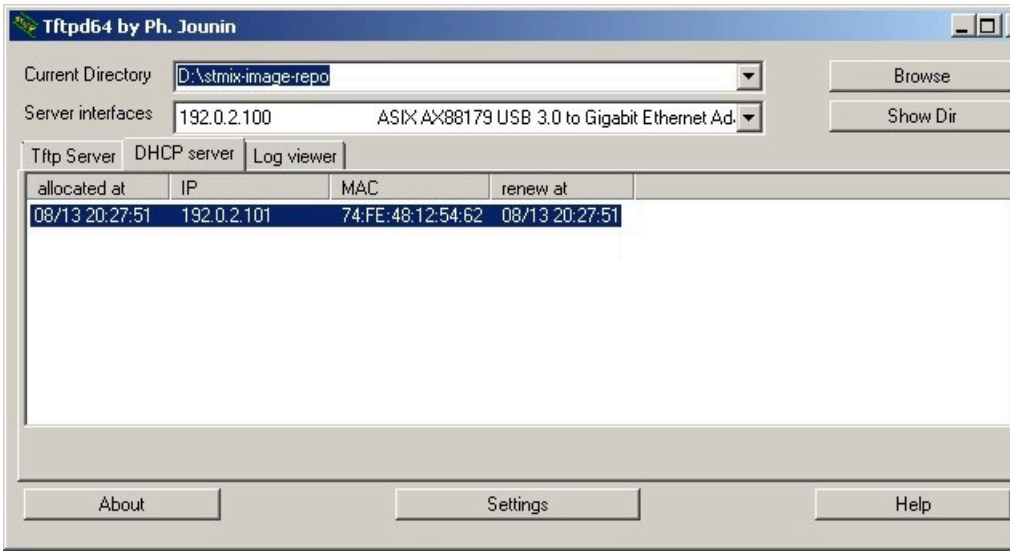


Figure 29: DHCP zugewiesene Adresse

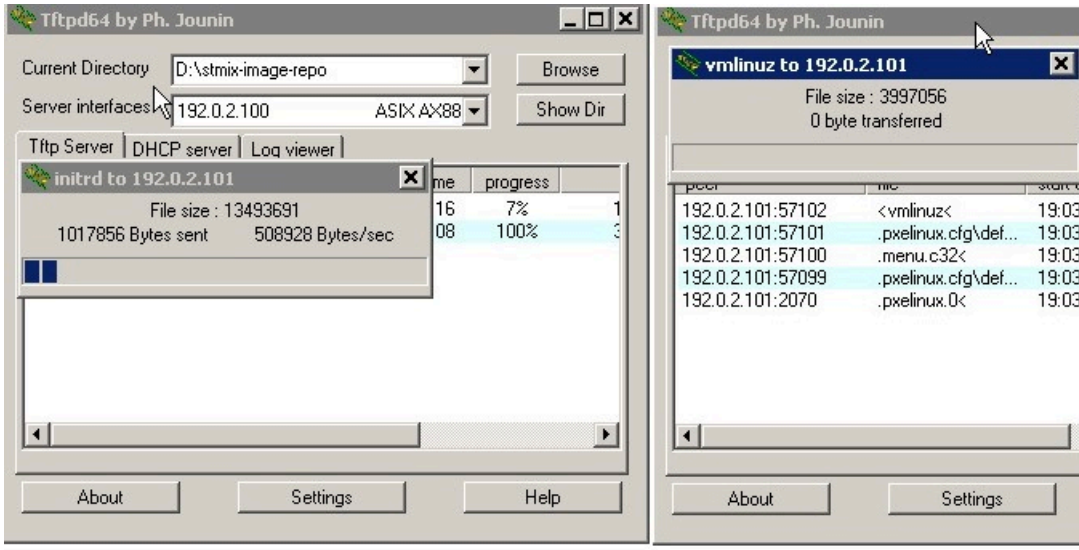


Figure 30: tftpd-Popups

Die Ausgabe im STMIX-Terminal sollte nun Folgendes anzeigen:

- vmlinuz wird geladen.....
- initrd wird geladen.....

Das Ladeprogramm wird gestartet und ruft das Image ab. Die Anzeige im Terminal sollte lauten: "Folgendes Image wird abgerufen: http://192.0.2.100/STMIX_JeOS_SLES11_SP4.x86_64-V10_R0.28.0.tar.gz"

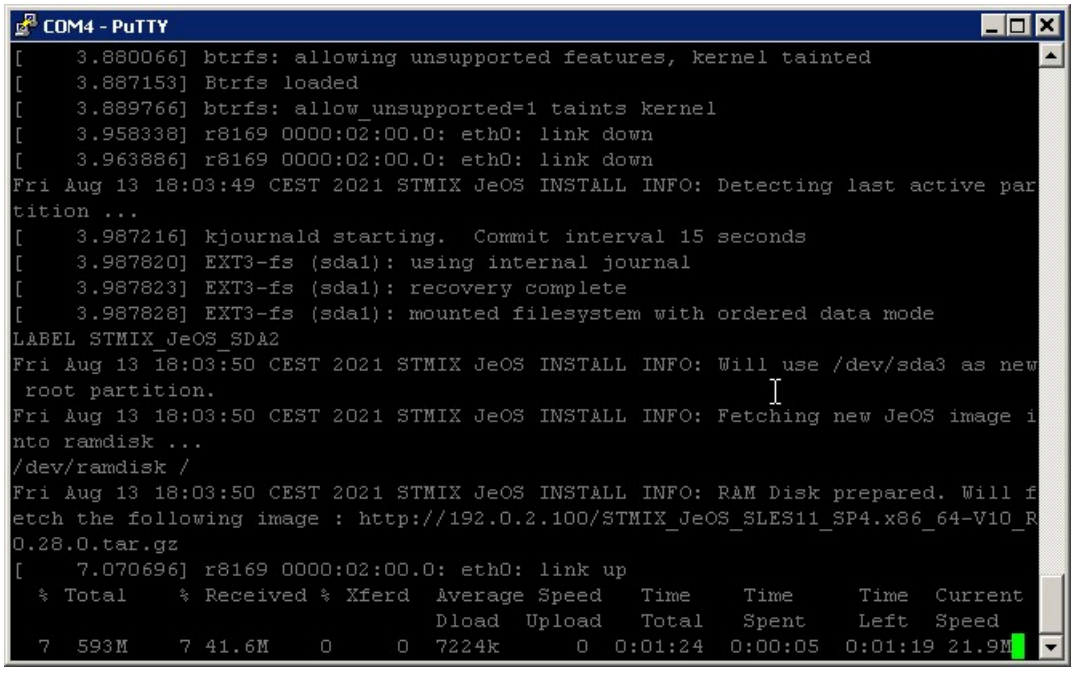


Figure 31: JeOS-Image-Abruf

Der Fileserver zeigt in der Protokollanzeige das geladene Image und die Prüfsumme an.

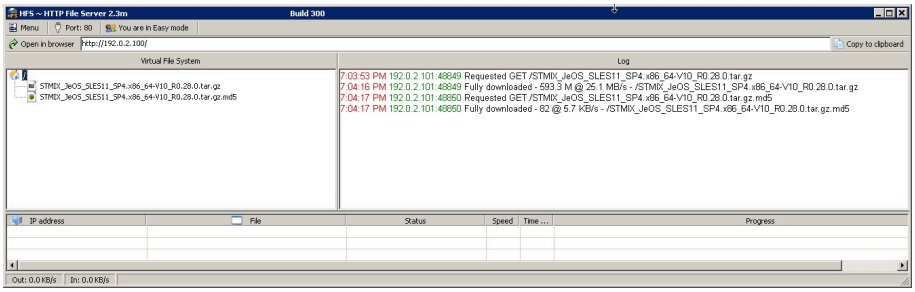


Figure 32: Image geladen

Das Image wird entweder auf sda2 oder sda3 geladen, wodurch die Partition aktiviert und neu gestartet wird.

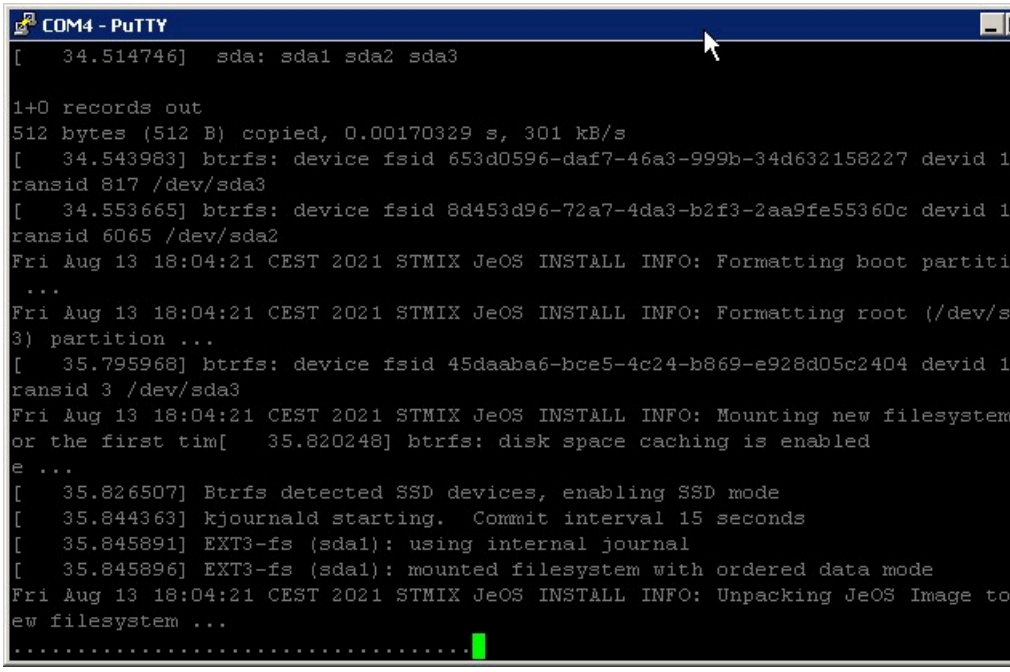


Figure 33: Image wird geschrieben

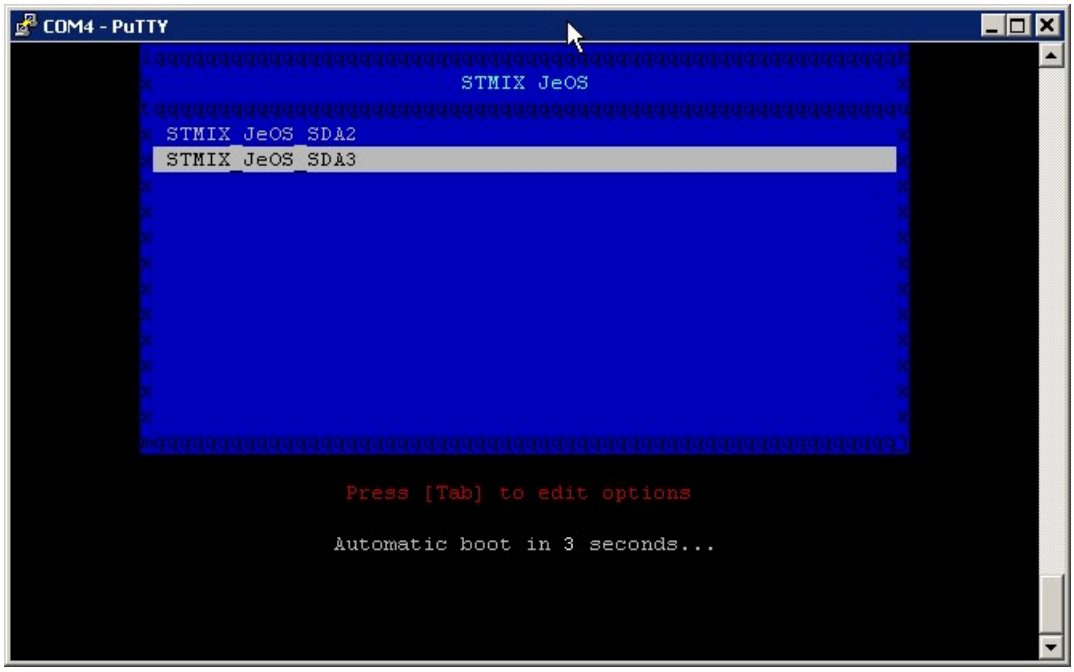


Figure 34: Automatischer Neustart

Auf SDA2 wird geschrieben, wenn SDA3 die letzte bekannte gute Partition war, die noch gebootet hat.

Auf SDA3 wird geschrieben, wenn SDA2 die letzte bekannte gute Partition war, die noch gebootet hat.

4) STMIX sollte nun von der soeben beschriebenen sda2/sda3 booten, die durch den Flashvorgang automatisch aktiviert wird (und bei entsprechender Konfiguration RMX READY wird).

NOTICE: Wenn Sie mehr als eine STMIX-Baugruppe hintereinander flashen, löschen Sie vor dem nächsten PXE-Bootvorgang den DHCP-Server-Cache (Registerkarte DHCP-Server im Programm tftpd, Rechtsklick auf die bereits verwendete Zuweisung und Löschen). Andernfalls wird die IP-Adresse 192.0.2.101 nicht erneut einer anderen MAC-Adresse zugewiesen.

2.11.6 STMIX- und STMIY-Werksreset

Die Werksreset-Prozedur für STMIX- und STMIY-Platinen wird über die WBM-Seite mit dem Pfad durchgeführt: **WBM>Wartung>Backup/Restore>Werksreset**.

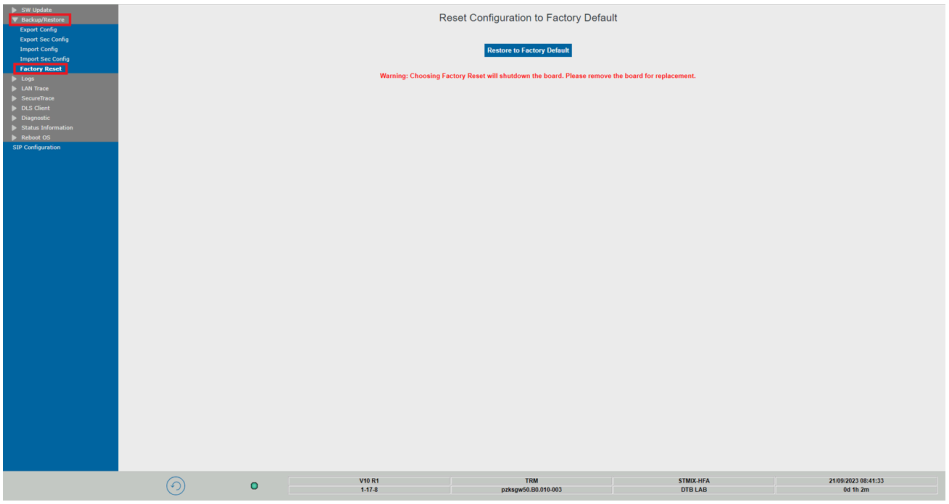


Abbildung 35: WBM-Seitenlayout

Die Aktion kann nur einmal ausgeführt werden, und nach dem Ende der Prozedur kann die Platine entfernt und an einem anderen Ort verwendet werden.

Beschreibung

1) Durch die Aktivierung von **Werksreset**, werden alle Verzeichnisse, die sensible Kundendaten enthalten, von der Platine gelöscht.

> **Anmerkung:** Einige Dateien werden durch Vorlagen gelöscht oder ersetzt (anfänglicher Status vor dem Hinzufügen einer kundenspezifischen Konfiguration).

2) Das Dateisystem wird dann mit SSD synchronisiert.
3) Alle Daten in den alternativen passiven Partitionen werden gelöscht.
4) Die Platine wird dann am Ende des Prozesses heruntergefahren und kann sicher entfernt werden.

2.12 Gateway HG 3575 - Ändern der mit AMO STMIB einstellbaren Parameter

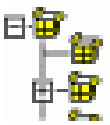
> **Wichtig:** Alle Einstellungen, die hier mit AMO vorgenommen werden können, sind im WBM nur lesbar!

Folgende Zweige werden unterstützt:

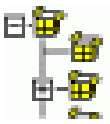
- TYP GLOBAL - Ändern des Ruhebitmusters
- TYP IFDATA - Ändern schnittstellenspezifischer Parameter des Access Point
- TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang
- TYP ASC - Ändern der Payload QoS-Einstellung des Access Points
- TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP Paketgröße, Voice Activity Detection und T.38 Fax
- TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen
- TYP DSP - Jitterbuffergröße des Access Points

- TYP DMCDATA - Ändern der Einstellung des Access Points für die Unterstützung von Direct Media Connections
- TYP H323 - Ändern der H323-Einstellungen des Access Points
- TYP JB - Konfiguration des Jitter-Buffers
- TYP SIGQOS - Qualitätsüberwachung für die Signalisierungsverbindung über IP
- TYP SNMP - Ändern der Community Strings für Lesezugriff
- TYP MGNTDATA - Management Data und Backup-Server
- TYP WBMDATA - Ändern von Login und Passwort für WBM
- TYP GWSECTOR - Ändern der Sektor-Nummer des Access Points für den Resource Manager
- TYPE DLSDATA - Konfigurieren von DLS Data
- Rücksetzen der Parameter auf Default-Werte

2.12.1 TYP GLOBAL - Ändern des Ruhebitmusters

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** Ruhebitmuster eingeben und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYPE=NCUI2, LTU=99, SLOT=99,TYPE=GLOBAL, PATTERN=213;`

Damit diese Änderung im Access Point wirksam wird, muss dieser aus- und wieder eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=UPDATAP,LTU=99;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt! Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

2.12.2 TYP IFDATA - Ändern schnittstellenspezifischer Parameter des Access Point

Die Einstellungen können sich von Access Point zu Access Point durchaus unterscheiden.

Eingestellt werden können Parameter

- der physischen Ethernet-Schnittstelle [`BITRATE`]
- der QoS-Unterstützung auf Schicht 2 nach IEEE 802.1 q/q [`VLAN, VLANID`]
- der QoS-Unterstützung auf Schicht 3 nach IETF RFC 2474 (DiffServ) [`TOSLAN, TOSMODEM`]

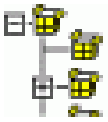
Die Ethernet-Schnittstelle **muss** bei beiden beteiligten Schnittstellenpartnern (HG 3575 bzw. LAN-Switch, -Router) **identisch** eingestellt werden!

Wichtig: Die feste Einstellung eines Schnittstellenpartners führt zusammen mit der „Autonegotiate“ Einstellung des anderen Partners zu Problemen. Fehlerhafte Einstellungen können vom System meist nicht erkannt und daher nicht gemeldet werden. Gerade wenn ein Gerät auf vollduplex, das andere auf halbduplex arbeitet, ist das nicht sofort bemerkbar. Unter hoher Last wird das auf halbduplex eingestellte Gerät verstärkt späte Kollisionen melden und die Paketverzögerung steigt stark an. Unterstützt der LAN-Port, mit dem die HG 3575 verbunden ist, keine Autonegotiation, oder funktioniert diese nicht zuverlässig, so muss die Ethernet-Schnittstelle der HG 3575 auf feste Werte eingestellt werden.

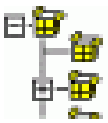
Nur wenn alle Router im Netzsegment des Access Points VLAN-Tagging unterstützen, darf VLAN-Tagging auch eingeschaltet werden. Ähnliches gilt für die DiffServ CodePoints. Unterstützen die Router kein DiffServ, müssen die Standard TOS-Werte ohne DiffServ eingestellt werden. Wird DiffServ unterstützt - aber nicht die CodePoints, so müssen die vom Netzbetreiber festgelegten Werte eingestellt werden.

Da bestimmte Hersteller von Netzwerkkomponenten entgegen IEEE 802.1p/q die Priorisierung nur mit VLAN-ID > 0 unterstützen, kann auch die VLAN-ID eingestellt werden. Generell gilt, dass von der HG 3575 Baugruppe bei aktiviertem VLAN-Schalter die Priorisierungsbits gesetzt werden. Werte siehe Tabelle 3 „TOS-Werte“. Laut Standard muss dann die VLAN-ID auf Null gesetzt sein, was mit der Standardeinstellung auch geschieht.

Im Beispiel werden VLAN-Tagging ausgeschaltet (auf den Default-Wert zurückgesetzt), die Standard TOS-Werte ohne DiffServ gesetzt (siehe dazu Tabelle 3 „TOS-Werte“, sowie die Ethernet-Schnittstelle auf 10 MBit/s Halbduplex eingestellt.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Quality of Service** unter Layer 2 und Layer 3 die TOS-Bytes eingeben. Auf Registerkarte **Ethernet-Schnittstelle** Übertragungsgeschwindigkeit und Modus einstellen und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYPE=NCUI2, LTU=99, TYP=IFDATA, VLAN=NEIN, TOSLAN=20,TOSMODEM=16, BITRATE=100MBFD;`

Damit diese Änderung im Access Point wirksam wird, muss dieser aus- und wieder eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=UPDATAP,LTU=99;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt! Vor dem `EXEC-USSU:UPDATAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

2.12.3 TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang

Die HG 3575 erlaubt den Anschluss eines TAP/Service PC über RS232/V.24 Schnittstelle.

Zwei Betriebsarten werden unterschieden:

- Terminal Mode
- Im Terminal-Mode wird über das Command Line Interface direkt mit der HG 3575 Loadware kommuniziert.

Wichtig: Zweistufiges CLI wird nicht unterstützt.

AENDERN-STMIB:MTYP=NCUI2,LTU=<LTU>,EBT=<EBT>,TYP=SERVIF,LOGINTRM=<Benutzer-

Login für Terminal-Mode>,LOGINPPP=<Benutzer-Login für PPP-Verbindung>,PASSW=<Passwort für Terminal-Mode>;

Die Standard-Login-Daten lauten:

Login: TRM (Parameter (**LOGINTRM**)

Passwort: PUBLIC (Parameter **PASSW**)

Nach erfolgreichem Login erscheint folgende Meldung:

Welcome to the HG 3575 V4.0 <LW-Version der aktuell geladenen LW> Command Line Interpreter.

vxTarget>

Eine Liste der verfügbaren Befehle kann nun über die lokale Hilfefunktion abgefragt werden, die über den Befehl `help` zur Verfügung steht.

- PPP Mode
- Im PPP-Mode wird über die HG 3575 unter der IP-Adresse, welche mit AMO APRT, Parameter **TAIPADR** eingestellt wurde, eine Verbindung des TAP/ Service PC in das Kundennetz hergestellt.

  Login (Standardeinstellung): PPP

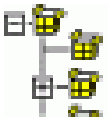
  Passwort: Es ist kein Passwort für PPP erforderlich!

Wichtig: Das eingerichtete Passwort kann aus Sicherheitsgründen nicht ausgelesen oder regeneriert werden. Beim Neu-Generieren einer Anlage aus dem REGEN-Stapel werden also die Passwörter gelöscht. Im

System eingerichtete Logins und Passwörter werden immer in Großbuchstaben konvertiert gespeichert.

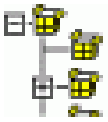
Diese 3 Parameter können pro Baugruppe unterschiedlich eingestellt werden.

Das Beispiel stellt für AP 17 die Logins auf TERMINAL und SURV, das Passwort auf HG3575 ein:

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Sicherheit** Benutzerdaten eingeben und auf **Sichern** klicken.

	`AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYPE=SERVIF,`
	
	`LOGINTRM=TERMINAL,LOGINPPP=SURV,PASSW2=HG3575;`

Damit diese Änderung im Access Point wirksam wird, muss dieser aus- und wieder eingeschaltet werden.

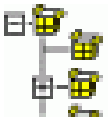
	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=UPDATAP,LTU=17;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt! Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

2.12.4 TYP ASC - Ändern der Payload QoS-Einstellung des Access Points

In diesem Zweig kann die Quality of Service für die Payload eines Access Points eingestellt werden. Die Einstellungen können sich von Access Point zu Access Point durchaus unterscheiden. Unterstützen die Router kein DiffServ, muss der Standard TOS-Wert ohne DiffServ eingestellt werden. Wird DiffServ unterstützt - aber nicht der CodePoint, so muss der vom Netzbetreiber festgelegte Wert eingestellt werden.

Im Beispiel wird für AP 99 der Standard TOS-Wert ohne DiffServ eingestellt (siehe dazu Tabelle 3 „TOS-Werte“.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Quality of Service** unter Layer 3-Diffserv TOS-Byte eingeben und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2,LTU=99,TYP=ASC,TOSPL=16;`

Diese Änderung wird unmittelbar auf den Access Point geladen und ohne Betriebsunterbrechung sofort wirksam.

2.12.5 TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP Paketgröße, Voice Activity Detection und T.38 Fax

Siehe auch Kapitel 14, „Codec-Einstellungen“.

Codec-Liste

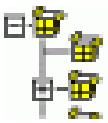
Die NCUI2 erlaubt es, dass Direct Media Connections von IP-Phones, Trunking Gateways oder HG 3500/75 Gateways vernetzter OpenScape 4000 Systeme auf der Baugruppe terminiert werden. Die Auswahl des Codec-Typs für DMC-Verbindungen geschieht anders als innerhalb IPDA nicht durch Classmarks, sondern durch eine Codec-Liste, auf der die beteiligten Partner sich über die unterstützten und bevorzugten Codec-Typen informieren.

Die HG 3575 unterstützt zwei Codec-Typen: G.711 und G.729

Die Reihenfolge der Nennung des Codec-Typs bestimmt die Präferenz. Der zuerstgenannte Typ wird bevorzugt.

Im Beispiel wird eingestellt, dass die NCUI2 G.711 und G.729 unterstützt, aber G.729 bevorzugt. Die Größe der Audio-Samples für G.711 und G.729A wird auf 60 ms eingestellt.

T.38 Fax

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** im Bereich **Direct Media Connection** unter **DMC Codec Liste G729**, **G711** auswählen und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2,LTU=99,TYP=ASC,,PRIO=PRIO1,CODEC=G729,R` `AENDERN-STMIB:MTYP=NCUI2,LTU=99,TYP=ASC,PRIO=PRIO2,CODEC=G711,RT`

Diese Änderung wird unmittelbar auf den Access Point geladen und ohne Betriebsunterbrechung sofort wirksam.

2.12.6 TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen



```
AENDERN-
STMIB:MTYP=NCUI2,LTU=99,TYP=ASC,RFCFMOIP=JA,RFCDTMF=JA,REDRFC
```

REDRFCTN	Redundante Übertragung der RFC2833 Töne nach RFC2198
RFCDTMF	Übertragung von DTMF Tönen nach RFC2833
RFCFMOIP	Übertragung von Fax/Modem Tönen nach RFC2833

Wichtig: Die oben genannten Parameter müssen in allen IPDA-Gateways (STMI2/4 respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

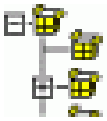
Mit der Einführung des Leistungsmerkmales „Codec-Umschaltung on the Fly“ in STMI4/NCUI4/OpenScape 4000 SoftGate ist **RFCMOIP=NEIN** in AMO CGWB und AMO STMIB die bessere Einstellung für Fax-/MOdem-Anrufe. Deshalb wurde die Standardeinstellung von JA auf NEIN geändert. Es besteht keine Notwendigkeit den Parameter in bestehenden Installationen zu ändern.

2.12.7 TYP DSP - Jitterbuffergröße des Access Points

Der Parameter JITBUFD ist nur wirksam, wenn der Parameter JBMODE im Zweig JB auf 0 (LEGACY MODE) steht.

2.12.8 TYP DMCDATA - Ändern der Einstellung des Access Points für die Unterstützung von Direct Media Connections

Mit diesen Parametern wird eingestellt, ob Direct Media Connections auf einer bestimmten HG 3575 erlaubt sind und wieviele davon gleichzeitig. Die Zählung erfolgt sowohl in der Software der OpenScape 4000 Zentrale, als auch auf der Baugruppe selber.



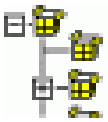
Configuration Management > Anlagendaten> IPDA > IPDA Access Point

Auf **Suchen** klicken und den Access Point auswählen.

Auf Registerkarte **Allgemein** unter **Direct Media Connection (DMC) enabled** eingeben und auf **Sichern** klicken.

	Der Access Point muss ausgeschaltet sein, wenn Sie den Wert für **DMCALLWD** ändern wollen.
	`DEACT-USSU:LTU=19;`
	Wenn man nur die Anzahl der DMC-Verbindungen (**DMCCONN**) ändert, muss der Access Point nicht ausgeschaltet werden.
	`AENDERN-STMIB:MTYP=NCUI2, LTU=99, TYP=DMCDATA,`**`DMCERL=JA, DMCCONN=30`**`;`

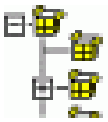
Damit diese Änderung wirksam wird, muss der Access Point neu gestartet bzw. wieder eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	Wenn DMCALLWD geändert wurde, muss der Access Point nun wieder eingeschaltet werden: `ACT-USSU:LTU=19;` Wenn man die Anzahl der DMC-Verbindungen (**DMCCONN**) geändert hat, muss ein UPDATAP für den Access Point durchgeführt werden: `EXEC-USSU:ART=UPDATAP,LTU=99;`

Wichtig: Beim UPDATAP werden die Verbindungen ohne weitere Nachfrage getrennt! Vor dem `EXEC-USSU:UPDATAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

2.12.9 TYP H323 - Ändern der H323-Einstellungen des Access Points

Direct Media Connections nutzen den H323 Fast-Connect-Mechanismus zum Verbindungsaufbau. Daher unterstützt die NCUI2/4- und STMI2/4-Plattform H.323. Es können zwei Timer des H.323-Stacks und der Gateway-Name verändert werden.

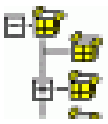
	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** unter **Direct Media Connection (DMC) enabled** eingeben und auf **Sichern** klicken.
	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=H323,Q931T1=50,` `Q931T2=500,GWNAME="HG3575-2";`

Diese Änderung wird unmittelbar auf den Access Point geladen und mit der nächsten H.323-Verbindung wirksam wird.

2.12.10 TYP JB - Konfiguration des Jitter-Buffers

Zur Konfiguration des Jitter-Buffers ist ein Grundverständnis der Arbeitsweise und der Konfigurationsparameter erforderlich. Lesen Sie dazu bitte Abschnitt 1.5, „Jitter-Buffer“.

Per Default ist der Delay-sparende, adaptive Jitter-Buffer (JBMODE=2) eingestellt.

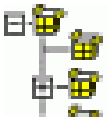
	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** unter **Jitter Buffer** die Parameter eingeben und auf **Sichern** klicken.

	`CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=JB,`
	`AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4,`
	`AVGDLYD=60,MAXDLYD=200,JBMODE=2;`

Diese Änderungen werden unmittelbar auf den Access Point geladen und sind mit der nächsten aufgebauten Verbindung wirksam.

2.12.11 TYP SIGQOS - Qualitätsüberwachung für die Signalisierungsverbindung über IP

Generierung

	**Configuration Management > Anlagendaten > IPDA > Access Point** Auf **Suchen** klicken, auf der Registerkarte **Quality of Service** im Bereich **Signaling Quality of Service** die gewünschten Parameter eintragen oder ändern, dann auf **Sichern** klicken.

	`AENDERN-`
	`STMIB:MTYP=NCUI2, LTU=99, TYP=SIGQOS, BANDW=40,`
	`MAXRTD=50`
	`0, MINTHRPT=30, SIGPTHSW=EXTEND, QOSSTAT=NEIN;`

Die Einstellung wird sofort wirksam.

Wichtig: Wenn die Bandbreite für das Shelf weniger als 64 kbit/s ist, dann sollte **BANDW** entsprechend spezifiziert werden. Wenn Signaling Survivability nicht installiert ist, dann sollte **SIGPTHSW=STD** verwendet werden.

2.12.12 TYP SNMP - Ändern der Community Strings für Lesezugriff

Die HG 3575 Baugruppe betreibt einen SNMP-Agenten, der über LAN angesprochen werden kann.

Der SNMP-Agent der HG 3575 unterstützt nur Lesezugriffe (READ-ONLY).

Zugangsberechtigung und Zugriffsrechte zu regelt der SNMP Agent über Community Strings.

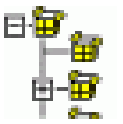
Ein MIB-Browser, der Anfragen an den SNMP-Agenten schickt, identifiziert sich als zugehörig zu einer Community. Die Community wird durch einen Community String identifiziert. Das ist ein einfacher, unverschlüsselter Text.

Die Standardeinstellung - und Vorbelegung für Community String 1 (CS1) - ist „public“, CS2 ist unwirksam.

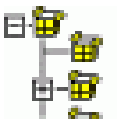
Diese Werte können verändert werden. Mittels CS2 kann einer zweiten Community der Lesezugriff auf den SNMP-Agenten gegeben werden.

Wird z.B. CS1=“ToP_SeCrEt23“ gesetzt und CS2=“11!$ZwY?“, so werden Zugriffe mit allen anderen Community Strings (auch „public“) abgewiesen.

For the parameters CS1 and CS2, all ASCII characters between «!» (exclamation mark, 33 Dec) and «~» (tilde, 126 Dec) are used with the exception of the characters «”» (34 Dec), «/» (47 Dec), «\» (92 Dec), and «^» (94 Dec). The space character « » (32 Dec) may not be used.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Sicherheit** unter **SNMP** eingeben und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2, LTU=99, TYP=SNMP, CS1=“ToP_SeCrEt23“, CS2=“11!$ZwY?“;`

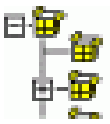
Damit diese Änderung im Access Point wirksam wird, muss dieser aus- und wieder eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`AUSSCHALTEN-USSU:LTG=1, LTU=99;` `EINSCHALTEN-USSU:EINHEIT=LTG, LTG=1, LTU=99;`

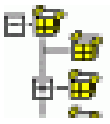
Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt!

CS1 kann nicht gelöscht werden. Zum Löschen von CS2 ist folgender Weg vorgesehen:

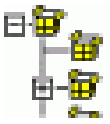
- Rücksetzen aller Parameter des AMO-Zweigs SNMP auf die Default-Werte (CS1=“public“, CS2 inaktiv)

	Das Initialisieren kann nur über den Expertenmodus angestoßen werden. **Expertenmodus > OpenScape 4000 > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`AENDERN-STMIB:MTYP=INITNCU2, LTU=99, TYP=SNMP;`

- Wiederherstellen des gewünschten Wertes von CS1

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Sicherheit** unter **SNMP** eingeben und auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2, LTU=99, TYP=SNMP,CS1="ToP_SeCrEt23";`

- Damit diese Änderung im Access Point wirksam wird, muss dieser aus- und wieder eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`AUSSCHALTEN-USSU:LTG=1, LTU=99;` `EINSCHALTEN-USSU:EINHEIT=LTG, LTG=1,LTU=99;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt!

2.12.13 TYP MGNTDATA - Verwaltungsdaten und Backup-Server

Für STMIB-Zweig **TYPE=MGNTDATA**, werden die folgenden Parameter nicht mehr verwendet: MGNTIP, MGNTPN, BUSIP und BUSPN. Sie werden von AMO STMIB ignoriert, wie in HINT 57 (H57) beschrieben.



```
<CHANGE-
STMIB:NCUI2,67,MGNTDATA,192.168.10.0,1024,192.168.10.1,1024;
H500:  AMO STMIB STARTED
H57: MGNTIP, MGNTPN, BUSIP & BUSPN ARE IGNORED AND DERIVED FROM
 AMO SIPCO

AMO-STMIB-111       CONFIGURATION OF HG3575-2 BOARDS

CHANGE COMPLETED;
  <
```

Die Assistant-IP-Adresse wird von SIPCO abgeleitet und nur angezeigt.



```
<DISPLAY-STMIB:MTYPE=NCUI2,LTU=67,TYPE=MGNTDATA;
H500:  AMO STMIB STARTED
+-----------------------------------------------------+
  NCUI2 BOARD DATA             SOCO1000
+-----------------------------------------------------+
  LTU = 67   SOURCE GROUP INDEX = 6

+-----------------------------------------------------+


  MANAGEMENT STATION AND BACK-UP SERVER

  ------------------------------------

  ASSISTANT IP   = 10.133.42.146 *

  UIMODE         = SECURITY (CLASSIC)

  * DERIVED FROM SIPCO

AMO-STMIB-111       CONFIGURATION OF HG3575-2 BOARDS

DISPLAY COMPLETED;
  <
```

2.12.14 TYP WBMDATA - Ändern von Login und Passwort für WBM

Der Zugang zum WBM kann in diesem Zweig konfiguriert werden.

	AENDERN-STMIB:MTYP=NCUI2, LTU=<LTU>, EBT=<EBT>, TYP=WBMDATA, LOGINWBM=<Benutzer-Login für WBM-Verbindung>, PASSWWBM=<Passwort für WBM-Verbindung>, ROLE=<Rolle des WBM-Benutzers; legt die Zugriffsrechte fest>;

Tabelle 10: WBM - Rechte

Rolle	Rechte
ADMIN	Administrator (Standardwert)
ENGR	Entwickler (Zugang zu allen Leistungsmerkmalen)
READONLY	Administrator mit nur Lesezugriff
SU	Superuser (Zugang zu allen Leistungsmerkmalen)

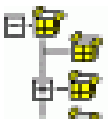
Die Login-Daten für die erstmalige Anmeldung als **engr** lauten:

Benutzername: `HP4K-DEVEL`

Passwort: `4K-admin`

2.12.15 TYP GWSECTOR - Ändern der Sektor-Nummer des Access Points für den Resource Manager

In diesem Zweig wird mit dem Parameter GWSECTNR dem HG 3575 Gateway eine Sektornummer im Sektorenkonzept des Resource Managers zugewiesen.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** die **Sektornummer des Gateways** eingeben und auf **Sichern** klicken.
	CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=GWSECTOR,GWSECTNO=7;

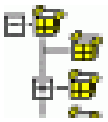
Diese Änderung wird ohne Betriebsunterbrechung sofort wirksam.

2.12.16 TYPE DLSDATA - Konfigurieren von DLS Data

	CHANGE-STMIB:MTYPE=NCUI2,LTU=99,TYPE=DLSDATA,DLSIPADR=<number>, DLSPORT=<number>,DLSACPAS=<param>;

2.12.17 Rücksetzen der Parameter auf Default-Werte

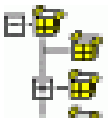
Sollen die Parameter eines oder aller Zweige der NCUI2/4-Daten auf Default-Werte zurückgesetzt werden - z.B. nach temporärer Änderung für Diagnosearbeiten - so kann dies im Zweig INITNCU2 gemacht werden. Das Beispiel setzt die ASC-Parameter alle auf Default-Werte.

	Das Initialisieren kann nur über den Expertenmodus angestoßen werden. **Expertenmodus > OpenScape 4000 > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`AENDERN-STMIB:MTYP=INITNCU2,LTU=17,TYP=ASC;`

Die Änderungen unter TYP ASC, DSP, H323, JB, SNMP, MGNTDATA, WBMDATA und DLSDATA **werden sofort und ohne Betriebsunterbrechung wirksam**.

Änderungen unter TYP GLOBAL, IFDATA, SERVIF, DMCDATA und SIGQOS **werden wirksam nachdem der Access Point neu geladen wurde**.

Dies gilt auch für das Kommando `AENDERN-STMIB:MTYP=INITNCU2,LTU=17,TYP=ALLE;`. Deshalb wird empfohlen nach einem Rücksetzen aller Parameter den Access Point neu zu laden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=UPDATAP,LTU=17;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt! Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

2.13 Hinweise zum Einrichten eines Common Gateways HG 3500

2.13.1 Änderungen der Common Gateway Konfiguration

Bitte beachten Sie, dass bei Konfigurationsänderungen die gesamte Baugruppe neu zu konfigurieren ist!

2.13.2 AMOs

- Die Konfiguration der STMI-Baugruppen erfolgt dies mit dem AMO CGWB bzw. wenn IPDA eingestellt wurde auch mit dem AMO BCSU (siehe Kapitel 15, „Multiple Feature Support Konfiguration am Common Gateway (Beispiel)“).
- Die Konfiguration der NCUI-Baugruppe erfolgt wie gewohnt mit dem AMO STMIB.
- Der AMO BFDAT wird für die Blockkonfiguration verwendet.
- Das Zusammenlegen der Funktionen auf eine Baugruppe erfolgt mit dem AMO BCSU.
- Der DB Line Bereich für ein Baugruppe muss durchgehend sein.
- Alle HG 3500 Baugruppen müssen am OpenScape 4000 LAN Segment angeschlossen sein.
- Die für eine Baugruppe konfigurierten Lines, sind nachträglich nicht mehr änderbar, d.h. wenn Sie zusätzliche Lines auf einer Baugruppe benötigen, müssen Sie die gesamte Baugruppe neu konfigurieren.
- Der Parameter FCTID im AMO BCSU muss immer auf 1 gesetzt werden.

2.13.3 Regeln

- Der Parameter für den Funktionsblock (**FCTBLK**) kann frei vergeben werden, er darf nur noch nicht belegt sein.
- Ein abgeschlossener (fertig konfigurierter) Funktionsblock kann einer oder mehreren Baugruppen zugeordnet werden.
- Der Parameter für die zu verwendende Baugruppe (**BGBKAN**) legt fest, wie viele B-Kanäle der Baugruppe maximal zur Verfügung stehen.
- Setzt man hier den Wert **BKAN60&BKAN120**, so kann eine STMI[3] mit 60- oder 120-B-Kanälen verwendet werden. Dieser Wert ist auch dann von Vorteil, wenn eine kleine STMI mit 60 B-Kanälen defekt wird. Dann kann diese auch durch eine große STMI mit 120 B-Kanälen ersetzt werden. Umgekehrt, eine große STMI durch eine kleine ersetzen, geht nicht.
- Parameter **ANZEINH**
  - 1 Einheit entspricht 10 B-Kanälen
  - Wird die Anzahl der Einheiten (**ANZEINH**) bei der Konfiguration nicht angegeben, werden 10 B-Kanäle (also **ANZEINH=1**) pro Satz konfiguriert.
  - Pro Satz können maximal 3 Einheiten angegeben werden.
  - Die Anzahl der Sätze (**ANZSATZ**) multipliziert mit den der Anzahl der Einheiten (**ANZEINH**) entsprechenden B-Kanälen, ergibt die maximale Anzahl der B-Kanäle für die Funktion. Beispiel: ANZSATZ=4, ANZEINH=3. 4 mal 3 mal 10 ist gleich 120 B-Kanäle.
- Soll eine IPDA-Funktion (HG3570) bei einer Multiple-Feature-Konfiguration eingerichtet werden, so muss diese als erste konfiguriert werden.
- Für **IPDA** muss nur die Anzahl der B-Kanäle (**ANZBKAN**) angegeben werden.
- Für **IP-Trunking** muss die Anzahl der Sätze (**ANZSATZ**) und die Anzahl der Einheiten (**ANZEINH**) angegeben werden.

[3] STMI steht für STMI2 (Q2316-X, Q2316-X10) und STMI4 (Q2324-X500,Q2324-X510)

- Für **HFA** und **SIP** mus die Anzahl der Sätze (**ANZSATZ**) und die Anzahl der B-Kanäle (**ANZBKAN**) angegeben werden.

  Wichtig: Werden auch reservierte HFA- oder SIP-Sätze konfiguriert, so müssen die dafür vorgesehenen B-Kanäle hier mitangegeben werden. Bei reservierten trunk-Sätzen ist das nicht nötig, da die Zuordnung über die Anzahl der Einheiten (**ANZEINH**) erfolgt.

- Für **WAML** muss nur die Anzahl der Einheiten (**ANZEINH**) angegeben werden.

  Wichtig: Für WAML ist nur ein Satz möglich! Ist **ANZEINH=1** dann kann dieser Parameter weggelassen werden!

- **Reserve-Funktion**
- Da eine Änderung der Baugruppenkonfiguration nur durch Löschen der Baugruppe möglich ist, wurde die Möglichkeit geschaffen Sätze für spätere Verwendung zu reservieren. Wenn dieses Leistungsmerkmal für die Funktionen HG3530, HG3540 oder HG3550 genutzt werden soll, muss die entsprechende Funktion direkt nach der eigentlichen Funktion konfiguriert sein, also z.B. HG3550&HG3550R. Die Reserve-Funktion muss immer nach der eigentlichen Funktion (also am Ende) stehen!

  Die Kombination HG3550&HG3530&HG3550R ist nicht zugelassen, da sonst ein unzulässiger Sprung in der Satz-Aufteilung entstehen würde (Trunk - HFA - Trunk).

  Das Einrichten mehrerer Reserve-Funktionen auf einer Baugruppe ist nicht möglich!

  Die reservierten Sätze können später mit

  AENDERN-
  BCSU:ART=IPGW,LTU=<LTU>,EBT=<ebt>,UMWRESLN=<anzahl>;

  /*<anzahl>: Anzahl der Sätze, die in verwendbare Sätze umgewandelt werden sollen

  in verwendbare Sätze umgewandelt werden.

  Wichtig: Danach ist ein Reset der Baugruppe durchzuführen! `RESET-BSSU:ADRART=LAGE,LTU=<ltu>,EBT=<ebt>;`

- Die Funktion **STANDBY** kann nur als Einzel-Funktion konfiguriert werden.
- Es sind 11 Single Feature Standard-Profile angelegt in der Datenbasis eingerichtet (siehe AMO-Beschreibung, AMO BFDAT).

- Die Konfiguration eines Funktionsblockes wird mit
- `AENDERN-BFDAT:CONFIG=OK,FCTBLK=<nummer>,ANTW=JA;`

  abgeschlossen.

  Der Status kann mit `ABFRAGEN-BFDAT:FCTBLK=<nummer>;` abgefragt werden.

  Ist die Konfiguration eines Funktionsblockes abgeschlossen worden, so ist der **STATUS=OK**.

  Wird nach Abschluss der Block-Konfiguration in dieser ein Fehler festgestellt, so muss dieser Funktionsblock gelöscht werden (`LOESCHEN-BFDAT:FCTBLK=<nummer>,ANTW=JA;`) und neu eingerichtet werden.

  Ist die Konfiguration eines Funktionsblockes nicht abgeschlossen worden, so ist der **STATUS=WEITER**. Der Funktionsblock kann nicht einer Baugruppe zugewiesen werden. Das wird durch den AMO BCSU mit der **Fehlermeldung F89** abgewiesen.

  F89: DER ANGEGEBENE FUNKTIONS-BLOCK IST NOCH NICHT VOLLSTAENDIG KONFIGURIERT.

  BITTE DIE KONFIGURATION ZUERST MIT AMO-BFDAT ABSCHLIESSEN.

2.13.4 Einschränkungen

- Pro Baugruppe kann nur ein Trunking-Protokoll eingerichtet werden (AMO CGWB). Mischung mit anderen Funktionen ist uneingeschränkt möglich.
- Bei Konfigurationsänderungen muss die gesamte Baugruppe neu konfiguriert werden.

2.13.5 Konfigurationsschritte im Überblick

Nachfolgend die Konfigurationsschritte für ein Common Gateway HG 3500 im Überblick:

1) Funktionsblöcke konfigurieren mit AMO BFDAT (Assistant: **Configuration Management > Anlagendaten > Baugruppe > CGW-Funktionsblock**)
2) Den Funktionsblock einer Baugruppe zuweisen mit AMO BCSU (Assistant: **Configuration Management > Anlagendaten > Baugruppe > Baugruppe**)
3) Leistungsmerkmale administrieren mit AMO CGWB

2.14 Gateway HG 3500 - Ändern der mit AMO CGWB einstellbaren Parameter

---

Wichtig: Alle Einstellungen, die hier mit AMO vorgenommen werden können, sind im WBM nur lesbar!

Folgende Zweige werden unterstützt:

- TYP ASC - Ändern der Payload QoS-Einstellung im Host System
- TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP-Paketgröße und Voice Activity Detection

- TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen
- TYP DMCDATA - Ändern der Einstellung der HG 3500 für die Unterstützung von Direct Media Connections
- TYP DSP - Ändern der DSP (Signalprozessor)-Einstellung einer HG 3500
- TYP GLOBIF - Ändern des Ruhebitmusters und schnittstellenspezifischer Parameter
- TYP GWSECTOR - Ändern der Sektor-Nummer der HG 3500 für den Resource Manager
- TYP MGNTDATA - Verbindung zum OpenScape 4000 Assistant
- TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang
- TYP WBMDATA - Ändern von Login und Passwort für WBM
- TYP JB - Konfiguration des Jitter-Buffers
- Rücksetzen der Parameter auf Default-Werte

2.14.1 TYP ASC - Ändern der Payload QoS-Einstellung im Host System

In diesem Zweig kann die Quality of Service für die Payload eines Access Point eingestellt werden. Die Einstellungen können sich von HG 3500 zu HG 3500 durchaus unterscheiden. Unterstützen die Router kein DiffServ, muss der Standard TOS-Wert ohne DiffServ eingestellt werden. Wird DiffServ unterstützt - aber nicht der CodePoint, so muss der vom Netzbetreiber festgelegte Wert eingestellt werden.

Im Beispiel wird für die HG 3500 in der LTU 5, Einbauteilung 91 der Standard TOS-Wert ohne DiffServ eingestellt (siehe dazu Tabelle 3, „TOS-Werte“).

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf der Registerkarte **Anlagendaten** unter **Payload-Verbindungen** Einstellungen vornehmen und auf **Sichern** klicken.
	`AENDERN-CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=ASC,TOSPL=16;`

Diese Änderung wird unmittelbar in die Baugruppe geladen und ohne Betriebsunterbrechung sofort wirksam.

2.14.2 TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP-Paketgröße und Voice Activity Detection

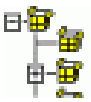
Siehe auch Kapitel 14, „Codec-Einstellungen“.

Die Parameter dieses Zweigs gelten nur für eine HG 3500 Baugruppe. Deshalb könnte jede HG 3500 Baugruppe in einem OpenScape 4000 System anders eingestellt werden.

Um das System handhabbar und diagnostizierbar zu halten, müssen diese Parameter aber für alle HG 3500 Baugruppen mit FUNCTION=HG3570 identisch eingestellt werden.

Im Beispiel wird für das Common Gateway HG 3500 1-5-91 die Größe der Audio-Samples für G.711 und G.729 auf 60 ms eingestellt. Das bedeutet

hohes Paketierungsdelay, aber vergleichsweise niedrigen Bedarf an Übertragungsbandbreite.

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und **STMI** auswählen. Auf der Registerkarte **STMI Baugruppendaten** die Zeiten für G.711 und G.729 einstellen und auf **Sichern** klicken.

	`AENDERN-`
	`CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=ASC,PRIO=PRIO1,CO-`
	`DEC=G711,RTP=60;`
	`AENDERN-`
	`CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=ASC,PRIO=PRIO2,CO-`
	`DEC=G729,RTP=60;`

Diese Änderungen werden unmittelbar auf die HG 3500 geladen und ohne Betriebsunterbrechung sofort wirksam.

2.14.3 TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen

	`AENDERN-`
	`CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=ASC,RFCFMOIP=JA,RFC-`
	`DTMF=JA,REDRFCTN=JA;`

REDRFCTN	Redundante Übertragung der RFC2833 Töne nach RFC2198
RFCDTMF	Übertragung von DTMF Tönen nach RFC2833
RFCFMOIP	Übertragung von Fax/Modem Tönen nach RFC2833

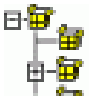
Wichtig: Die oben genannten Parameter müssen in allen IPDA-Gateways (STMI2/4 respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

Mit der Einführung des Leistungsmerkmales „Codec-Umschaltung on the Fly“ in STMI4/NCUI4/OpenScape 4000 SoftGate, ist **RFCMOIP=NEIN** in AMO CGWB und AMO STMIB die bessere Einstellung für Fax-/MOdem-Anrufe. Deshalb wurde die Standardeinstellung von JA auf NEIN geändert. Es besteht keine Notwendigkeit den Parameter in bestehenden Installationen zu ändern.

2.14.4 TYP DMCDATA - Ändern der Einstellung der HG 3500 für die Unterstützung von Direct Media Connections

Mit diesem Parameter wird eingestellt, wieviele Direct Media Connections auf einer bestimmten HG 3500 gleichzeitig erlaubt sind. Die Zählung erfolgt sowohl

in der Software der OpenScape 4000 Zentrale, als auch auf der Baugruppe selber.

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und **STMI** auswählen. Auf der Registerkarte **STMI Baugruppendaten** unter **Anzahl DMC-Verbindungen** Einstellungen vornehmen und auf **Sichern** klicken. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** Auf **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`AENDERN-CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=DMCDATA,DMCCONN=30; Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit`
	
	`RESTART-BSSU:ADRART=LAGE,LTU=5,EBT=91; neu geladen werden.`

Wichtig: Bestehende **Verbindungen werden dadurch getrennt.**

2.14.5 TYP DSP - Ändern der DSP (Signalprozessor)-Einstellung einer HG 3500

Der Parameter **JITBUFD** ist nur wirksam, wenn der Parameter JBMODE im Zweig JB auf 0 (LEGACY MODE) steht.

Der Parameter **VADEN** ist nicht mehr gültig. Bitte nutzen Sie für die Konfiguration der Voice Activity Detection den Parameterzweig TYP=ASC, Parameter VAD (siehe Kapitel 13.2, „TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP-Paketgröße und Voice Activity Detection“).

2.14.6 TYP GLOBIF - Ändern des Ruhebitmusters und schnittstellenspezifischer Parameter

Die Einstellung der physikalischen Ethernet-Schnittstelle kann für individuelle HG 3500 unterschiedlich sein.

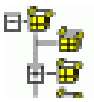
Die Ethernet-Schnittstelle muss bei beiden beteiligten Schnittstellenpartnern (HG 3500 bzw. LAN-Switch, -Router) identisch eingestellt werden!

Wichtig: Die feste Einstellung eines Schnittstellenpartners führt zusammen mit der „Autonegotiate“ Einstellung des anderen Partners zu Problemen. Fehlerhafte Einstellungen können

vom System meist nicht erkannt und daher nicht gemeldet werden. Gerade wenn ein Gerät auf vollduplex, das andere auf halbduplex arbeitet, ist das nicht sofort bemerkbar. Unter hoher Last wird das auf halbduplex eingestellte Gerät verstärkt späte Kollisionen melden und die Paketverzögerung steigt stark an. Unterstützt der LAN-Port, mit dem die HG 3500 verbunden ist, keine Autonegotiation, oder funktioniert diese nicht zuverlässig, so muss die Ethernet-Schnittstellen der HG 3500 auf feste Werte eingestellt werden.

Die Einstellung der QoS-relevanten Parameter erfolgt für alle HG 3500-Baugruppen zusammen mit SL100/200 identisch über den AMO SIPCO.

Im Beispiel wird die Ethernet-Schnittstelle auf 10 MBit/s Halbduplex und das Ruhebitmuster auf 213 eingestellt.

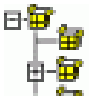
	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und **Baugruppenname=STMI2** oder **Baugruppenname=STMI4** auswählen. Auf Registerkarte **STMI Baugruppendaten** entsprechende Einstellungen vornehmen und auf **Sichern** klicken. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`CHANGE-CGWB:MTYPE=CGW,LTU=5,SLOT=91,TYPE=GLOBIF,PATTERN=213, BI-TRATE=100MBFD;`
	`Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit`
	`RESTART-BSSU:ADRART=LAGE,LTU=5,EBT=91; neu geladen werden.`

Wichtig: Bestehende **Verbindungen werden dadurch getrennt.**

2.14.7 TYP GWSECTOR - Ändern der Sektor-Nummer der HG 3500 für den Resource Manager

In diesem Zweig wird mit dem Parameter GWSECTNR dem HG 3500 Gateway eine Sektornummer im Sektorenkonzept des Resource Managers zugewiesen.

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und **STMI** auswählen. Auf der Registerkarte **STMI Baugruppendaten** unter **Sektornummer des Gateway** entsprechende Einstellungen vornehmen und auf **Sichern** klicken.
	AENDERN- CGWB:MTYP=CGW,LTU=5,EBT=91,TYP=GWSECTOR,GWSECTNR=1;

Diese Änderung wird ohne Betriebsunterbrechung sofort wirksam.

2.14.8 TYP MGNTDATA - Verbindung zum OpenScape 4000 Assistant

Für CGWB-Zweig **TYPE=MGNTDATA**, werden die folgenden Parameter nicht mehr verwendet: MGNTIP, MGNTPN, BUSIP und BUSPN.

Sie werden von AMO CGWB ignoriert, wie in HINT 76 (H76) beschrieben.



```
<CHANGE-
CGWB:CGW,1,14,MGNTDATA,192.168.10.0,1024,192.168.10.1,1024;
H500:  AMO CGWB  STARTED
H76: MGNTIP, MGNTPN, BUSIP & BUSPN ARE IGNORED AND DERIVED FROM
 AMO SIPCO

AMO-CGWB -111       CONFIGURATION OF HG3500 BOARD

CHANGE COMPLETED;
  <
```

Die Assistant-IP-Adresse wird von SIPCO abgeleitet und nur angezeigt.



```
<DISPLAY-CGWB:LTU=1,SLOT=14,TYPE=MGNTDATA;
H500:  AMO CGWB  STARTED
------------------------------------------------------------
|  CGW BOARD DATA                                          |
------------------------------------------------------------
|   HG3530     SIP         HG3550            HG3570       |
------------------------------------------------------------
|   LTU = 1    SLOT = 14   SMODE = NORMAL    POOLNO: 0    |
------------------------------------------------------------


  MANAGEMENT STATION AND BACK-UP SERVER

  -------------------------------------

  ASSISTANT IP   = 10.133.42.146 *

  UIMODE         = SECURITY (CLASSIC)

  * DERIVED FROM SIPCO

AMO-CGWB -111       CONFIGURATION OF HG3500 BOARD

DISPLAY COMPLETED;
  <
```

2.14.9 TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang

Mit dem Parameterzweig TYP=SERVIF können Sie die Zugangsdaten für das Command Line Interface festlegen.

Mehr Informationen zum CLI finden Sie im Kapitel 18, „Command Line Interface CLI beim HG 3500“.



```
AENDERN-
CGWB:MTYP=CGW,LTU=<LTU>,EBT=<EBT>,TYP=SERVIF,LOGINTRM=<Be-
nutzer-Login für Terminal-Mode>,PASSW=<Passwort
 für Terminal-Mode>;
```

Die Standard-Login-Daten lauten:

Login: TRM (Parameter (**LOGINTRM**)

Passwort: PUBLIC (Parameter **PASSW**)

2.14.10 TYP WBMDATA - Ändern von Login und Passwort für WBM

Der Zugang zum WBM kann in diesem Zweig konfiguriert werden.

	AENDERN- CGWB:MTYP=CGW,LTU=<LTU>,EBT=<EBT>,TYP=WBMDATA,LOGINWBM=< nutzer-Login für WBM- Verbindung>,PASSWWBM=<Passwort für WBM- Verbindung>,ROLE=<Rolle des WBM-Benutzers; legt die Zugriffsrechte fest>;

Tabelle 11: WBM - Rechte

Rolle	Rechte
ADMIN	Administrator (Standardwert)
ENGR	Entwickler (Zugang zu allen Leistungsmerkmalen)
READONLY	Administrator mit nur Lesezugriff
SU	Superuser (Zugang zu allen Leistungsmerkmalen)

Die Login-Daten für die erstmalige Anmeldung als **engr** lauten:

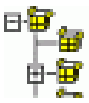
Benutzername: `HP4K-DEVEL`

Passwort: `4K-admin`

2.14.11 TYP JB - Konfiguration des Jitter-Buffers

Zur Konfiguration des Jitter-Buffers ist ein Grundverständnis der Arbeitsweise und der Konfigurationsparameter erforderlich. Lesen Sie dazu bitte Kapitel 1.5, „Jitter-Buffer“.

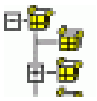
Per Default ist der Delay-sparende, adaptive Jitter-Buffer eingestellt.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** unter **Jitter Buffer** die Parameter eingeben und auf **Sichern** klicken.
	CHANGE-CGWB:MTYPE=CGWB,LTU=5,SLOT=91,TYPE=JB, AVGDLYV=40,MAXDLYV=120,MINDLYV=20,PACKLOSS=4, AVGDLYD=60,MAXDLYD=200, JBMODE=2;
WBM	**Konfiguration > Payload > HW-Module > DSP Jitter-Einstellungen bearbeiten**

Diese Änderungen werden unmittelbar auf den Access Point geladen und sind mit der nächsten aufgebauten Verbindung wirksam.

2.14.12 Rücksetzen der Parameter auf Default-Werte

Sollen die Parameter eines oder aller Zweige der STMI2/4-Daten auf Default-Werte zurückgesetzt werden - z.B. nach temporärer Änderung für Diagnosearbeiten - so kann dies im Zweig INITCGW gemacht werden. Das Beispiel setzt die DMCDATA-Parameter alle auf Default-Werte.

	Das Initialisieren und eventuell notwendige Nachladen kann nur über den Expertenmodus ausgeführt werden. **Expertenmodus > OpenScape 4000 > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`AENDERN-` `CGWB:MTYP=INITCGW,LTU=5,EBT=91,TYP=DMCDATA;`

Die Änderungen unter TYP ASC, DSP, MGNTDATA, SIPTRERH, WBMDATA, DLSDATA (DLSACPAS) und JB **werden sofort** und ohne Betriebsunterbrechung wirksam.

Änderungen unter TYP DMCDATA, GKDATA, GLOBIF, GWDATA, GWSECTOR, H235DATA, SIPTRSSA und DLSDATA (DLSIPADR & DLSPORT) **werden erst wirksam, nachdem die HG 3500** mit `RESTART-BSSU:ADRART=LAGE,LTU=5,EBT=91;` neu geladen wurde

Wichtig: Bestehende **Verbindungen werden dabei getrennt.**

2.15 Codec-Einstellungen

2.15.1 HFA und Trunking

Im AMO CGWB für HG 3500 und entsprechend im AMO STMIB für HG 3575 wird eine Prioritätsliste der Codecs eingerichtet. Auf die so konfigurierten Codecs greifen die Gatways bei Codec-Verhandlungen zurück.

Beispiele:

- Gateway ist ein DMC-Endpunkt
- Master-Verbindungen bei HFA und IP-Trunking

Beispiel

- HG 3500 (STMI)

```
AENDERN-
GWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,UDPPRTLO=29100,TOSPL=0,TOSS
IGNL=0,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,REDRFCTN=JA,PRIO=PRIO
1,CODEC=G711,VAD=JA,RTP="20";
AENDERN-
```

```
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO2,CODEC=G711U,VAD
=JA,RTP="20";
AENDERN-
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO3,CODEC=G729A,VAD
=NEIN,RTP="20";
AENDERN-
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO4,CODEC=G729B,VAD
=JA,RTP="20";
AENDERN-
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO5,CODEC=G729AB,VA
D=JA,RTP="20";
AENDERN-
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO6,CODEC=NONE,VAD=
NEIN,RTP="20";
AENDERN-
CGWB:MTYP=CGW,LTU=3,EBT=11,TYP=ASC,PRIO=PRIO7,CODEC=NONE,VAD=
NEIN,RTP="20";
```

- HG 3575 (NCUI)

```
AENDERN-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,TOSPL=48,PRIO=PRIO1,CODEC=G71
1,VAD=JA,RTP="20";
AENDERN-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO2,CODEC=G711U,VAD=JA
,RTP="20";
AENDERN-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO3,CODEC=G729AB,VAD=J
A,RTP="40";
AENDERN-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO4,CODEC=G729B,VAD=JA
,RTP="20";
AEND-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO5,CODEC=NONE;
AEND-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO6,CODEC=NONE;
AEND-
STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO7,CODEC=NONE;
```

2.15.2 IPDA

Bei IPDA werden die Codecs für die Master-Verbindung vom DNIL geschalten und im AMO SDAT / AMO TDCSU etc. konfiguriert, also in den Teilnehmer/ Satzdaten der beteiligten Geräte (siehe „IP Distributed Architecture (IPDA))“ > Abschnitt 2.4, „Teilnehmersätze in Access Points“).

Wichtig: Das heißt, dass eine Konfiguration der Codecs im AMO CGWB und AMO STMIB für die IPDA-masterverbindung nicht notwendig ist!

Für IPDA-Verbindungen werden die Codecs wie zuvor beschrieben im AMO STMIB bzw. AMO CGWB konfiguriert (siehe auch Abschnitt 11.5, „TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP Paketgröße, Voice Activity Detection und T.38 Fax“, Abschnitt 13.2, „TYP ASC - Einstellen der Codec-Liste für DMC-Verbindungen, RTP-Paketgröße und Voice Activity

Detection“ bzw. Abschnitt 11.6, „TYP ASC - Übertragung von DTMF-/Fax-/Modem-Tönen“).

Wichtig: Die Parameter **RFCFMOIP**, **RFCDTMF** und **REDRFCTN** im Zweig **TYP=ASC** müssen in allen IPDA-Gateways (STMI2/4 respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

2.16 Multiple Feature Support Konfiguration am Common Gateway (Beispiel)

2.16.1 Wichtige Hinweise / Einschränkungen

- **IPDA** Wenn die Funktion IPDA (HG3570) auf einer STMI-Baugruppe eingerichtet wurde, dann muss die IP-Adresse des Common Gateways mit dem AMO BCSU zugewiesen werden. Für alle anderen Funktionen der Baugruppe muss die IP-Adresse mit dem AMO CGWB zugewiesen werden.
- **IPDA** Sind in einem Funktionsblock mehrere Funktionen definiert (IPDA und weitere), dann muss für IPDA die IP-Adresse mit dem AMO BCSU konfiguriert werden, für die anderen Fnktionen muss die **selbe** IP-Adresse mit dem AMO CGWB konfiguriert werden!
- **VLAN-Einstellungen** in AMO CGWB: Wenn MFS konfiguriert ist, werden die folgenden AMOs genutzt:
  - MFS mit IPDA-Funktionalität: AMO SIPCO
  - MFS ohne IPDA-Funktionalität: AMO CGWB
- **Trunking-Protokolle** Es darf nur ein Trunking-Protokoll pro Common Gateway Baugruppe konfiguriert werden (also entweder SIP oder H323)! Sollen beide Protokolle für Trunking verwendet werden, müssen eigene Baugruppen verwendet werden.
- **IPDA/WAML** Keine Unterstützung von WAML- **und** HG3570 (IPDA)-Funktion auf **einer** Common Gateway Baugruppe, da es sonst zu Halbwegen bei APNW Access Points kommen kann.

2.16.2 Konfiguration der Funktionsblöcke mit AMO BFDAT

- Funktionsblock 1: IPDA (HG3570)
- Funktionsblock 2: IPDA (HG3570), IP-Trunking (HG3550) und HFA-Teilnehmer (HG3530)
- Funktionsblock 3: IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)
- Funktionsblock 4: IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)
- Funktionsblock 5: IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)
- Funktionsblock 6: IP-Trunking (HG3550) und HFA-Teilnehmer (HG3530)

- Funktionsblock 7: IP-Trunking, HFA-Teilnehmer (HG3530) und Reserve HFA-Teilnehmer (HG3530R)

Funktionsblock 1

/* Funktionsblock 1: Einrichten der Funktion IPDA (HG3570)
```
EINR-BFDAT:FCTBLK=1,FUNCTION=HG3570,BGBKAN=BKAN120;
```

>>>>> IPDA mit 120 B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3570,ANZBKAN=120;
```

>>>>> Konfiguration dieses Blockes beenden
```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA;
```

Funktionsblock 2

/* Funktionsblock 2: Einrichten der Funktionen IPDA (HG3570), IP-Trunking (HG3550) und HFA-Teilnehmer (HG3530)
```
EINR-
BFDAT:FCTBLK=2,FUNCTION=HG3570&HG3550&HG3530,BGBKAN=BKAN;
```

>>>>> IPDA mit 30 B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=2,FUNCTION=HG3570,ANZBKAN=30;
```

>>>>> IP-Trunking mit einem Satz mit drei Einheiten (=30 B-Kanälen)
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=2,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=3;
```

>>>>> HFA mit 60 Sätzen mit 60 B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=2,FUNCTION=HG3530,ANZSATZ=60,ANZBKAN=6
```

>>>>> Konfiguration dieses Blockes beenden
```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=2,ANTW=JA;
```

Funktionsblock 3

/* Funktionsblock 3: Einrichten der Funktionen IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)
```
EINR-
BFDAT:FCTBLK=3,FUNCTION=HG3570&HG3550&WAML&HG3530,BGBKAN=BKAN120;
```

>>>>> IPDA mit 30 B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=HG3570,ANZBKAN=30;
```

>>>>> IP-Trunking mit einem Satz mit drei Einheiten (=30 B-Kanälen)
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=3;
```

>>>>> WAML
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=WAML,ANZEINH=3;
```

>>>>> HFA mit 30 Sätzen mit 30 B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=HG3530,ANZSATZ=30,ANZBKAN=3
```

>>>>> Konfiguration dieses Blockes beenden
```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=3,ANTW=JA;
```

Funktionsblock 4

/* Funktionsblock 4: Einrichten der Funktionen IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)

```
EINR-
BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BGBKAN=BKAN120;
```

>>>>> IPDA mit 30 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3570,ANZBKAN=30;
```

>>>>> IP-Trunking mit einem Satz mit einer Einheit (=10 B-Kanälen)

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=1;
```

>>>>> WAML mit einer Einheit (=10 B-Kanälen)

```
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA mit 70 Sätzen mit 70 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3530,ANZSATZ=70,ANZBKAN=70;
```

>>>>> Konfiguration des Blockes beenden

```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=4,ANTW=JA;
```

Funktionsblock 5

/* Funktionsblock 5: Einrichten der Funktionen IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)

```
EINR-
BFDAT:FCTBLK=5,FUNCTION=HG3570&HG3550&WAML&HG3530,BGBKAN=BKAN120;
```

>>>>> IPDA mit 30 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=5,FUNCTION=HG3570,ANZBKAN=30;
```

>>>>> IP-Trunking mit einem Satz mit 10 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=5,FUNCTION=HG3550,ANZSATZ=1;
```

>>>>> WAML mit einer Einheit (=10 B-Kanälen)

```
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=5,FUNCTION=WAML;
```

>>>>> HFA mit 140 Sätzen mit 70 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=5,FUNCTION=HG3530,ANZSATZ=140,ANZBKAN=70;
```

>>>>> Konfiguration des Blockes beenden

```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=5,ANTW=JA;
```

Funktionsblock 6

/* Funktionsblock 6: Einrichten der Funktionen IP-Trunking (HG3550) und HFA-Teilnehmer (HG3530)

```
EINR-BFDAT:FCTBLK=6,FUNCTION=HG3550&HG3530,BGBKAN=BKAN120;
```

>>>>> IP-Trunking mit einem Satz mit 30 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=6,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=3;
```

>>>>> HFA mit 90 Sätzen mit 90 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=6,FUNCTION=HG3530,ANZSATZ=90,ANZBKAN=90;
```

>>>>> Konfiguration dieses Blockes beenden
```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=6,ANTW=JA;
```

Funktionsblock 7

/* Funktionsblock 7: IP-Trunking, Funktion HFA-Teinehmer (HG3530) und Reserve-HFA-Teilnehmer (HG3530R)

Wichtig: Die reservierten HFA-B-Kanäle müssen bei der Konfiguration der HG3530-Funktion mit angegeben werden, da bei der Reservierung keine Teilnehmer-B-Kanäle akzeptiert werden.

```
EINR-
BFDAT:FCTBLK=7,FUNCTION=HG3550&HG3530&HG3530R,BGBKAN=BKAN120;
```

>>>>> HFA mit 80 Sätzen mit 80 B-Kanälen und 20 Reserve-B-Kanälen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=7,FUNCTION=HG3530,ANZSATZ=80,ANZBKAN=1
```

>>>>> Reserve HFA-Teilnehmer mit 20 Sätzen
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=7,FUNCTION=HG3530R,ANZSATZ=20;
```

>>>>> IP-Trunking mit 10 Sätzen mit einer Einheit (=10 B-Kanälen)
```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=7,FUNCTION=HG3550,ANZSATZ=10,ANZEINH=1
```

Abfragen aller Funktionsblöcke

```
ABFRAGEN-BFDAT;
H500:  AMO BFDAT GESTARTET
-------------------------------------------------------------------
| FCTBLK =  1    BGBKAN : BKAN120
 STATUS=      OK           |
-------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS ??  BCHLCNT
 120  TOTAL BCHAN 120
|
-------------------------------------------------------------------
-------------------------------------------------------------------
| FCTBLK =  2    BGBKAN : BCHL120
 STATUS=      OK           |
-------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT
 30  TOTAL BCHAN  30  |
|  3rd FUNCT : HG3530      60 LINES    UNITS 60  BCHLCNT
 60  TOTAL BCHAN  60  |
-------------------------------------------------------------------
-------------------------------------------------------------------
| FCTBLK =  3    BGBKAN : BCHL120
 STATUS=      OK           |
-------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
```

```
|  2nd FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT
 30  TOTAL BCHAN  30  |
|  3rd FUNCT : WAML         1 LINES    UNITS  3  BCHLCNT
 30  TOTAL BCHAN  30  |
|  4th FUNCT : HG3530      30 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
-------------------------------------------------------------------------
-------------------------------------------------------------------------
| FCTBLK =  4    BGBKAN : BCHL120
 STATUS=      OK           |
-------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT
 70  TOTAL BCHAN  70  |
-------------------------------------------------------------------------
-------------------------------------------------------------------------
| FCTBLK =  5    BGBKAN : BCHL120
 STATUS=    CONT           |
-------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
| 4th FUNCT : HG3530 140 LINES UNITS 70 BCHLCNT 70 TOTAL
 BCHAN 70 |
-------------------------------------------------------------------------
-------------------------------------------------------------------------
| FCTBLK =  6    BGBKAN : BCHL120
 STATUS=      OK           |
-------------------------------------------------------------------------
|  1st FUNCT : HG3550       1 LINES    UNITS  3  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3530      90 LINES    UNITS 90  BCHLCNT
 90  TOTAL BCHAN  90  |
-------------------------------------------------------------------------
-------------------------------------------------------------------------
| FCTBLK =  7    BGBKAN : BCHL120
 STATUS=      OK           |
-------------------------------------------------------------------------
|  1st FUNCT : HG3530      80 LINES    UNITS 80  BCHLCNT
 100  TOTAL BCHAN 100  |
|  2nd FUNCT : HG3530R     20 LINES    UNITS 20  BCHLCNT
 0  TOTAL BCHAN   0  |
|  3rd FUNCT : HG3550      10 LINES    UNITS 10  BCHLCNT
 10  TOTAL BCHAN  10  |
-------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR
 CGW BOARDS
DISPLAY COMPLETED;
```

<

2.16.3 Konfigurieren der Common Gateway Baugruppe mit AMO BCSU

Zuordnung für Funktionsblock 1

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=2,EBT=37,SACHNR=Q2316-X10,FCTID=1,FCTBLK=1,IPA►
DR=198.16.16.45;
ABFRAGEN-BCSU:ART=TAB,LTG=1,LTU=2;
H500:  AMO BCSU  GESTARTET
ADDRESS :  LTG  1   LTU 2    SOURCE GROUP 1    ALARMNO-LTU 0

-----+-----------+--------+---+-+-+---+-+------------+------------+------------
     |           |        |   |S|H|AL-| |            |            |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |    HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE INFO  | STATUS
-----+-----------+--------+---+-+-+---+-+------------+------------+------------
  19 | Q2258-X   ACGEN              0|*| AVAILABLE  |            | NPR
  25 | Q2205-X   WAML       1   A   0|*|            |            | NPR
  31 | AVAILABLE                    0| | AVAILABLE  |            |
  37 | Q2316-X10 STMI2      1   A   0|*|            |            | NPR
     +-------------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 45         B-CHANNELS : 120    BCHLCNT :   2
     | BLOCK NO   :   1                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS : 120    BCHLCNT :   2
     +-------------------------------+-+------------+------------+------------
  43 | Q6401-X   PBCDG-FU   3   A   0|*|            |            | NPR
  49 | AVAILABLE                    0| | AVAILABLE  |            |
  55 | Q2214-X   TMOM2          A   0|*|            |            | NPR
  61 | Q2195-X   DIU-N4     1   A   0|*|            |            | NPR
  67 |                              0| |            |            |
  73 | Q2248-X   LTUCE              0|*| AVAILABLE  |            | NPR
  79 | Q2096-X200 DIU-S2        A   0|*|            |            | NPR
  85 | Q2096-X200 DIU-S2        A   0|*|            |            | NPR
  91 | Q2096-X200 DIU-S2        A   0|*|            |            | NPR
  97 | Q2096-X200 DIU-S2        A   0|*|            |            | NPR
 103 | AVAILABLE                    0| | AVAILABLE  |            |
 109 | AVAILABLE                    0| | AVAILABLE  |            |
 115 | Q2096-X200 DIU-S2        A   0|*|            |            | NPR
 121 | Q2174-X   STMD           A   0|*|            |            | NPR
DISPLAY COMPLETED;
```

Zuordnung für Funktionsblock 2

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=31,SACHNR=Q2316-X10,FCTID=1,FCTBLK=2,IPA►
DR=198.16.16.31;
```

Zuordnung für Funktionsblock 3

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=37,SACHNR=Q2316-X10,FCTID=1,FCTBLK=3,IPAD►
DR=198.16.16.37;
```

Zuordnung für Funktionsblock 4

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=43,SACHNR=Q2316-X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
```

Zuordnung für Funktionsblock 5

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=49,PARTNO=Q2316-X10,FCTID=1,FCTBLK=5,IPAD►
DR=198.16.16.49;
```

Zuordnung für Funktionsblock 6

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=55,SACHNR=Q2316-X10,FCTID=1,FCTBLK=6,IPAD►
DR=198.16.16.55;
```

Zuordnung für Funktionsblock 7

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=61,SACHNR=Q2316-X10,FCTID=1,FCTBLK=7,IPAD►
DR=198.16.16.59;
```

Reservierte HFA-Sätze in benutzbare Sätze umwandeln

```
AENDERN-BCSU:TYPE=IPGW,LTG=1,LTU=1,EBT=61,UMWRESLN=13;
ABFRAGEN-BCSU:ART=TAB,LTG=1,LTU=1;
H500:  AMO BCSU  GESTARTET
ADDRESS :  LTG  1   LTU 1    SOURCE GROUP 1    ALARMNO-LTU 0
-----+-----------+--------+---+-+-+---+-+------------+------------+------------
     |           |        |   |S|H|AL-| |            |            |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |    HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE INFO  | STATUS
-----+-----------+--------+---+-+-+---+-+------------+------------+------------
  19 | Q7065-X    APPS              0|*| AVAILABLE  |            | NPR
  25 | Q2117-X    SLMS          A   0|*|            |            | NPR
  31 | Q2316-X10  STMI2     1    A   0|*|            |            | NPR
     +-----------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 31         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   2                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  3rd FUNCT  : STMI-HFA2    60 LINES   B-CHANNELS :  60    BCHLCNT :  60
     +-----------------------------+-+------------+------------+------------
  37 | Q2316-X10  STMI2     1    A   0|*|            |            | NPR
     +-----------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 37         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   3                     PRERESERVED LINES ASSIGNED     NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  4th FUNCT  : STMI-HFA2    30 LINES   B-CHANNELS :  30    BCHLCNT :  30
     +-----------------------------+-+------------+------------+------------
  43 | Q2316-X10  STMI2     1    A   0|*|            |            | NPR
     +-----------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 43         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   4                     PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  4th FUNCT  : STMI-HFA2    70 LINES   B-CHANNELS :  70    BCHLCNT :  70
     +-----------------------------+-+------------+------------+------------
  49 | Q2316-X10  STMI2     1    A   0|*|            |            | NPR
     +-----------------------------+-+------------+------------+------------
     | IP ADDRESS : 198. 16. 16. 49         B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   5                     PRERESERVED LINES ASSIGNED  :  NO
```

```
     |  1st FUNCT  : STMI2-IPDA    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  3rd FUNCT  : STMI2-WAML    1 LINES   B-CHANNELS :  10    BCHLCNT :  10
     |  4th FUNCT  : STMI-HFA2   140 LINES   B-CHANNELS :  70    BCHLCNT :  70
     +-------------------------------+-+-----------+-----------+-----------
  55 | Q2316-X10  STMI2      1   A   0|*|           |           | NPR
     +-------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS :  198. 16. 16. 55       B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   6                    PRERESERVED LINES ASSIGNED  :  NO
     |  1st FUNCT  : STMI2-IPGW    1 LINES   B-CHANNELS :  30    BCHLCNT :  30
     |  2nd FUNCT  : STMI-HFA2    90 LINES   B-CHANNELS :  90    BCHLCNT :  90
     +-------------------------------+-+-----------+-----------+-----------
  61 | Q2316-X10  STMI2      1   A   0|*|           |           | NPR
     +-------------------------------+-+-----------+-----------+-----------
     | IP ADDRESS :  198. 16. 16. 59       B-CHANNELS : 120    BCHLCNT : 120
     | BLOCK NO   :   7                    PRERESERVED LINES ASSIGNED  : YES
     |  1st FUNCT  : STMI-HFA2    93 LINES   B-CHANNELS : 100    BCHLCNT : 100
     |  2nd FUNCT  : STMI-HFA2R    7 LINES   B-CHANNELS :   0    BCHLCNT :   0
     |  3rd FUNCT  : STMI2-IPGW   10 LINES   B-CHANNELS :  10    BCHLCNT :  10
     +-------------------------------+-+-----------+-----------+-----------
  67 | AVAILABLE                     0| | AVAILABLE |           |
  73 | Q2248-X    LTUCE              0|*| AVAILABLE |           | NPR
  79 | Q2164-X    SLMO16     1   A   0|*|           |           | NPR
  85 | Q2168-X    SLMO24     1   A   0|*|           |           | NPR
  91 | Q2153-X100 SLMQ           A   0|*|           |           | NPR
  97 | Q2150-X    SLMB           A   0|*|           |           | NPR
 103 | Q2480-X    SLMAR          A   0|*|           |           | NPR
 109 | Q2246-X    SLMA24         A   0|*|           |           | NPR
 115 | Q2025-X300 TMBD           A   0|*|           |           | NPR
 121 | AVAILABLE                     0| | AVAILABLE |           |
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
DISPLAY COMPLETED;
```

Es wurden sieben Common Gateway Baugruppen (hier: Q2316-X10, STMI2) eingerichtet.

2.16.4 Einrichten von SIP Trunking

Einrichten von SIP-Trunking auf der Baugruppe STMI2 in 1-1-55:

```
ADD-CGWB:LTU=1,SLOT=55,SMODE=NORMAL,IPADDR=198.16.16.55,NET►
MASK=255.255.255.0,TRPRSIP=30;
```

Wichtig: Ab V10R0 wird die Unterstützung für STMI2 nicht mehr angeboten. Der Ersatz für STMI2 ist STMIX.

Wichtig: Es ist nur ein Trunking-Protokoll pro Common Gateway Baugruppe möglich!

2.16.5 Nicht abgeschlossener und abgeschlossener Funktionsblock

2.16.5.1 Nicht abgeschlossener Funktionsblock

/* Funktionsblock 4: Einrichten der Funktionen IPDA (HG3570), IP-Trunking (HG3550), WAML und HFA-Teilnehmer (HG3530)

```
EINR-
BFDAT:FCTBLK=4,FUNCTION=HG3570&HG3550&WAML&HG3530,BGBKAN=BKAN120;
```

>>>>> IPDA mit 30 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3570,ANZBKAN=30;
```

>>>>> IP-Trunking mit 1 Satz und 1 Einehit (=10 B-Kanälen)

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=1;
```

>>>>> WAML mit einer Einheit (=10 B-Kanälen)

```
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=WAML;
```

>>>>> HFA mit 70 Sätzen und 70 B-Kanälen

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3530,ANZSATZ=70,ANZBKAN=70;
```

>>>>> Konfiguration des Blockes nicht beenden

```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=4,ANTW=NEIN;
```

Abfrage Funktionsblock

```
ABFRAGEN-BFDAT:FCTBLK=4;
H500:  AMO BFDAT GESTARTET
-------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120
  STATUS=   CONT            |
-------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT
 70  TOTAL BCHAN  70  |
-------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR
 CGW BOARDS
DISPLAY COMPLETED;
```

Zuordnung für Funktionsblock 4

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=43,SACHNR=Q2316-
X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
H500:  AMO BCSU  GESTARTET
F89: THE GIVEN FUNCTION BLOCK IS NOT COMPLETELY
 CONFIGURED.
     PLEASE FINISH CONFIGURATION BY MEANS OF AMO_BFDAT
 FIRST.
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT

ADD NOT COMPLETED;
```

Wichtig: Wenn die Konfiguration eines Funktionsblockes mit AMO BFDAT nicht abgeschlossen wurde, so kann dieser auch keiner Baugruppe mit AMO BCSU zugewiesen werden. Es muss zuerst die Konfiguration des Funktionsblockes mit AMO BFDAT abgeschlossen werden, dann kann das Kommando erfolgreich durchgeführt werden.

2.16.5.2 Abgeschlossener Konfigurationsblock

>>>>> Konfiguration des Blockes beenden

```
AENDERN-BFDAT:CONFIG=OK,FCTBLK=4,ANTW=JA;
```

Abfrage Funktionsblock

```
ABFRAGEN-BFDAT:4;
H500:  AMO BFDAT GESTARTET
------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120
  STATUS=      OK           |
------------------------------------------------------------------------
|  1st FUNCT : HG3570       1 LINES    UNITS 30  BCHLCNT
 30  TOTAL BCHAN  30  |
|  2nd FUNCT : HG3550       1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  3rd FUNCT : WAML         1 LINES    UNITS  1  BCHLCNT
 10  TOTAL BCHAN  10  |
|  4th FUNCT : HG3530      70 LINES    UNITS 70  BCHLCNT
 70  TOTAL BCHAN  70  |
------------------------------------------------------------------------
AMO-BFDAT-54        CONFIGURATION OF FUNCTIONAL BLOCKS FOR
 CGW BOARDS
DISPLAY COMPLETED;
```

Zuordnung für Funktionsblock 4

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=43,SACHNR=Q2316-
X10,FCTID=1,FCTBLK=4,IPAD►
DR=198.16.16.43;
H500:  AMO BCSU  GESTARTET
H01: BD  1.1 . 43 ASSIGNED
AMO-BCSU -54        BOARD CONFIGURATION, SWITCHING UNIT
ADD COMPLETED;
```

2.17 Ressource Manager Funktionalität

2.17.1 Allgemeines

Mit dem Ressource Management werden für die Leistungsmerkmale HFA (ohne feature HFA Mobile und ohne HFA Desktop clients), IPDA und DMC zwei verschiedene Arten von Ressourcen verwaltet, beobachtet und ausgewertet:

- Die zur Verfügung stehende Bandbreite in bestimmten Abschnitten im Netz und deren Auslastung durch Verbindungen und
- die (DSP-) Kanäle von Gateways.

Der Ressource Manager (RM) in jedem OpenScape 4000 System ab 2.0 ist immer aktiv. Zur Berechnung der erforderlichen Bandbreite benötigt der RM Kenntnis über die aktuelle Topologie des IP-Netzes. Ist die Topologie nicht eingerichtet, so nimmt der RM an, dass unendliche Bandbreite zur Verfügung steht.

Wozu wird der RM benötigt?

Schon in der HiPath 4000 V1.0 gab es für IPDA eine Art von Ressourcen-Management. So kann man für eine HG 3570/3575 die Anzahl der B-Kanäle, die in das IP-Netz des Kunden vermittelt werden, begrenzen. Aber diese Methode, die immer noch zur Verfügung steht, kann nicht für alle Fälle herangezogen werden.

- HFA- Telefone in einer Filiale hinter einer begrenzten WAN-Strecke können nur über den Ressourcen Manager verwaltet werden. SIP-Teilnehmer können auch verwendet werden. Sie haben die identische Konfiguration im AMO SDAT.
- Mehrere Access Points IP (IPDA Rahmen) an einem Standort, der über ein bandbegrenztes WAN an den Host angebunden ist (nur der Weg zum Host muss begrenzt werden, Gespräche zwischen den IPDA-Rahmen nicht).

Die nachfolgenden Begriffe Sektor und Cluster sind für das weitere Verständnis der Funktion wesentlich.

2.17.2 Schlüsselbegriffe

2.17.2.1 Sektor

Ein Sektor ist ein bei der Netzplanung festgelegter Abschnitt eines Kundennetzes, der im Rahmen des Ressource Managements betrachtet wird.

Ein Sektor kann entweder einem Gateway oder einem beliebigen Abschnitt im IP-Netz zugewiesen werden. Dabei ist es dem Anwender überlassen, welche physikalischen Einrichtungen im Netz einen gemeinsamen Sektor bilden. Um die Administration nicht zu verkomplizieren, ist es sinnvoll, möglichst große, breitbandige Abschnitte zusammenzufassen und sich auf besonders Ressourcen-schwache Abschnitte (z.B. schmalbandige Anbindungen an das WAN) zu konzentrieren.

Sektordefinitionen

- LAN-Sektoren sind Sektoren mit unbegrenzter Bandbreite
- WAN-Sektoren haben eine begrenzte Bandbreite und verbinden die LAN-Sektoren.
- Gateway (GW)-Sektoren sind Sektoren der HG 3570/3575
- HFA-Sektoren sind LAN-Sektorenan denen ein HFA-Phone angeschlossen ist.

2.17.2.2 Cluster

Die Lage von Endpunkten im Netz wird durch ihre Zugehörigkeit zu einem Sektor bestimmt. Zur Vereinfachung der Administration der HFA-Teilnehmer werden diese als Endpunkte gleicher Erreichbarkeit zu sogenannten Clustern zusammengefasst. Ein Cluster kann enthalten:

- allen HFA Endgeräten im OpenScape 4000 System
- allen HFA Endgeräten an einem Access Point

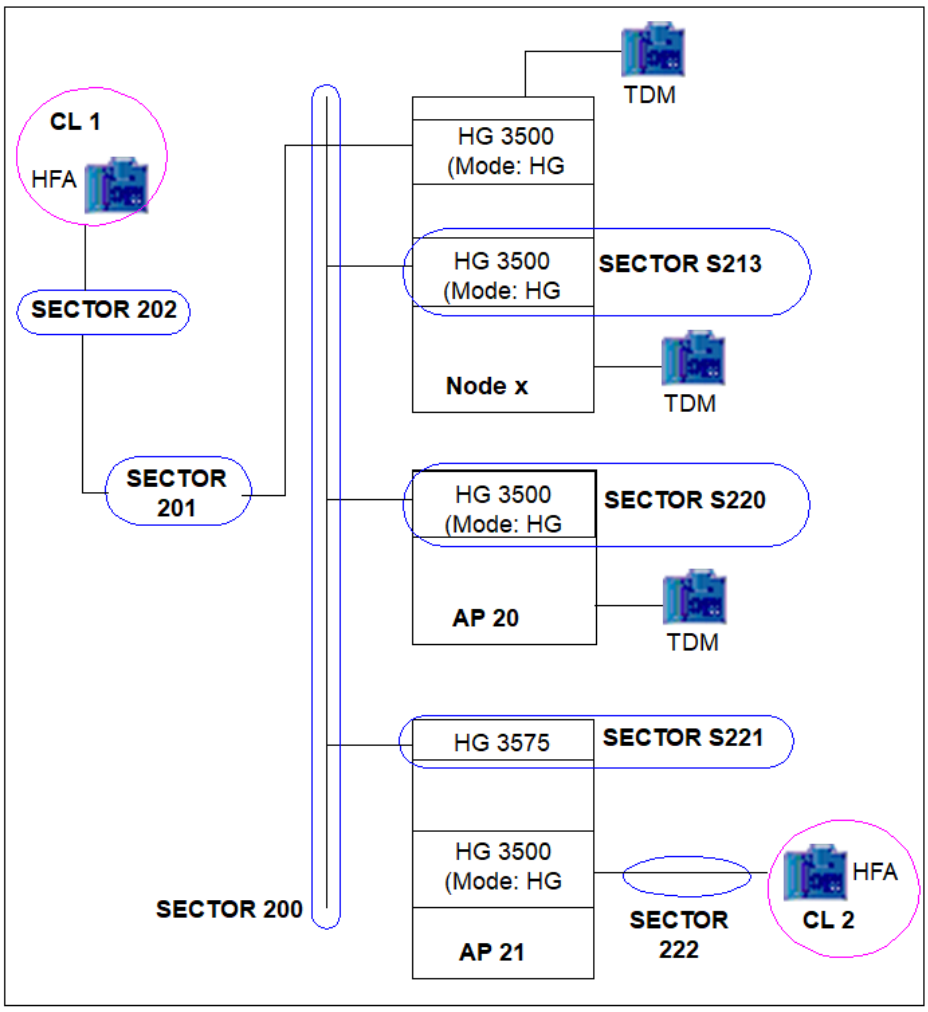


Abbildung 36: Sektor/Cluster Definition an einem OpenScape 4000 Knoten (Beispiel)

HFA Endgeräte können, obwohl sie an einer Baugruppe konfiguriert sind, verschiedenen Clustern zugeordnet sein. Dies ist dann der Fall, wenn die Endgeräte selbst an verschiedenen LAN/WAN Sektoren angeschlossen sind.

2.17.2.3 Sektor-Pfad

Ein Sektor-Pfad ist die Beschreibung eines Weges durch das Kunden-LAN und WAN zwischen zwei Endpunkten. Ein Sektor-Pfad wird immer aus Sicht der

Anlage definiert, um einen Gateway-Sektor oder einen LAN/WAN-Sektor zu erreichen.

2.17.2.4 Definitionen

2.17.2.4.1 AMO GKTOP: Parameter im Zweig TYP=RESMGMT1

Grundsätzlich wird zwischen 2 Sektor-Typen unterschieden.

Ein Sektortyp beschreibt ein Gateway (GW), der andere ein IP Segment im Kundennetz (LAN oder WAN), die jeweils als Sektor Attribut einzurichten sind.

Beschreibung zu weiteren Attributen:

SEKATTR: GW

Dieses Attribut muss für Gateway-Sektoren gesetzt werden (nur für HG 3570 und HG 3575). Jeder GW-Sektor muss mit einem LAN-Sektor (unbegrenzte Bandbreite) verbunden sein.

SEKATTR: LAN / WAN

Dieses Attribut beschreibt ein IP-Segment im Kundennetz. Es ist nur in Verbindung mit dem Attribut **EIGENER**&**EXKLUSIV** zu setzen.

Folgende Regel hat sich bewährt:

Ist der Abschnitt im Kunden IP-Netz unbegrenzt, setzt man das Attribut **LAN**.

Handelt es sich um einen begrenzten Sektor, wird dieser mit dem Attribut **WAN** gekennzeichnet.

WAN -Sektoren liegen immer zwischen LAN-Sektoren!

An einen WAN-Sektor dürfen keine HFA-Teilnehmer angeschaltet werden. Diese müssen immer einem LAN-Sektor zugeordnet werden.

SEKATTR: EIGENER & EXKLUSIV

Der Sektor wird vom RM des eigenen (**EIGENER**) Knotens ausschließlich (**EXKLUSIV**) verwaltet. Würde das Attribut **EXKLUSIV** nicht mit angegeben werden, würde vom RM keine Bandbreite (bei LAN) belegt bzw. keine Kanäle hochgezählt werden (bei GW).

SECATTR: HHS/AP

Diese Attribute sind alternativ nur zusätzlich zum Attribut GW zu setzen und lokalisieren den Shelf-Typ, in dem sich das GW befindet.

Ist das Attribut **AP** gesetzt, muss ein Sektor-Pfad diesem Sektor zugewiesen werden.

SEKATTR: KEINDMC

Dieses Attribut blockiert DMC (Direct Media Connection), wenn dieser so markierte Sektor für ein Gespräch benutzt wird.

Sektor Attribut Sektor Typ	O W N	E X C L	A P	H H S	N O D M C
GW	X	X	A	A	

LAN/WAN	X	X			O

- Pflicht-Attribut ist mit „X“ markiert.
- Attribute, die innerhalb einer durch Doppelstriche begrenzten Gruppe mit „A“ markiert sind, können nur alternativ angegeben werden.
- Attribute, die durch „O“ markiert sind, können optional gesetzt werden (je nach Anwendungsfall).

Die Administration folgender Parameter kann je nach Anwendungsfall (Sektor Typen/Attribute) entfallen.

BANDBR:

Verfügbare Bandbreite in Kbit/s (Achtung: BANDBR=0 bedeutet unbegrenzt!)

GWLAN:

Nummer des LAN-Sektors, mit dem der Gateway-Sektor verbunden ist. Nur, wenn **GWLAN** eingetragen ist, kann man die Belegung der HG 3570/HG 3575 mit AMO GKTOP abfragen.

SEKPFNR1:

Sektor-Pfad Nummer 1 wird für die Leistungsmerkmale HFA und IPDA verwendet. Sektor-Pfad Nummer 1 (**SEKPFNR1**) definiert den Weg vom Host zu einem entfernten Sektor, an dem sich entweder angeschaltete HFA-Telefone befinden oder der eine HG 3575 beschreibt.

Unter dieser Sektorpfadnummer werden alle Sektoren eingegeben, die durchlaufen werden, um diesen Sektor von einem HHS aus zu erreichen. Der Sektorpfad Nummer 1 beginnt mit dem Sektor, der dem HHS am nächsten liegt und endet mit dem entferntesten.

Man fängt mit dem Sektor nächst dem HHS an und endet beim entferntesten.

Der Zielsektor ist nicht Bestandteil des Sektorpfades.

Da der RM für IP-Trunking nicht freigegeben ist, werden die **SEKPFNR2** und **SEKPFNR3** nicht verwendet.

Beispiel für Abbildung „Beispiel für Sektor/Cluster.....“: Sektorpfad für Cluster 1: 200&201 (nicht 202)

2.17.2.4.2 AMO GKTOP: Parameter im Zweig TYP=IPDA (nur für HFA)

GWSEK

Ein **GWSEK** muss nur angegeben werden, wenn eine HG 3530 in einem AP-IP eingerichtet ist. In diesem Falle wird als GWSEK die Sektor-Nummer der HG 3575 eingetragen.

HFASEK

Für Cluster mit HFA Phones ist hier die Sektor Nummer des LAN/WAN anzugeben, an dem die HFA Phones angeschlossen sind.

2.17.3 Konfigurationsregeln

- Jeder HG 3570/3575 wird ein GW-Sektor zugewiesen.
- Jeder GW-Sektor muss mit einem LAN-Sektor (**BANDW=0**, unbegrenzte Bandbreite) verbunden sein.

- Jedem Endpunkt muss ein Sektorpfad zugewiesen werden. Endpunkte sind
  - ein GW-Sektor im Access Point (HG 3575),
  - ein HFA-Sektor.
- Der Endpunkt (GW-Sektor / HFA-Sektor) ist nicht Bestandteil der Pfadbeschreibung.
- Allen HFA-Teilnehmern muss eine Cluster-ID zugewiesen werden.
- Eine Cluster-ID, deren HFA-Teilnehmer im Hostsystem konfiguriert sind, muss ein HFA-Sektor zugewiesen werden.
- Eine Cluster-ID, deren HFA-Teilnehmer im Access Point konfiguriert sind, muss ein HFA-Sektor und der GW-Sektor des Access Points zugewiesen werden.

2.17.4 Verwendete Bandbreiten

```
ABFRAGEN-SIPCO:TYP=BANDW;
```

Wichtig: Bandbreiten-Tabelle muss kundenspezifisch angepasst werden. `AENDERN-SIPCO:TYP=BANDW,.....;`

2.17.5 Einrichtung des Ressource Managements für eine HFA-Konfiguration

2.17.5.1 Ausgangssituation

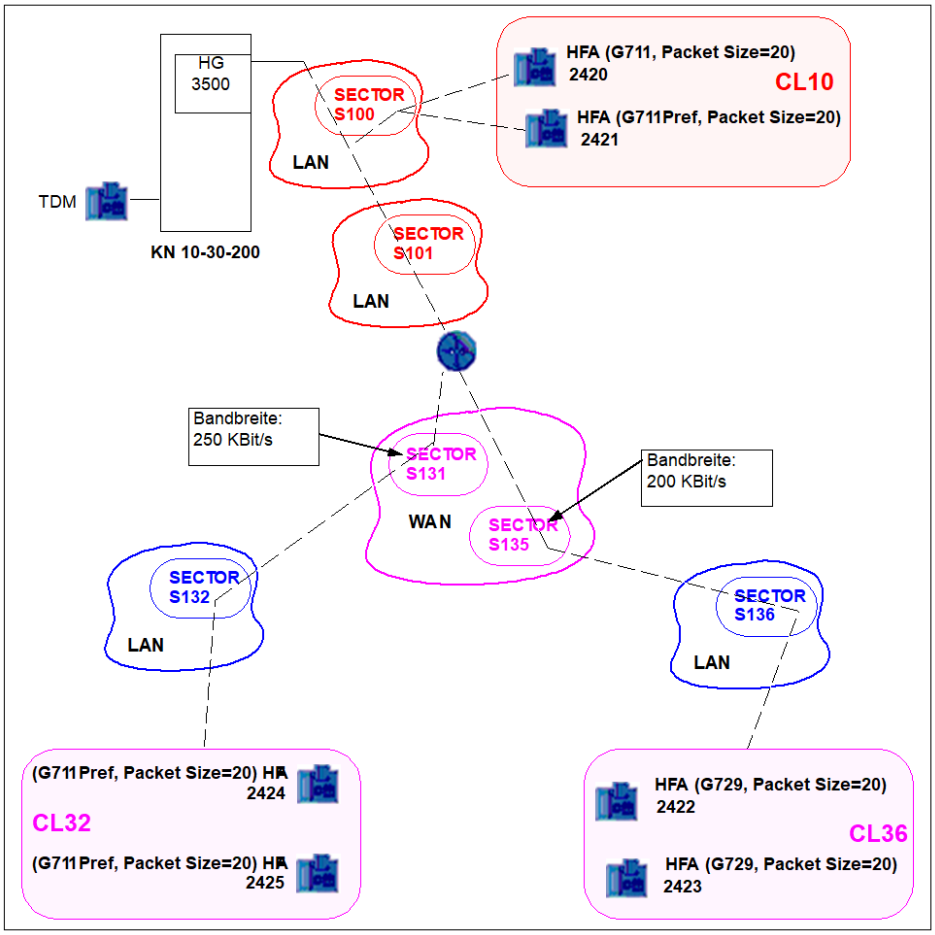


Abbildung 37: Ressource Management für HFA-Konfiguration

Netzplan für das Ressource Management

Die Ausgangssituation ist wie folgt:

Am Knoten 10-30-200 gibt es das Merkmal HFA. Diese Funktion ist bereits konfiguriert. Nun wird davon ausgegangen, dass es vier (2x2) HFA-Teilnehmer gibt, die teils hinter bandbegrenzten WAN-Strecken und teils im lokalen Netz des Hosts liegen. Diese Situation wird für das Ressource Management durch die Sektoren 131/135 (bandbegrenztes WAN), durch die Sektoren 132/136 (HFA im lokalen, unbegrenzten LAN) sowie durch die Sektoren 100/101 (lokales, unbegrenztes Netz am Host) abgebildet. Der Sektor 101 wird nur benötigt, um eine DMC-Verbindung zwischen Cluster 32 und 36 korrekt abbilden zu können.

Es müssen jeweils Sektor-Pfade definiert werden, um eine Verbindung von Sektor 132N (136) zum Host berechnen zu können.

Die HFA Teilnehmer sind enthalten in Cluster 32 (bis S132), Cluster 36 (bis S136) und Cluster 10 (bis S100).

Alle HFA Teilnehmer haben das Merkmal „DMC erlaubt“.

```
CHANGE-SDAT:STNO=2420&&2425, TYPE=ATTRIBUT, AATTR=DMCALLWD;
```

Die RTP-Sample-Größe hat Auswirkungen auf die Bandbreite. Alle IP-Telefone in dieser Dokumentation verwenden eine Sample-Größe von 20ms für G711 und G.729A. Dies kann in der Datenbank des IP-Telefons oder über DLS konfiguriert werden.

2.17.5.2 Codec-Einstellungen für die HFA-Teilnehmer

Die für einen Anruf verwendeten Codec-Informationen müssen dem Ressourcenmanager zur Verfügung stehen, um die erforderliche Bandbreite zu berechnen.

Bei HFA-Endgeräten **muss** die Einstellung im AMO mit der Einstellung im Endgerät (Configuration) übereinstimmen. In unserem Beispiel sind die HFA-Teilnehmer über DLS bzw. lokalem WBM so eingestellt worden, dass die HFA-Geräte im Host G.711 bevorzugen und die HFA-Teilnehmer hinter der WAN-Strecke G.729A erzwingen.

Die Samplesize der IP-Phones beeinflusst die benötigte Bandbreite. Hier wird von einer Samplesize von 20ms sowohl bei G.711 als auch beim G.729 A ausgegangen. Diese Werte können am Endgerät (bzw. über DLS) eingestellt werden.

```
AENDERN-SBCSU:TLNNU=2420&2421,ART=OPTI,IPCODEC=G711P;
AENDERN-SBCSU:TLNNU=2422&2423,ART=OPTI,IPCODEC=G729A;
AENDERN-SBCSU:TLNNU=2424&2425,ART=OPTI,IPCODEC=G711P;
```

2.17.5.3 Sektoren für das LAN/WAN

Hier werden zunächst die Sektoren, die das LAN/WAN beschreiben, definiert. Dies sind die Sektoren S100, S101, S131, S132, S135 und S136. Die Sektoren 131 und S135 sind WAN-Sektoren. Deren Bandbreite ist 200 kBit/s bzw. 250 kBit/s begrenzt.

Sektor 100, 101, 132 und 136:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um LAN-Sektoren mit unbegrenzter Bandbreite.

```
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=100,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=101,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=132,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=136,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
```

Sektor 131 und 135:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um WAN-Sektoren mit begrenzter Bandbreite.

```
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=131,SEKATTR=EIGENER&EXKLUSIV&WAN,PKNNR=10-
```

```
30-200,BANDBR="250";
EINRICHTEN-
GKTOP:TYP=RESMGMT1,SEKNR=135,SEKATTR=EIGENER&EXKLUSIV&WAN,PKNNR=1
30-200,BANDBR="200";
```

2.17.5.4 Zuordnung der HFA-Teilnehmer zu den Sektoren

Hier wird definiert, dass die Teilnehmer 2420 und 2421 im Cluster 10 an das HFA-LAN (Sektor 100) angeschlossen sind.

```
EINRICHTEN-GKTOP:TYP=IPDA,CLUSTID=10,HFASEK=100;
AENDERN-SDAT:TLNNU=2420,TYP=DATEN1,CLUSTID=10;
AENDERN-SDAT:TLNNU=2421,TYP=DATEN1,CLUSTID=10;
```

Hier wird definiert, dass die Teilnehmer 2422 und 2423 im Cluster 36 an das HFA-LAN (Sektor 136) angeschlossen sind.

```
EINRICHTEN-GKTOP:TYP=IPDA,CLUSTID=36,HFASEK=136;
AENDERN-SDAT:TLNNU=2422,TYP=DATEN1,CLUSTID=36;
AENDERN-SDAT:TLNNU=2423,TYP=DATEN1,CLUSTID=36;
```

Hier wird definiert, dass die Teilnehmer 2424 und 2425 im Cluster 32 an das HFA-LAN (Sektor 132) angeschlossen sind.

```
EINRICHTEN-GKTOP:TYP=IPDA,CLUSTID=32,HFASEK=132;
AENDERN-SDAT:TLNNU=2424,TYP=DATEN1,CLUSTID=32;
AENDERN-SDAT:TLNNU=2425,TYP=DATEN1,CLUSTID=32;
```

Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 2424 zu 2425 (Cluster intern).

```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;
   ---------
+-------------------------------------------------------------
+

   SECTOR   |               100
               |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
               |

   VERW-BB  |                 0
               |

   R-GW-MC  |                 0
               |
```

```
   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SECTOR   |               101
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                 0
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               131
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               250
            |

   VERW-BB  |                 0
            |
```

```
   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SECTOR   |              132
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |              182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |              135
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+
```

```
   S-BB     |               200
            |

   VERW-BB  |                 0
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               136
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                 0
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:



 ---------------------------------------------------------------------

  +-------+----------------------+----------------
+---------------+
```

INDEX	CODEC TYP	RAHMENGROESSE (MS)	RESERVIERTE BANDBR.(KBIT)
1	G711_HFA	30	89
2	G729_HFA	40	22
3	G723_HFA	30	25
4	G711_F10_IPDA	10	120
5	G711_F20_IPDA	20	92
6	G711_F30_IPDA	30	83
7	G711_F60_IPDA	60	74
8	G729_F20_IPDA	20	36
9	G729_F40_IPDA	40	22
10	G729_F60_IPDA	60	18
11	G711_DMC	30	182
12	G729_DMC	40	72
13	G723_DMC	30	27
14	G711_FS_UNKNOWN	60	83

Interpretation:

Es wird nur die Bandbreite in dem Sektor (132) reserviert, dem die beiden Teilnehmer zugeordnet sind. Beide Teilnehmer benutzen G711 mit DMC (AMO SIPCO:BANDW -> Index 11). Ist der Wert der Bandbreite für den Index 11 kleiner als der doppelte Wert des Index 1, so wird zweimal Index 1 berechnet und angezeigt.

Zu diesem Zeitpunkt sind noch keine Sektorpfade definiert, daher wird die Band-breite für die Masterverbindung noch nicht reserviert.

Sämtliche Bandbreiten, die in diesen Beispielen im AMO SIPCO verwendet werden, haben keinen Anspruch auf Wahrheit. Die eingestellten Werte dienen nur zur Demonstration!!! Die Tabelle im AMO SIPCO ist immer kundenspezifisch einzustellen.

2.17.5.5 Sektorpfade definieren

Die Sektorpfade werden benötigt, um die Bandbreite in allen benutzten Sektoren belegen zu können.

In diesem Beispiel werden 2 Sektorpfade benötigt.

Sektorpfad 1 definiert den Weg vom Host zu Zielsektor 132:
```
EINRICHTEN-GKTOP:TYP=SEKPFAD,SEKPFNR=1,SEKBE=100&101&131;
```

Sektorpfad 2 definiert den Weg vom Host zu Zielsektor 136:
```
EINRICHTEN-GKTOP:TYP=SEKPFAD,SEKPFNR=2,SEKBE=100&101&135;
```

2.17.5.6 Sektorpfade zuordnen

```
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=132,SEKPFNR1=1;
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=136,SEKPFNR1=2;
```

Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 2424 zu 2425 (Cluster intern).
```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;
```

```
   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               100
                |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
                |
```

```
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                178
             |
   R-GW-MC   |                  0
             |
   R-GW-DMC  |                  0
             |
   ---------
+-------------------------------------------------------------
+
   SEKTOR    |                101
             |
   ---------
+-------------------------------------------------------------
+
   PKNNR     |         10- 30-200
             |
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                178
             |
   R-GW-MC   |                  0
             |
   R-GW-DMC  |                  0
             |
   ---------
+-------------------------------------------------------------
+
   SEKTOR    |                131
             |
   ---------
+-------------------------------------------------------------
+
```

```
   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |                72
            |

   VERW-BB  |               178
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               132
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               135
            |
```

```
   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               200
               |

   VERW-BB  |                 0
               |

   R-GW-MC  |                 0
               |

   R-GW-DMC |                 0
               |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               136
               |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
               |

   VERW-BB  |                 0
               |

   R-GW-MC  |                 0
               |

   R-GW-DMC |                 0
               |
```

```
   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:



 ------------------------------------------------------------------------

  +-------+----------------------+-----------------
+---------------+

  | INDEX |  CODEC TYP           | RAHMENGROESSE   |
 RESERVIERTE   |

  |       |                      |     (MS)        |
 BANDBR.(KBIT) |

  +-------+----------------------+-----------------
+---------------+

  |    1  | G711_HFA             |       30        |
 89     |

  |    2  | G729_HFA             |       40        |
 22     |

  |    3  | G723_HFA             |       30        |
 25     |

  |    4  | G711_F10_IPDA        |       10        |
 120     |

  |    5  | G711_F20_IPDA        |       20        |
 92     |

  |    6  | G711_F30_IPDA        |       30        |
 83     |

  |    7  | G711_F60_IPDA        |       60        |
 74     |

  |    8  | G729_F20_IPDA        |       20        |
 36     |

  |    9  | G729_F40_IPDA        |       40        |
 22     |

  |   10  | G729_F60_IPDA        |       60        |
 18     |

  |   11  | G711_DMC             |       30        |
 182     |
```

```
  |    12   | G729_DMC              |        40         |
 72      |
```

Interpretation:

Um die Reservierung der Bandbreite für die Masterverbindung vornehmen zu können, bestimmt der Ressourcen-Manager „resultierende Sektorpfade“. Dazu werden die Sektorpfade der beiden Endpunkte miteinander verglichen. In diesem Beispiel ist der Sektorpfad des A-Teilnehmers 2424 S100&S101&S131, Zielsektor S132. Der Sektorpfad des B-Teilnehmers 2425 lautet S100&S101&S131, Zielsektor S132. Dies liefert das Resultat, dass alle Sektoren gemeinsam sind. Daher müssen die Sektoren S100, S101 und S131 die Sektoren der Masterverbindung sein (Reservierung mit zweimal Index 1). Die DMC-Verbindung findet im gleichen Zielsektor 132 statt. Hier wird die Bandbreite 182 kBit/s reserviert (Index 11).

Zweites Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 2424 zu 2422 (Cluster übergreifend).

```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;
   ---------
+-------------------------------------------------------------
+

   SEKTOR    |               100
             |

   ---------
+-------------------------------------------------------------
+

   PKNNR     |         10- 30-200
             |

   ---------
+-------------------------------------------------------------
+

   S-BB      |         UNBEGRENZT
             |

   VERW-BB   |               111
             |

   R-GW-MC   |                 0
             |

   R-GW-DMC  |                 0
             |

   ---------
+-------------------------------------------------------------
+
```

```
   SEKTOR   |               101
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               131
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |                68
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |
```

```
   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               132
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               135
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |                18
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |
```

```
   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               136
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |               182
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:



 ---------------------------------------------------------------------

  +-------+----------------------+-----------------
+---------------+

  | INDEX |  CODEC TYP           | RAHMENGROESSE   |
 RESERVIERTE   |

  |       |                      |     (MS)        |
 BANDBR.(KBIT) |
```

```
  +-------+----------------------+-----------------
+---------------+

  |    1  | G711_HFA             |        30         |
 89      |

  |    2  | G729_HFA             |        40         |
 22      |

  |    3  | G723_HFA             |        30         |
 25      |

  |    4  | G711_F10_IPDA        |        10         |
 120      |

  |    5  | G711_F20_IPDA        |        20         |
 92      |

  |    6  | G711_F30_IPDA        |        30         |
 83      |

  |    7  | G711_F60_IPDA        |        60         |
 74      |

  |    8  | G729_F20_IPDA        |        20         |
 36      |

  |    9  | G729_F40_IPDA        |        40         |
 22      |

  |   10  | G729_F60_IPDA        |        60         |
 18      |

  |   11  | G711_DMC             |        30         |
 182      |

  |   12  | G729_DMC             |        40         |
 72      |

  |   13  | G723_DMC             |        30         |
 27      |

  |   14  | G711_FS_UNKNOWN      |        60         |
 83      |
```

Interpretation:

Um die Reservierung der Bandbreite für die Masterverbindung vornehmen zu können, bestimmt der Ressourcen-Manager „resultierende Sektorpfade“. Dazu werden die Sektorpfade der beiden Endpunkte miteinander verglichen. In diesem Beispiel ist der Sektorpfad des A-Teilnehmers 2424 S100&S101&S131, Zielsektor S132. Der Sektorpfad des B-Teilnehmers 2422 lautet S100&S101&S135, Zielsektor S136. Dies liefert das Resultat, dass der Sektor S101 der letzte gemeinsame Sektor ist. Daher muss der Sektor S100 der Sektor der Masterverbindung sein (Reservierung mit einmal Index 1 plus

einmal Index 2). Die DMC-Verbindung findet ab dem letzten gemeinsamen Sektor statt (Sektor S101). In allen betroffenen Sektoren (S101, S131, S135, S132 und S136) wird die Bandbreite 182 kBit/s reserviert (Index 11).

2.17.6 Einrichtung des Ressource Managements für eine IPDA-Konfiguration mit TDM-Teilnehmern

2.17.6.1 Ausgangssituation

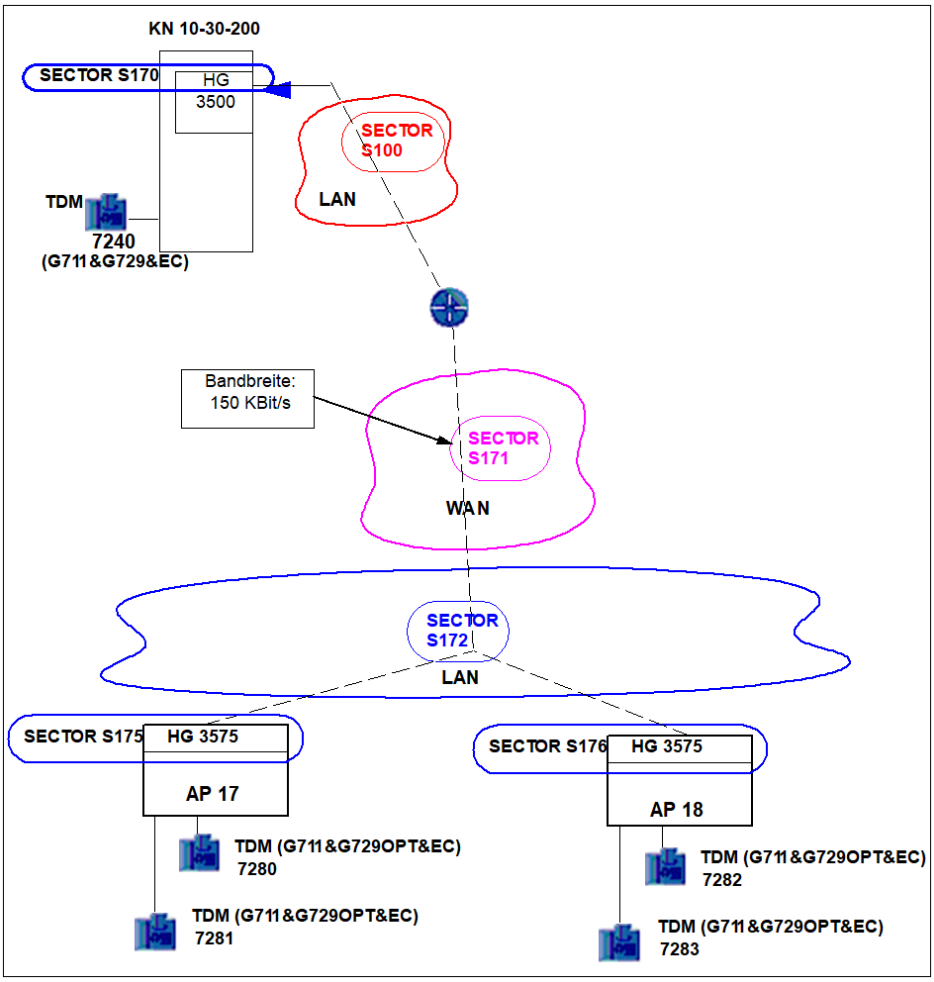


Abbildung 38: Ressource Management für IPDA-Konfiguration mit TDM-Teilnehmern

Die Ausgangssituation ist wie folgt:

Am Knoten 10-30-200 gibt es das bereits eingerichtete Leistungsmerkmal IPDA. mit den Access Points 17 und 18. Es wird davon ausgegangen, dass sich beide Access Points hinter einem bandbreitenbegrenzten WAN befinden. Diese Situation wird für das Ressource Management durch den bandbegrenzten Sektor 171, und durch die unbegrenzten LAN-Sektoren 100 (Host) und 172 (Access Points) abgebildet. Bei IPDA benötigen die HG 3570 und HG 3575

eigene Gateway-Sektoren (S170, S175 und S176). Der Sektor 172 wird benötigt, um die direkte Verbindung zwischen den beiden HG 3575 korrekt abbilden zu können. Für die HG 3575 müssen Sektorpfade definiert werden, um ihre Lage zum Host richtig darstellen zu können.

Die Samplesize für G711 wird für alle HG 3570/75 auf 20 ms gesetzt:

```
AENDERN-CGWB:MTYP=CGW, LTU=1, EBT=61, TYP=ASC, PRIO=PRIO2,
 CODEC=G711A, RTP=20;
AENDERN-STMIB:MTYP=NCUI2, LTU=17, TYP=ASC, PRIO=PRIO1,
 CODEC=G711A, RTP=20;
AENDERN-STMIB:MTYP=NCUI2, LTU=18, TYPE=ASC, PRIO=PRIO1,
 CODEC=G711A, RTP=20;
```

Der Codec G729 sollte für einen Anruf zwischen einem Host-Terminal und einem AP-Terminal verwendet werden. Der Codec G711 sollte für einen Anruf zwischen einem AP-Endgerät des Zugangspunkts 17 und einem AP-Endgerät im Zugangspunkt 18 verwendet werden.

```
AENDERN-SDAT:STNO=7240, TYPE=DATEN1,
 CLASSMRK=G711&G729A&EC;
AENDERN-SDAT:STNO=7280&&7282, TYP=DATEN1,
 CLASSMRK=G711&G729AOPT&EC;
```

2.17.6.2 Sektoren für das LAN/WAN

Hier werden zunächst die Sektoren, die das LAN/WAN beschreiben, definiert. Dies sind die Sektoren S100, S171 und S172. Der Sektor 171 ist ein WAN-Sektor. Seine Bandbreite ist auf 150 kBit/s begrenzt.

Sektor 100 und 172:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um LAN-Sektoren mit unbegrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=100,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=172,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
```

Sektor 171:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um einen WAN-Sektor mit begrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=171,SEKATTR=EIGENER&EXKLUSIV&WAN,PKNNR=10-
30-200,BANDBR="150";
```

2.17.6.3 Sektoren für die Gateways

Dabei handelt es sich um die Sektoren S170, S175 und S176.

Der Sektor 170 hat die Attribute **EIGENER**&**EXKLUSIV** (siehe vorher) sowie HHS (liegt im Host) und GW (ist ein Gateway).

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=170,SEKATTR=EIGENER&EXKLUSIV&HHS&GW, PKN►
NR=10-30-200,GWLAN=100;
```

Die Sektoren 175 und 176 haben die Attribute **EIGENER**&**EXKLUSIV** (siehe vorher) sowie AP (liegt im Host) und GW (ist ein Gateway).

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=175,SEKATTR=EIGENER&EXKLUSIV&AP&GW, PKN►
```

```
NR=10-30-200,GWLAN=172;
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=176,SEKATTR=EIGENER&EXKLUSIV&AP&GW, PKN►
NR=10-30-200,GWLAN=172;
```

2.17.6.4 Zuordnung der Gateways zu ihren Sektoren

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=61,TYP=GWSECTOR,GWSECTNR=170;
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYP=GWSECTOR,GWSECTNR=175;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYP=GWSECTOR,GWSECTNR=176;
```

2.17.6.5 Sektorpfad definieren

Es wird in diesem Beispiel nur ein Sektorpfad benötigt, da Access Point 17 und 18 die gleiche Erreichbarkeit haben.

```
EINRICHTEN-GKTOP:TYP=SEKPFAD,SEKPFNR=1,SEKBE=100&171&172;
```

2.17.6.6 Sektorpfad zuordnen

```
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=175,SEKPFNR1=1;
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=176,SEKPFNR1=1;
```

1. Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 7280 zu 7282 (GW-Sektor 175 zu GW-Sektor 176).

```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;


---------
+-------------------------------------------------------------------
+

   SEKTOR   |               100
               |

   ---------
+-------------------------------------------------------------------
+

   PKNNR    |         10- 30-200
               |

   ---------
+-------------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
               |

   VERW-BB  |                 0
               |
```

```
   R-GW-MC  |                  0
            |

   R-GW-DMC |                  0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               170
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
            |

   VERW-BB  |                  0
            |

   R-GW-MC  |                 60
            |

   R-GW-DMC |                  0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               171
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               150
            |
```

```
   VERW-BB  |                 0
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               172
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |               184
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               175
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |
```

```
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                  0
             |
   R-GW-MC   |                 59
             |
   R-GW-DMC  |                  0
             |
   ---------
+-------------------------------------------------------------
+
   SEKTOR    |                176
             |
   ---------
+-------------------------------------------------------------
+
   PKNNR     |         10- 30-200
             |
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                  0
             |
   R-GW-MC   |                 59
             |
   R-GW-DMC  |                  0
             |
   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:
```

```
 ----------------------------------------------------------------------

  +-------+----------------------+-----------------
+---------------+

  | INDEX |  CODEC TYP           | RAHMENGROESSE   |
 RESERVIERTE   |

  |       |                      |     (MS)        |
 BANDBR.(KBIT) |

  +-------+----------------------+-----------------
+---------------+

  |    1  | G711_HFA             |       30        |
 89     |

  |    2  | G729_HFA             |       40        |
 22     |

  |    3  | G723_HFA             |       30        |
 25     |

  |    4  | G711_F10_IPDA        |       10        |
 120     |

  |    5  | G711_F20_IPDA        |       20        |
 184     |

  |    6  | G711_F30_IPDA        |       30        |
 83     |

  |    7  | G711_F60_IPDA        |       60        |
 74     |

  |    8  | G729_F20_IPDA        |       20        |
 36     |

  |    9  | G729_F40_IPDA        |       40        |
 22     |

  |   10  | G729_F60_IPDA        |       60        |
 18     |

  |   11  | G711_DMC             |       30        |
 182     |

  |   12  | G729_DMC             |       40        |
 72     |

  |   13  | G723_DMC             |       30        |
 27     |

  |   14  | G711_FS_UNKNOWN      |       60        |
 83     |
```

Interpretation:

Es wird nur die Bandbreite in dem Sektor (172) reserviert, der die beiden GW-Sektoren von AP17 und AP18 miteinander verbindet. Beide Teilnehmer benutzen G711 mit 20ms Samplesize (AMO SIPCO:BANDW -> Index 5).

In den GW-Sektoren 175 und 176 sieht man, dass nur noch 59 B-Kanäle frei sind.

2. Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 7282 zu 7240 (GW-Sektor 175 zu GW-Sektor 170).

```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;


---------
+-------------------------------------------------------------------
+

   SEKTOR   |               100
            |

   ---------
+-------------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
            |

   VERW-BB  |                72
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------------
+

   SEKTOR   |               170
            |

   ---------
+-------------------------------------------------------------------
+
```

```
   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                0
            |

   R-GW-MC  |               59
            |

   R-GW-DMC |                0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |              171
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               78
            |

   VERW-BB  |               72
            |

   R-GW-MC  |                0
            |

   R-GW-DMC |                0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |              172
            |
```

```
   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
               |

   VERW-BB  |                72
               |

   R-GW-MC  |                 0
               |

   R-GW-DMC |                 0
               |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               175
               |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
               |

   VERW-BB  |                 0
               |

   R-GW-MC  |                60
               |

   R-GW-DMC |                 0
               |
```

```
   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               176
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |         10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |         UNBEGRENZT
            |

   VERW-BB  |                 0
            |

   R-GW-MC  |                59
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:



 ------------------------------------------------------------------------

  +-------+----------------------+-----------------
+---------------+

  | INDEX |  CODEC TYP           | RAHMENGROESSE   |
 RESERVIERTE   |

  |       |                      |     (MS)        |
 BANDBR.(KBIT) |

  +-------+----------------------+-----------------
+---------------+

  |    1  | G711_HFA             |       30        |
 89     |
```

```
 |    2  | G729_HFA             |       40        |
22     |

 |    3  | G723_HFA             |       30        |
25     |

 |    4  | G711_F10_IPDA        |       10        |
120    |

 |    5  | G711_F20_IPDA        |       20        |
184    |

 |    6  | G711_F30_IPDA        |       30        |
83     |

 |    7  | G711_F60_IPDA        |       60        |
74     |

 |    8  | G729_F20_IPDA        |       20        |
72     |

 |    9  | G729_F40_IPDA        |       40        |
22     |

 |   10  | G729_F60_IPDA        |       60        |
18     |

 |   11  | G711_DMC             |       30        |
182    |

 |   12  | G729_DMC             |       40        |
72     |

 |   13  | G723_DMC             |       30        |
27     |

 |   14  | G711_FS_UNKNOWN      |       60        |
83     |
```

Interpretation:

Es wird die Bandbreite in allen belegten Sektoren (172&171&100) reserviert, die den AP18 mit dem Host verbinden. Bei diesem Gespräch wird der Codec G729 mit 20ms Samplesize (AMO SIPCO:BANDW -> Index 8) verwendet.

In den GW-Sektoren 170 und 176 sieht man, dass nur noch 59 B-Kanäle frei sind.

2.17.7 Einrichtung des Ressource Managements für eine IPDA-Konfiguration mit TDM-Teilnehmern und HFA im Access Point

2.17.7.1 Ausgangssituation

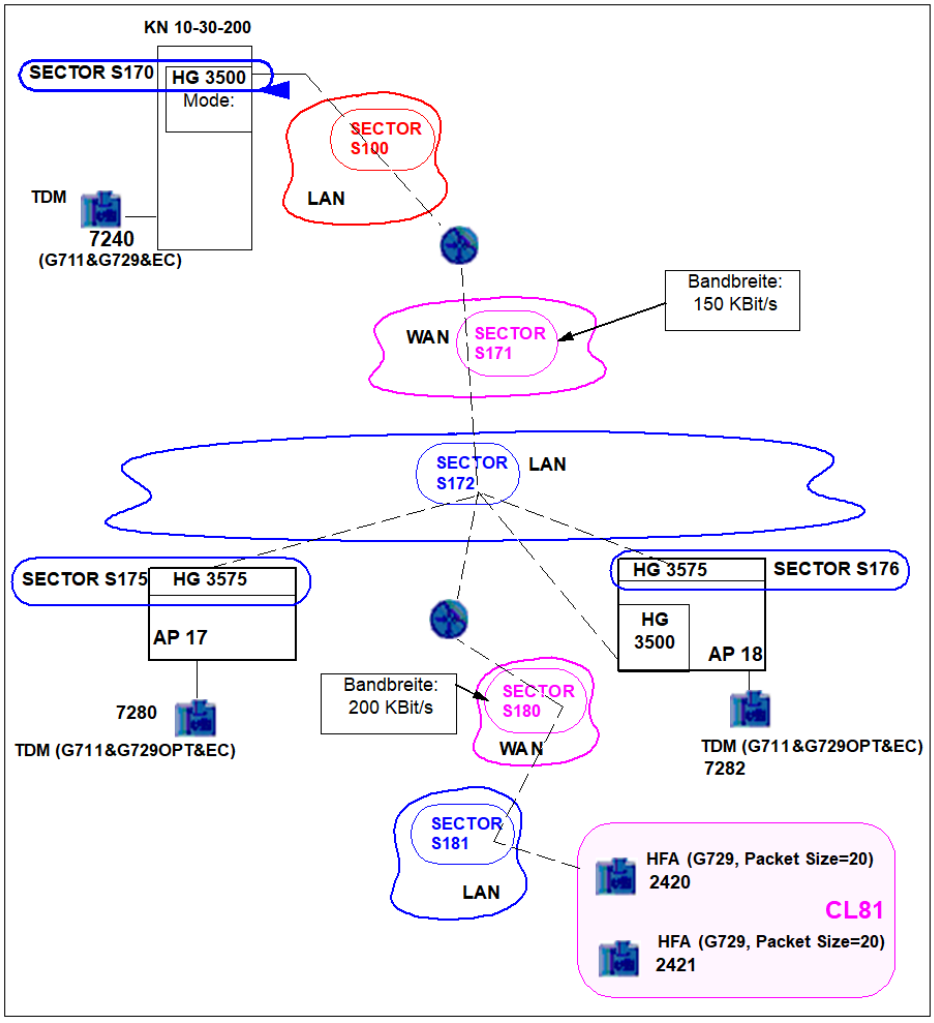


Abbildung 39: Ressource Management für IPDA-Konfiguration mit TDM-/ HFA-Teilnehmern

Die Ausgangssituation ist wie folgt:

Am Knoten 10-30-200 gibt es das bereits eingerichtete Leistungsmerkmal IPDA. mit den Access Points 17 und 18. Das Leistungsmerkmal HFA ist in AP18 konfiguriert. Es wird davon ausgegangen, dass sich beide Access Points hinter einem bandbreitenbegrenzten WAN befinden. Diese Situation wird für das Ressource Management durch den bandbegrenzten Sektor 171, und durch die unbegrenzten LAN-Sektoren 100 (Host) und 172 (Access Points) abgebildet. Bei IPDA benötigen die HG 3570 und HG 3575 eigene Gateway-Sektoren (S170, S175 und S176). Der Sektor 172 wird benötigt, um die direkte Verbindung zwischen den beiden HG 3575 korrekt abbilden zu können. Für die HG 3575 müssen Sektorpfade definiert werden, um ihre Lage zum Host richtig darstellen zu können.

Das WAN für HFA ist an dem Standort des abgesetzten Shelves angeschlossen. Im Ressource Management wird diese Situation so dargestellt, dass der WAN-Sektor 180 an den Sektor 172 grenzt und von der anderen Seite an den LAN-Sektor 181 stößt, an dem das HFA-Cluster 81 angeschaltet ist.

Die Samplesize für G711 wird für alle HG 3570/75 auf 20 ms gesetzt:

```
AENDERN-CGWB:MTYP=CGW,LTU=1,EBT=61,TYP=ASC,PRIO=PRIO2,CODEC=G711A,

RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
```

Der Codec G729 sollte für einen Anruf zwischen einem Host-Terminal und einem AP-Terminal verwendet werden. Der Codec G711 sollte für einen Anruf zwischen einem AP-Endgerät des Zugangspunkts 17 und einem AP-Endgerät im Zugangspunkt 18 verwendet werden.

```
AENDERN-SDAT:STNO=7240,TYPE=DATEN1,CLASSMRK=G711&G729A&EC;
AENDERN-SDAT:STNO=7280&&7282,TYP=DATEN1,CLASSMRK=G711&G729AOPT&EC;
```

Alle HFA Teilnehmer haben das Merkmal „DMC erlaubt“.

```
AENDERN-SDAT:TLNNU=2420&&2421,TYP=MERKMAL,EMERK=DMCERL;
```

Die IPDA-Gateways sollen DMC unterstützen.

- HG 3570:
  ```
  AENDERN-SIPCO:TYP=DMCDATA,DMCERL=JA;
  AENDERN-
  CGWB:MTYP=CGW,LTU=1,EBT=61,TYP=DMCDATA,DMCCONN=45;
  ```
- HG 3575:

```
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYP=DMCDATA,DMCERL=JA,
DMCCONN=45;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYP=DMCDATA,DMCERL=JA,
DMCCONN=45;
```

Einstellungen der Codec-Liste für die Gateways (für DMC-Verbindungen).

```
AENDERN-CGWB:MTYP=CGW,LTU=1,SLOT=69,TYPE=ASC,PRIO=PRIO1,CODEC=G711A,RTP=20;
AENDERN-CGWB:MTYP=CGW,LTU=1,SLOT=69,TYPE=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYPE=ASC,PRIO=PRIO1,CODEC=G711,RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYP=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO1,CODEC=G711,RTP=20;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYP=ASC,PRIO=PRIO2,CODEC=G729A,RTP=20;
```

2.17.7.2 Einstellungen für die HFA-Teilnehmer

Die Codec-Informationen, die für einen Anruf verwendet werden, müssen dem Resource Manager zur Verfügung stehen, um die erforderliche Bandbreite zu reservieren.

Bei HFA-Endgeräten **muss** die Einstellung im AMO mit der Einstellung im Endgerät (Configuration) übereinstimmen.

```
AENDERN-SBCSU:TLNNU=2420&2421,ART=OPTI,IPCODEC=G729A;
```

Codec-Einstellung der HFA-Teilnehmer für die Master-Verbindung im IPDA-Abschnitt.

```
AENDERN-
SDAT:TLNNU=2420&&2421,TYP=DATEN1,CLASSMRK=G711&G729AOPT&EC;
```

2.17.7.3 Sektoren für das LAN/WAN

Hier werden zunächst die Sektoren, die das LAN/WAN beschreiben, definiert. Dies sind die Sektoren S100, S171 und S172. Der Sektor 171 ist ein WAN-Sektor. Seine Bandbreite ist auf 150 kBit/s begrenzt.

Sektor 100 und 172:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um LAN-Sektoren mit unbegrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=100,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=172,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
```

Sektor 171:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um einen WAN-Sektor mit begrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=171,SEKATTR=EIGENER&EXKLUSIV&WAN,PKNNR=10-
30-200,BANDBR="150";
```

Sektor 181:

Für die HFA-Konfiguration werden die Sektoren 181 (LAN) und 181 (WAN) benötigt.

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um einen LAN-Sektor mit unbegrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=181,SEKATTR=EIGENER&EXKLUSIV&LAN,PKNNR=10-
30-200,BANDBR="0";
```

Sektor 180:

Die Attribute **EIGENER**&**EXKLUSIV** sind Pflichtparameter. Es handelt sich um einen WAN-Sektor mit begrenzter Bandbreite.

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=180,SEKATTR=EIGENER&EXKLUSIV&WAN,PKNNR=10-
30-200,BANDBR="200";
```

2.17.7.4 Sektoren für die Gateways

Dabei handelt es sich um die Sektoren S170, S175 und S176.

Der Sektor 170 hat die Attribute **EIGENER**&**EXKLUSIV** (siehe vorher) sowie HHS (liegt im Host) und GW (ist ein Gateway).

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=170,SEKATTR=EIGENER&EXKLUSIV&HHS&GW, PKN►
NR=10-30-200,GWLAN=100;
```

Die Sektoren 175 und 176 haben die Attribute **EIGENER**&**EXKLUSIV** (siehe vorher) sowie AP (liegt im Host) und GW (ist ein Gateway).

```
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=175,SEKATTR=EIGENER&EXKLUSIV&AP&GW, PKN►
NR=10-30-200,GWLAN=172;
EINRICHTEN-GKTOP:TYP=RESMGMT1,SEKNR=176,SEKATTR=EIGENER&EXKLUSIV&AP&GW, PKN►
NR=10-30-200,GWLAN=172;
```

2.17.7.5 Zuordnung der HFA-Teilnehmer zu den Sektoren

Hier wird definiert, dass die Teilnehmer 2420 und 2421 im Cluster 81 an das HFA-LAN (Sektor 181) angeschlossen sind. Da sie zusätzlich Teilnehmer des AP 18 sind, muss unter **GWSEK** der GW-Sektor ihrer HG 3575 eingetragen werden (176).

```
EINRICHTEN-GKTOP:TYP=IPDA,CLUSTID=81,HFASEK=181,GWSEK=176;
AENDERN-SDAT:TLNNU=2420,TYP=DATEN1,CLUSTID=81;
AENDERN-SDAT:TLNNU=2421,TYP=DATEN1,CLUSTID=81;
```

2.17.7.6 Zuordnung der Gateways zu ihren Sektoren

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=61,TYP=GWSECTOR,GWSECTNR=170;
AENDERN-STMIB:MTYP=NCUI2,LTU=17,TYP=GWSECTOR,GWSECTNR=175;
AENDERN-STMIB:MTYP=NCUI2,LTU=18,TYP=GWSECTOR,GWSECTNR=176;
```

2.17.7.7 Sektorpfade definieren

Es wird in diesem Beispiel für IPDA nur ein Sektorpfad benötigt, da Access Point 17 und 18 die gleiche Erreichbarkeit haben.

```
EINRICHTEN-GKTOP:TYP=SEKPFAD,SEKPFNR=1,SEKBE=100&171&172;
```

Für die HFA-Teilnehmer im Cluster 81 muss ein eigener Sektorpfad vom Host ausgehend zum Zielsektor 181 definiert werden.

```
EINRICHTEN-
GKTOP:TYP=SEKPFAD,SEKPFNR=2,SEKBE=100&171&172&180;
```

2.17.7.8 Sektorpfade zuordnen

```
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=175,SEKPFNR1=1;
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=176,SEKPFNR1=1;
AENDERN-GKTOP:TYP=RESMGMT1,SEKNR=181,SEKPFNR1=2;
```

Beispiel für eine Bandbreitenbelegung zu diesem Zeitpunkt:

Rufsituation von 2420 zu 7280 (Sektor 181 zu GW-Sektor 175).

```
ABFRAGEN-GKTOP:TYP=ALLE,ANZEIGE=DYN;


---------
+-------------------------------------------------------------------
+

   SEKTOR   |               100
                |

   ---------
+-----------------------------------------------------------
+

   PKNNR    |         10- 30-200
                |
```

```
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                  0
             |
   R-GW-MC   |                  0
             |
   R-GW-DMC  |                  0
             |
   ---------
+-------------------------------------------------------------
+
   SEKTOR    |               170
             |
   ---------
+-------------------------------------------------------------
+
   PKNNR     |         10- 30-200
             |
   ---------
+-------------------------------------------------------------
+
   S-BB      |         UNBEGRENZT
             |
   VERW-BB   |                  0
             |
   R-GW-MC   |                 60
             |
   R-GW-DMC  |                 45
             |
   ---------
+-------------------------------------------------------------
+
   SEKTOR    |               171
             |
```

```
   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               150
               |

   VERW-BB  |                 0
               |

   R-GW-MC  |                 0
               |

   R-GW-DMC |                 0
               |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               172
               |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
               |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
               |

   VERW-BB  |               220
               |

   R-GW-MC  |                 0
               |

   R-GW-DMC |                 0
               |

   ---------
+-------------------------------------------------------------
+
```

```
   SEKTOR   |              175
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                0
            |

   R-GW-MC  |               58
            |

   R-GW-DMC |               44
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |              176
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                0
            |

   R-GW-MC  |               59
            |

   R-GW-DMC |               45
            |
```

```
   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               180
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |               122
            |

   VERW-BB  |                78
            |

   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+

   SEKTOR   |               181
            |

   ---------
+-------------------------------------------------------------
+

   PKNNR    |        10- 30-200
            |

   ---------
+-------------------------------------------------------------
+

   S-BB     |        UNBEGRENZT
            |

   VERW-BB  |                78
            |
```

```
   R-GW-MC  |                 0
            |

   R-GW-DMC |                 0
            |

   ---------
+-------------------------------------------------------------
+


ABFRAGEN-SIPCO:TYP=BANDW;
  BANDBREITENBERECHNUNGSTABELLE:



 ------------------------------------------------------------------------

  +-------+----------------------+-----------------
+---------------+

  | INDEX |  CODEC TYP           | RAHMENGROESSE   |
 RESERVIERTE   |

  |       |                      |     (MS)        |
 BANDBR.(KBIT) |

  +-------+----------------------+-----------------
+---------------+

  |    1  | G711_HFA             |       30        |
 89     |

  |    2  | G729_HFA             |       40        |
 36     |

  |    3  | G723_HFA             |       30        |
 25     |

  |    4  | G711_F10_IPDA        |       10        |
 120     |

  |    5  | G711_F20_IPDA        |       20        |
 184     |

  |    6  | G711_F30_IPDA        |       30        |
 83     |

  |    7  | G711_F60_IPDA        |       60        |
 74     |

  |    8  | G729_F20_IPDA        |       20        |
 36     |

  |    9  | G729_F40_IPDA        |       40        |
 22     |
```

```
  |   10  | G729_F60_IPDA         |        60         |
18     |

  |   11  | G711_DMC              |        30         |
182    |

  |   12  | G729_DMC              |        40         |
78     |

  |   13  | G723_DMC              |        30         |
27     |

  |   14  | G711_FS_UNKNOWN       |        60         |
83     |
```

Interpretation:

Es wird die Bandbreite in dem Sektoren für HFA (180 und 181) reserviert. Hier wird für die komprimierte DMC-Verbindung die Bandbreite aus Index 12 berechnet, da der Pauschalwert im Index 12 grösser ist als der doppelte Wert aus Index 2. Im Sektor 172 wird die Masterverbindung mit G711 (Index 5) zwischen den APs addiert mit der Bandbreite der Masterverbindung von HFA-Telefon zur HG 3530 (G729, Index 2).

Im GW-Sektor 176 ist nur die Masterverbindung aktiv, d.h. nur ein Master-Kanal ist belegt (59 frei). Im Sektor 175 ist die Masterverbindung und eine DMC-Verbindung aktiv, d.h. 2 DSP-Kanäle sind belegt, von denen einer für die Master-Verbindung und der andere für die DMC-Verbindung benutzt wird (58/44 frei).

2.17.8 Anmerkungen und Einschränkungen

Bemerkungen zu RM:

- RESMAN sollte nie eine Route mit mehr als 16 Sektoren enthalten.
- **Es werden** nur **WAN-Sektoren bei der Bandbreitenberechnung unterstützt, jedoch** keine LAN-Sektoren.
- Jedes **RESMGMT1**-Segment aus der AMO GKTOP muss die AMO ZAND **PKNNO** unter dem Parameter **PKNNO** enthalten, d.h. dies ist **nicht** der AMO KNDEF-Eintrag.
- IP-Trunking wird nicht unterstützt.
- Die netzweite Konfiguration ist extrem zeitaufwändig, und wenn ein Partnersystem einen fehlerhaften Sektor empfängt, wird DMC nicht geschaltet (eine einfachere alternative Konfiguration finden Sie in MSC15245).
- In einer DMC-Verbindung wird die Bandbreite bei einem Codec niedrigerer Qualität so lange nicht verringert, bis die Verbindung getrennt ist. Wird für die DMC-Verbindung eine höhere Bandbreite verwendet, so wird der Wert wie üblich erhöht.
- MOBHFA wird unterstützt. Nach erfolgreicher Anmeldung wird die Cluster-ID des Gastanschlusses ebenfalls gespeichert. Bei der Bandbreitenberechnung wird die Strecke vom Gastanschluss zum Home-Gateway und weiter zum gerufenen Teilnehmer berücksichtigt. DMC kann die Bandbreite auch in

Abhängig davon erhöhen, welcher CODEC für die Master-Verbindung verwendet wird.

- Die Bandbreite wird **immer** der Konfiguration entsprechend errechnet, d.h. von Hostsystem in Richtung des AP. Bei Verbindungen zwischen zwei APs werden die Routen miteinander verglichen, um die richtige Route zu ermitteln.
- Zur korrekten Bandbreitenberechnung muss bei HFA-Telefonen der AMO SBCSU-Parameter **IPCODEC** konfiguriert werden.
- Bei Verwendung der AMO KCSU erfolgt keine Bandbreitenreservierung im Rufzustand (erst bei hergestellter Verbindung).
- Jedes Gateway sollte mit einem LAN-Sektor (und nicht direkt mit dem WAN!) verbunden sein.

2.17.9 Diagnose

Überprüfung der zur Zeit benutzten Bandbreite aller Sektoren:
`ABFRAGEN-GKTOP:TYP=RESMGMT1,ANZEIGE=DYN;`

Will man die Einrichtung des Ressource Managements überprüfen, so ist es in dieser Darstellung zunächst erst einmal ausreichend, wenn man Gesprächsverbindungen über alle eingerichteten Wegen aufbaut. Dann sollte man, wenn die zulässige Bandbreite in einem Sektor überschritten wird, gassenbesetzt erhalten.

Keine Bandbreite verfügbar

Bei konfiguriertem Ressourcenmanager sind manchmal Verbindungen gesperrt, wenn keine Ressourcen frei sind. In diesem Fall wird eine Hinweismeldung F4436 ausgegeben. In der Regel ist die Ursache für die Fehlermeldung zutreffend und durch die Konfiguration definiert, d.h. es versuchen mehr Verbindungen, einen Pfad zu verwenden, als laut der AMO GKTOP-Konfiguration zulässig sind, oder eine DMC-Verbindung wurde durch das AMO GKTOP-Attribut **NODMC** eingeschränkt. In Ausnahmefällen wird die Hinweismeldung aufgrund hängender Bandbreite ausgegeben. Dies bedeutet, dass ein DIS-GKTOP anzeigt, dass Bandbreite belegt ist, obwohl auf dem betreffenden Pfad keine Verbindungen aktiv sind. Hängende Bandbreite kann durch Ausführen eines DIS-GKTOP während eines Zeitraums mit geringem Verkehrsaufkommen überprüft werden.

Die Fehlermeldung F4436 enthält wichtige Hinweise dazu, welche Route genau nicht verfügbar ist.

2.18 Command Line Interface CLI beim HG 3500

2.18.1 Allgemeine Informationen

Das Common Gateway unterstützt ein Command Line Interface (CLI) für die Installation und Grundkonfiguration, beispielsweise für eine IP-Infrastruktur. Über das V.24-CLI lassen sich sicherheitsrelevante Daten (z. B. die SSL-Konfiguration) ändern, da V.24 als sicher gilt. Außerdem erlaubt das CLI die Überwachung wichtiger Zähler und Statistiken.

Der Zugriff auf CLI ist über V.24, nicht aber über Telnet möglich, da Telnet ein unsicheres Protokoll ist.

Um einen Überblick über die Befehle zu erhalten, geben Sie den Befehl `help` ein und Sie erhalten eine alphabetische Liste aller Befehle.

Wie Sie die Zugangsdaten für die CLI konfigurieren, erfahren Sie unter Kapitel 13.10, „TYP SERVIF - Ändern von Login und Passwort für den Service-Zugang“.

Im Folgenden wird die Grundfunktion des CLI beschrieben. In den folgenden Abschnitten werden die CLI-Befehle in sieben Kategorien eingeteilt:

- Allgemeine Operationen
- Zugriffskontrolle
- Gateway-Setup
- Handling von Images/Dateien
- Wartung
- SSL für WBM
- DLS

Anmerkung: Die CLI wird auf STMIX nicht unterstützt.

2.18.2 Allgemeine Operationen

Um eine Sitzung zu eröffnen, muss sich der Administrator authentifizieren. Hierzu muss der Admin-Name und das Passwort eingegeben werden.

- Um die Sitzung zu verlassen, verwenden Sie den

logout

- Befehl.
- Eine Liste sämtlicher unterstützter Befehle (außer den versteckten Befehlen) erhalten Sie über die:

help

2.18.3 Zugriffskontrolle

- Bevor Speicher-, Upload- und Download-Befehle ausgeführt werden können, benötigen Sie Schreibzugriff für die Konfiguration. Aufgrund der implementierten „weichen Sperre“ muss zuerst überprüft werden, ob ein anderer Benutzer den Schreibzugriff gesetzt hat.

who has write access

get write access

release write access

2.18.4 Gateway-Setup

Die folgenden Befehle sind erforderlich, um Konfigurationsaktivitäten für die System-Initialisierung und Grundverwaltung zuzulassen.

- Einstellen und Ändern des Gateway-Namens:

set hostname <Hostname>

- Der Parameter `Hostname` ist ein zufälliger Name für das Gateway und muss ein Zeichen-String sein (setzen Sie den Hostname z. B. auf Gateway1). Der Name stimmt mit dem Bootline-Parameter „Zielname“ überein.
- Einstellen und Ändern der IP-Adresse für den Ethernet-Port:

set ip address <IP-Adresse>

set ip subnet <IP-Subnetz-Maske>

Der Parameter `IP-Adresse` ist ein String im Format x.x.x.x, wobei x ein Integer ist (z. B. 1.2.3.4).

Der Parameter `IP-Subnetz-Maske` ist ein String im Format x.x.x.x, wobei x ein Integer zwischen 0 und 255 ist (z. B. 255.255.255.224).

Damit Einstellungen oder Änderungen der IP-Adresse oder des IP-Subnetzes für den Ethernet-Port wirksam werden, ist vermutlich ein Gateway-Neustart nötig.

- Einstellen und Ändern der IP-Adresse des Default-Gateways über die Tabelle der statischen Routen:

set default gateway <IP-Adresse>

- Der Parameter `IP-Adresse` ist ein String im Format x.x.x.x, wobei x ein Integer ist (z. B. 1.2.3.4).
- Anzeigen/Ändern des ausgewählten Identifiers:

  get id <parameter name>

  set id <parameter name>

2.18.5 Handling von Images/Dateien

Bei Common Gateway-Software ist weder eine Konfiguration und Distribution noch der Upload oder Download von Konfigurationsdaten über CLI erforderlich, da dies über WBM erfolgt.

Zudem werden Operationen für die Analyse von Event- und Trace-Daten unterstützt.

Die Trace-/Event-Protokolle sind verfügbar unter:
`/trace/trace.txt`

`/trace/trace.bak`
`/evtlog/evtlog.txt`

`/evtlog/evtlog.bak`

2.18.6 Wartung

Mit den Wartungsbefehlen lässt sich der aktuelle Betriebsstatus des Gateways untersuchen, außerdem ist der Zugriff auf Diagnose-Tools sowie auf die Interface- und Gateway-Steuerung möglich.

Anzeige

- Befehle, die Informationen über die Software-Konfiguration des Gateways bereitstellen:

  show version

  show uptime
- Anzeigen der IP-Adresse, des Subnetzes und des Gateways:

  show all parameters
- Anzeigen des Hostnamens und der IP-Adressen:

  show host
- Abfragen des Gateway-Namens:

  show hostname
- Anzeigen des Arp-Caches:

  show arp cache
- Dieser ist außerdem in der Bootline als Zielname gespeichert.
- Anzeigen der IP-Adresse und der Subnetzmaske für den Ethernet-Port:

  show ip address

  show ip subnet
- Bei der Zeitangabe wird die Zeit und das Datum angezeigt:

  show time
- Befehl zur Abfrage der IP-Adresse des Standard-Gateways aus der Tabelle der statischen Routen:

  show default gateway
- Befehl zum Anzeigen der Einträge der statischen Routen:

  show routes
- Anzeigen der Statistiken der Interface-Tabelle:

  show if counters
- Auflistung aller bestehenden Schnittstellen:

  show interfaces
- Abfragen der Admin- und Betriebszustände:

  show if states

  Ping und Tracert
- Diagnose-Befehle:

  ping <ip address>

  Target-Shell
- vxWorks Shell-Logon/-Logout:

  shell

  exit

Gateway-Neustart

Für den Administrator sind zwei unterschiedliche Neustart-Befehle interessant. Einerseits muss das Gateway mit der aktuellen Konfiguration neu gestartet werden. Andererseits könnte die Unterstützung für einen Konfigurationsdatenaustausch erforderlich sein, d. h. es soll eine externe Konfigurationsdaten-Datei verwendet werden, oder es soll der aktuelle

Konfigurationsdatenspeicher ausgelassen und der nächstältere verwendet werden.

Der Administrator ist für die Koordinierung eines Gateway-Neustarts verantwortlich.

- Normaler Gateway-Neustart mithilfe der aktuellen Konfigurationsdaten:

  reset
- Zurücksetzen sämtlicher Konfigurationsdaten auf die Werkseinstellung und Neustart:

  reset factory
- Spezieller Gateway-Neustart mithilfe eines selbstextrahierenden Images, um einen Software-Download abzuschließen:

  activate software

2.18.7 SSL für WBM

SSL für WBM (z.B. https) ist im Auslieferungszustand aktiviert. Es kann nicht deaktiviert werden.

Folgende Befehle sind für die Grundkonfiguration von SSL erforderlich.

- Anzeigen des Fingerabdrucks des aktuellen aktivierten Zertifikates für den WBM-Zugriff über https.

  show fingerprint
- Vor Bestätigung einer Zertifikat-Warnung im Browser, wird dringend empfohlen, dass der Administrator den im Browser angezeigten Fingerabdruck mit dem Fingerabdruck vergleicht, der im CLI angezeigt wird. Das Zertifikat darf nur bestätigt werden, wenn beide Fingerabdrücke identisch sind.

2.18.8 DLS

- IP-Adresse des DLS-Servers setzen
  `set dls ip_address <ip address[:port]>`

  Die IP-Adresse des DLS-Servers kann optional manuell mittels `set dls ip_address` konfiguriert werden. Alternativ wird die IP-Adresse automatisch eingetragen, wenn am DLS die Funktion **IP Devices > IP Device Interaktion > IP Devices scannen** verwendet wird (dabei die Checkbox **Sende DLS Adresse** im **Register „Konfiguration“** aktivieren!).
- IP-Adresse des DLS-Servers anzeigen
  `show dls ip_address`

  Das Gateway enthält einen DLS-Client. Damit ist die IP-Adresse des DLS-Clients dem Gateway automatisch bekannt.

- DLS-PIN

  IP Devices > IP Device Verwaltung > IP Device Konfiguration > Register „DLS Verbindung“

  Beim Anlegen eines sogenannten virtuellen Gerätes im DLS, gibt es bei den Sicherheitseinstellungen unter **PIN Modus** drei Möglichkeiten:

  – **Keine PIN**,
  – **Standard PIN**,
  – **Individuelle PIN**.

  Siehe auch Kapitel 9, „DLS-Client-Bootstrapping“.

  Wenn im Gateway **dls pin_required** auf **TRUE** gesetzt wird, dann lehnt das Gateway eine Verbindung vom DLS mit der Einstellung **Keine PIN** ab. Diese Einstellung bietet erhöhte Sicherheit.

  Die PIN wird automatisch von DLS generiert und unter **Administration > Workpoint Interface Konfiguration > Register „Secure Modus“** im **Feld Standard PIN:** im DLS angezeigt. Sie hat eine vergleichbare Funktion wie ein Passwort.

  `set dls pin_required <wert>`

  Mögliche Werte:

  – **0**: Es wird keine PIN benötigt. Im DLS ist der **PIN Modus „Keine PIN“** eingestellt.
  – **1**: Eine PIN wird benötigt. Im DLS ist der **PIN Modus „Standard PIN“** oder **„Individuelle PIN“** eingestellt.

  `show dls pin_required`

  Mögliche Werte:

  – **FALSE**: Es wird keine PIN benötigt. Im DLS ist der **PIN Modus „Keine PIN“** eingestellt.
  – **TRUE**: Es wird eine PIN benötigt. Im DLS ist der **PIN Modus „Standard PIN“** oder **„Individuelle PIN“** eingestellt.

- DLS PIN aktivieren

  `activate dls pin <pin>`

  Wenn im DLS als PIN Modus **Standard PIN** oder **Individuelle PIN** gewählt wurde, dann muss mit diesem Kommando die im DLS angezeigte PIN eingegeben werden.

- Bootstrapping

  Mit `reset dls bootstrapping` wird das Gateway bezüglich DLS-Client-Bootstrapping in den Werkszustand versetzt und es kann eine neues Bootstrapping stattfinden (siehe auch Kapitel 9, „DLS-Client-Bootstrapping“).

  `reset dls bootstrapping`

- DLS-Client Status

  Zeigt den Wert „secure“ oder „insecure“ an. In Klammer folgt noch eine Zahl, die nur zu Diagnosezwecken dient.

  `show dls_client_state`

  Mögliche Werte:

  – **secure**: DLS Client Bootstrapping ist bereits erfolgt.
  – **insecure**: DLS Client Bootstrapping wurde noch nicht durchgeführt oder es war nicht erfolgreich.

- DLS-Server kontaktieren
  `contact dls`

  Dieses Kommando versucht den DLS Server zu kontaktieren.

  Dies ist nur nötig, nachdem die IP-Adresse des DLS-Servers manuell mittels `set dls ip_address` konfiguriert wurde, um das DLS Client Bootstrapping zu starten.

  Ansonsten kann `contact dls` verwendet werden um zu testen, ob eine Kommunikation zwischen Gateway und DLS Server möglich ist. Es erscheint eine entsprechende Meldung.

2.18.9 Ändern von Login und Passwort für WBM/CLI

Das CLI-Login muss über die selben Accounts erfolgen wie das WBM-Login. Die jeweiligen Accounts können über AMO CGWB eingerichtet und geändert werden. Der Parameter ROLE legt die Zugriffsrechte fest.

Wichtig: Zweistufuges CLI wird nicht unterstützt.

```
AENDERN-
STMIB:MTYP=CGW,LTU=<LTU>,EBT=<EBT>,TYP=WBMDATA,LOGINWBM=<Benutzer-
Login
für WBM-Verbindung>,PASSWWBM=<Passwort für WBM-
Verbindung>,ROLE=<Rolle des WBM-
Benutzers>;
```

Die Login-Daten für die erstmalige Anmeldung als **engr** lauten

```
Benutzername: HP4K-DEVEL
Passwort: 4K-admin
```

Nach erfolgreichem Login erscheint folgende Meldung:

```
Willkommen zur HG 3575 <Aktuell geladene LW-Version>
 Command
Line Interpreter.
vxTarget>
```

2.19 Command Line Interface CLI beim HG 3575 V4

Siehe „IP Distributed Architecture (IPDA)“ > Kapitel 4, „Lokale Administration des Access Points am CLI mittels Terminal“.

2.20 SNMP Support HG 3500 / HG 3575

Die Baugruppen HG 3500 / HG 3575 unterstützen das Abfragen von Daten über SNMP.Unterstützt werden die Standard-MIB (MIB-2) sowie zwei Private Enterprises MIBs für unternehmensspezifische Gateway-Daten:

MIB-2:

- (1) System Group (RFC1213)
- (2) Interfaces Group (RFC2233)

- (3) AT Group (RFC1213)
- (4) IP Group (RFC2011/RFC1213)
- (5) ICMP Group (RFC2011)
- (6) TCP Group (RFC2012)
- (7) UDP Group (RFC2013)
- (8) EGP Group (RFC1213)
- (10) Transmission Group (RFC2127)
- (11) SNMP Group (RFC1213)
- (16) RMON Group (RFC1757)
- (30) ianaifType (IANA)
- (31) ifMIB Group (RFC2233)

SNI-spezifisch (hg3550) MIB:

- (1) Error Sig Group
- (2) Control Group
- (3) Monitoring Group
- (4) Statistics Group
- (5) Send Alarm with Values (Traps)
- (6) File Overflow (Traps)
- (7) All Serve Group
- (8) Ethernet Statistics Group
- (9) QOS Statistics Group
- (10) B-Channel Statistics Group
- (11) Notification Group (Traps)
- (12) IP Phone Group
- (13) RG2500 MIB (Plattform, Management, globale Daten, Traps, ...)

Firmen-spezifisch (hg3550 v11) MIB:

- (2) I&C Admin MIB (systemOID)

Hinweise

Um die MIBs einem MIB-Browser bekanntzumachen, werden folgende Dateien benötigt:

MIB-2-Teile:

- mib-2.my: standard MIB-II (1.3.6.1.2.1.1-11)
- iana.my: IANAifType (1.3.6.1.2.1.30)
- my_rmon2.my: RMON MIB (1.3.6.1.2.1.16.19)
- rfc2127.my: ISDN-MIB (1.3.6.1.2.1.10.20)
- rfc2233.my: IF-MIB (1.3.6.1.2.1.2 and 1.3.6.1.2.1.31)

SNI-spezifische Teile (hg3550) MIB:

- hg1500.my: HG3550 MIB (1.3.6.1.4.1.231.7.2.7.1-12)
- ar2500_platform.my: Platform MIB (1.3.6.1.4.1.231.7.2.7.13.1)
- ar2500_management.my: Management MIB (1.3.6.1.4.1.231.7.2.7.13.2)
- cg2500.my: CG2500 MIB (1.3.6.1.4.1.231.7.2.7.13.3)

Firmen-spezifische Teile (hg3550 v11) MIB:

- hg3550_v11.my: system OID for hg3550 V2 (1.3.6.1.4.1.4329.2.24)

Diese Dateien sind Teil einer jeden offiziellen Produktion (eingepackt in einer zip-Datei).

Die SNMP MIBs können mit Hilfe des **SNMP-Konfigurator**, Registerkarte **SNMP-Steuerung** im OpenScape 4000 Assistant (**Diagnose > Faul Management**) heruntergeladen werden oder über sftp aus dem Verzeichnis **/ opt/ncc/mib**.

Alle Informationen zu Object Identifiers (OID) finden Sie unter dem folgenden Link: https://wpb.global-intra.net/comwiki/bin/view.pl/Standardization/OIDs.

Mehr Informationen zum SNMP-Konfigurator finden Sie in der Online-Hilfe oder in der OpenScape 4000 Assistant Dokumentation zum Simple Network Management Protocol.

Die SNMP-Signalisierung bestimmter Eventlog-Nachrichten kann unter der Reaktionstabelle in WBM gesteuert werden: Maintenance > Events > Reaction Table.

Einige MIB-Objekte und MIB-Dateien haben alte historisch bedingte Namen. Diese MIB-Objekte und MIB-Dateien sind bereits früher erstellt worden, für vorhergehende Produkte (CG2500, AR2500, HG1500 etc.). Diese Objekte und Dateien wurden für die neuen Produkte mit wenigen (oder gar keinen) Änderungen angepasst und übernommen. Deshalb haben die neuen Produkte (HG 3500, HG 3575) weiterhin die alten Objekt- und Dateinamen.

Die folgenden Tabellen beschreiben die Details der unterstützten Objekte, sortiert nach der Object ID. Die letzte Tabelle enthält eine wiederholte und gesammelte Liste der SNMP-Traps im MIB-Objektbaum.

Die SNMP-Traps sind in der Spalte „Syntax“ mit „TRAP“ gekennzeichnet. Sie werden gesammelt und in der letzten Tabelle wiederholt.

Die Spalte „Zugriff“ enthält Verknüpfungen zu den Zugriffsmöglichkeiten auf die Objektdaten:

- RO: Read-Only
- RW: Read-Write
- RC: Read-Create

Wenn diese Zelle leer ist, dann ist das Objekt kein Daten-Container-Objekt und es kann nicht direkt darauf zugegriffen werden.

Die Texte in der Spalte „Beschreibung“ sind im allgemeinen ein Auszug aus der MIB-Source-Datei. Damit können sie Referenzen zu alten, historischen Produktnamen enthalten. Diese sind aber für die aktuellen Produkte auch gültig.

Weitere Informationen finden Sie in den MIB-Dateien selber.

Tabelle 12: Daten in der Standard MIB-2

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.1	system			System MIB, see mib-2.my
1.3.6.1.2.1.1.1	sysDescr	DisplayString (SIZE (0..255))	RO	Textbeschreibung des Systems, einschließlich des vollständigen Namens und der Versionskennung des Hardwaretyps des Systems, des Software-Betriebssystems und der Netzwerksoftware

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.1.2	sysObjectID	OBJECT IDENTIFIER	RO	Die verbindliche Identifizierung des in der Entität enthaltenen Subsystems für das Netzwerkmanagement durch den Lieferanten
1.3.6.1.2.1.1.3	sysUpTime	TimeTicks	RO	Die Zeit (in Hundertstelsekunden) seit der letzten Neuinitialisierung des Netzwerkmanagementteils des Systems
1.3.6.1.2.1.1.4	sysContact	DisplayString (SIZE (0..255))	RW	Die textliche Identifizierung der Kontaktperson für diesen verwalteten Knoten sowie Informationen darüber, wie Sie diese Person kontaktieren können
1.3.6.1.2.1.1.5	sysName	DisplayString (SIZE (0..255))	RW	Ein vom Administrator zugewiesener Name für diesen verwalteten Knoten. Per Konvention ist dies der vollqualifizierte Domänenname des Knotens.
1.3.6.1.2.1.1.6	sysLocation	DisplayString (SIZE (0..255))	RW	Der physische Standort dieses Knotens.
1.3.6.1.2.1.1.7	sysServices	INTEGER (0..127)	RO	Ein Wert, der die Menge der Dienste angibt, die diese Einheit hauptsächlich anbietet
1.3.6.1.2.1.2	interfaces			MIB-Schnittstellen, siehe mib-2.my und rfc2233.my
1.3.6.1.2.1.2.1	ifNumber	INTEGER	RO	Die Anzahl der auf diesem System vorhandenen Netzwerkschnittstellen (unabhängig vom aktuellen Zustand).
1.3.6.1.2.1.2.2	ifTable	SEQUENCE OF IfEntry		Eine Liste der Interface-Einträge. Die Anzahl der Einträge wird durch den Wert von ifNumber angegeben.
1.3.6.1.2.1.2.2.1	ifEntry	IfEntry		Ein Eintrag mit Verwaltungsinformationen, die für eine bestimmte Schnittstelle gelten.
1.3.6.1.2.1.2.2.1.1	ifIndex	INTEGER	RO	Ein eindeutiger Wert, der größer als Null ist, für jede Schnittstelle.
1.3.6.1.2.1.2.2.1.2	ifDescr	DisplayString (SIZE (0..255))	RO	Eine textuelle Zeichenkette, die Informationen über die Schnittstelle enthält.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.2.2.1.3	ifType	INTEGER	RO	Die Art der Schnittstelle.
1.3.6.1.2.1.2.2.1.4	ifMtu	INTEGER	RO	Die Größe des größten Pakets, das auf der Schnittstelle gesendet/ empfangen werden kann, angegeben in Oktetts.
1.3.6.1.2.1.2.2.1.5	ifSpeed	Gauge	RO	Eine Schätzung der aktuellen Bandbreite der Schnittstelle in Bit pro Sekunde.
1.3.6.1.2.1.2.2.1.6	ifPhysAddress	PhyCountersAddress	RO	Die Adresse der Schnittstelle auf ihrer Protokollunterebene.
1.3.6.1.2.1.2.2.1.7	ifAdminStatus	INTEGER	RW	Der gewünschte Zustand der Schnittstelle. - up(1) bereit, Pakete zu übergeben - down(2) - testing(3) in einem Testmodus
1.3.6.1.2.1.2.2.1.8	ifOperStatus	INTEGER	RO	Der aktuelle Betriebszustand der Schnittstelle. - up(1) bereit, Pakete zu übergeben - down(2) - testing(3) in einem Testmodus - unknown(4) Status kann aus irgendeinem Grund nicht bestimmt werden. - dormant(5) - notPresent(6) fehlt eine Komponente - lowerLayerDown(7) down aufgrund des Zustands der Unterschicht-Schnittstelle(n)
1.3.6.1.2.1.2.2.1.9	ifLastChange	TimeTicks	RO	Der Wert von sysUpTime zum Zeitpunkt, zu dem die Schnittstelle in ihren aktuellen Betriebszustand eingetreten ist.
1.3.6.1.2.1.2.2.1.10	ifInOctets	Counter	RO	Die Gesamtzahl der auf der Schnittstelle empfangenen Oktette, einschließlich Framingzeichen.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.2.2.1.11	ifInUcastPkts	Counter	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die nicht an eine Multicast- oder Broadcast-Adresse in dieser Unterschicht adressiert wurden.
1.3.6.1.2.1.2.2.1.12	ifInNUcastPkts	Counter	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die an eine Multicast- oder Broadcast-Adresse in dieser Unterschicht adressiert wurden. veraltet
1.3.6.1.2.1.2.2.1.13	ifInDiscards	Counter	RO	Die Anzahl der eingehenden Pakete, die so gewählt wurden, dass sie verworfen werden, obwohl keine Fehler erkannt wurden, um zu verhindern, dass sie an ein höherwertiges Protokoll ausgeliefert werden können.
1.3.6.1.2.1.2.2.1.14	ifInErrors	Counter	RO	Bei paketorientierten Schnittstellen die Anzahl der eingehenden Pakete, die Fehler enthielten, die verhindern, dass sie an ein höherwertiges Protokoll ausgeliefert werden können.
1.3.6.1.2.1.2.2.1.15	ifInUnknownProtos	Counter	RO	Bei paketorientierten Schnittstellen die Anzahl der über die Schnittstelle empfangenen Pakete, die aufgrund eines unbekannten oder nicht unterstützten Protokolls verworfen wurden.
1.3.6.1.2.1.2.2.1.16	ifOutOctets	Counter	RO	Die Gesamtzahl der über die Schnittstelle übertragenen Oktette, einschließlich Framingzeichen.
1.3.6.1.2.1.2.2.1.17	ifOutUcastPkts	Counter	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die nicht an eine Multicast- oder Broadcast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.2.2.1.18	ifOutNUcastPkts	Counter	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die an eine Multicast- oder Broadcast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden. veraltet
1.3.6.1.2.1.2.2.1.19	ifOutDiscards	Counter	RO	Die Anzahl der ausgehenden Pakete, die so gewählt wurden, dass sie verworfen werden, obwohl keine Fehler erkannt wurden, um ihre Übertragung zu verhindern.
1.3.6.1.2.1.2.2.1.20	ifOutErrors	Counter	RO	Bei paketorientierten Schnittstellen die Anzahl der ausgehenden Pakete, die aufgrund von Fehlern nicht übertragen werden konnten. Bei paketorientierten Schnittstellen die Anzahl der ausgehenden Pakete, die aufgrund von Fehlern nicht übertragen werden konnten.
1.3.6.1.2.1.2.2.1.21	ifOutQLen	Gauge	RO	Die Länge der Ausgabepaketwarteschlange (in Paketen).
1.3.6.1.2.1.2.2.1.22	ifSpecific	OBJECT IDENTIFIER	RO	Ein Verweis auf MIB-Definitionen, die spezifisch für das jeweilige Medium sind, das zur Realisierung der Schnittstelle verwendet wird. veraltet
1.3.6.1.2.1.3	unter			Adressübersetzung MIB, siehe mib-2.my Hinweis: Diese Gruppe ist von MIB-II veraltet, d.h. sie wird ausschließlich aus Kompatibilitätsgründen mit MIB-I-Knoten aufgenommen und höchstwahrscheinlich von MIB-III-Knoten ausgeschlossen
1.3.6.1.2.1.3.1	atTable	SEQUENCE OF AtEntry		Das MIB-Modul zur Beschreibung generischer Objekte für Unterebenen der Netzwerkschnittstelle. Diese MIB ist eine aktualisierte Version der ifTable von MIB-II und enthält die in RFC 1229 definierten Erweiterungen.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.3.1.1	atEntry	AtEntry		Jeder Eintrag enthält eine NetworkAddress zu „physischer“ Adressäquivalenz
1.3.6.1.2.1.3.1.1.1	atIfIndex	INTEGER	RW	Die Schnittstelle, auf der die Äquivalenz dieses Eintrags wirksam ist
1.3.6.1.2.1.3.1.1.2	atPhysAddress	PhysAddress	RW	Die medienabhängige „physikalische“ Adresse
1.3.6.1.2.1.3.1.1.3	atNetAddress	NetworkAddress	RW	Die Netzwerkadresse (z. B. die IP-Adresse), die der medienabhängigen „physikalischen“ Adresse entspricht
1.3.6.1.2.1.4	ip			IP MIB, see mib-2.my
1.3.6.1.2.1.4.1	ipForwarding	INTEGER	RW	Angabe, ob diese Einheit als IP-Gateway für die Weiterleitung von Datagrammen fungiert, die von dieser Einheit empfangen werden, aber nicht an diese gerichtet sind forwarding(1): als Gateway fungieren not-forwarding(2): NICHT als Gateway agierend
1.3.6.1.2.1.4.2	ipDefaultTTL	INTEGER	RW	Der Standardwert, der in das Feld Time-To-Live des IP-Headers von Datagrammen eingefügt wird, stammt von dieser Entität, wenn ein TTL-Wert nicht vom Transportschichtprotokoll geliefert wird
1.3.6.1.2.1.4.3	ipInReceives	Counter	RO	Die Gesamtzahl der von Schnittstellen empfangenen Eingangsdatagramme, einschließlich der fehlerhaft empfangenen
1.3.6.1.2.1.4.4	ipInHdrErrors	Counter	RO	Die Anzahl der Eingabedatagramme, die aufgrund von Fehlern in ihren IP-Headern verworfen wurden, einschließlich schlechter Prüfsummen, Fehlanpassungen der Versionsnummer, anderer Formatfehler, Überschreitung der Time-to-Live, Fehler bei der Verarbeitung ihrer IP-Optionen usw.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.4.5	ipInAddrErrors	Counter	RO	Die Anzahl der eingegebenen Datagramme wurde verworfen, weil die IP-Adresse im Zielfeld des IP-Headers keine gültige Adresse war, die bei dieser Entität empfangen werden sollte
1.3.6.1.2.1.4.6	ipForwDatagrams	Counter	RO	Die Anzahl der Eingangsdatagramme, für die diese Entität nicht ihr endgültiges IP-Ziel war, wodurch versucht wurde, eine Route zu finden, um sie an dieses endgültige Ziel weiterzuleiten
1.3.6.1.2.1.4.7	ipInUnknownProtos	Counter	RO	Die Anzahl der lokal adressierten Datagramme, die erfolgreich empfangen, aber aufgrund eines unbekannten oder nicht unterstützten Protokolls verworfen wurden
1.3.6.1.2.1.4.8	ipInDiscards	Counter	RO	Die Anzahl der IP-Eingangsdatagramme, bei denen keine Probleme aufgetreten sind, um ihre weitere Verarbeitung zu verhindern, die aber verworfen wurden (z. B. aus Mangel an Pufferspeicher)
1.3.6.1.2.1.4.9	ipInDelivers	Counter	RO	Die Gesamtzahl der erfolgreich an IP-Benutzerprotokolle (einschließlich ICMP) gelieferten Eingabedatenblätter
1.3.6.1.2.1.4.10	ipOutRequests	Counter	RO	Die Gesamtzahl der IP-Datagramme, die lokale IP-Benutzerprotokolle (einschließlich ICMP) an IP bei Anfragen zur Übertragung geliefert haben
1.3.6.1.2.1.4.11	ipOutDiscards	Counter	RO	Die Anzahl der IP-Ausgangsdatagramme, bei denen kein Problem aufgetreten ist, um ihre Übertragung an ihr Ziel zu verhindern, die aber verworfen wurden (z. B. aus Mangel an Pufferplatz)
1.3.6.1.2.1.4.12	ipOutNoRoutes	Counter	RO	Die Anzahl der IP-Datagramme wurde verworfen, da keine Route gefunden werden konnte, um sie an ihr Ziel zu übertragen

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.4.13	ipReasmTimeout	INTEGER	RO	Die maximale Anzahl von Sekunden, die empfangene Fragmente gehalten werden, während sie auf die Wiederzusammenstellung in dieser Einheit warten
1.3.6.1.2.1.4.14	ipReasmReqds	Counter	RO	Die Anzahl der empfangenen IP-Fragmente, die bei dieser Entität wieder zusammengebaut werden mussten
1.3.6.1.2.1.4.15	ipReasmOKs	Counter	RO	Die Anzahl der IP-Datagramme wurde erfolgreich wieder zusammengesetzt
1.3.6.1.2.1.4.16	ipReasmFails	Counter	RO	Die Anzahl der vom IP-Wiederzusammenbau-Algorithmus erkannten Fehler (aus welchem Grund auch immer: Timeout, Fehler usw.)
1.3.6.1.2.1.4.17	ipFragOKs	Counter	RO	Die Anzahl der IP-Datagramme, die in dieser Entität erfolgreich fragmentiert wurden
1.3.6.1.2.1.4.18	ipFragFails	Counter	RO	Die Anzahl der IP-Datagramme, die verworfen wurden, weil sie in dieser Entität fragmentiert werden mussten, aber nicht sein konnten, z. B. weil ihr Don't Fragment Flag gesetzt wurde
1.3.6.1.2.1.4.19	ipFragCreates	Counter	RO	Die Anzahl der IP-Datagrammfragmente, die als Ergebnis der Fragmentierung in dieser Entität erzeugt wurden
1.3.6.1.2.1.4.20	ipAddrTable	SEQUENCE OF IpAddrEntry		Die Tabelle der Adressierungsinformationen, die für die IP-Adressen dieser Stelle relevant sind
1.3.6.1.2.1.4.20.1	ipAddrEntry	IpAddrEntry		Die Adressierungsinformationen für eine der IP-Adressen dieser Organisation
1.3.6.1.2.1.4.20.1.1	ipAdEntAddr	IpAddress	RO	Die IP-Adresse, an die die Adressierungsinformationen dieses Eintrags gerichtet sind, bezieht sich auf Folgendes
1.3.6.1.2.1.4.20.1.2	ipAdEntIfIndex	INTEGER	RO	Der Indexwert, der das Interface, auf das dieser Eintrag zutrifft, eindeutig identifiziert

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.4.20.1.3	ipAdEntNetMask	IpAddress	RO	Die Subnetzmaske, die der IP-Adresse dieses Eintrags zugeordnet ist
1.3.6.1.2.1.4.20.1.4	ipAdEntBcastAddr	INTEGER	RO	Der Wert des am wenigsten signifikanten Bits in der IP-Adresse, die zum Senden von Datagrammen auf der (logischen) Schnittstelle verwendet wird, die der IP-Adresse dieses Eintrags zugeordnet ist
1.3.6.1.2.1.4.20.1.5	ipAdEntReasmMaxSize	INTEGER (0..65535)	RO	Die Größe des größten IP-Datagramms, das diese Entität aus eingehenden IP-fragmentierten Datagrammen, die auf dieser Schnittstelle empfangen werden, wieder zusammensetzen kann
1.3.6.1.2.1.4.21	ipRouteTable	SEQUENCE OF IpRouteEntry		Die IP-Routingtabelle dieser Entität
1.3.6.1.2.1.4.21.1	ipRouteEntry	IpRouteEntry		Eine Route zu einem bestimmten Ziel
1.3.6.1.2.1.4.21.1.1	ipRouteDest	IpAddress	RW	Die Ziel-IP-Adresse dieser Route. Ein Eintrag mit einem Wert von 0.0.0.0 wird als Standardroute betrachtet
1.3.6.1.2.1.4.21.1.2	ipRouteIfIndex	INTEGER	RW	Der Indexwert, der das lokale Interface eindeutig identifiziert, über das der nächste Hop dieser Route erreicht werden soll
1.3.6.1.2.1.4.21.1.3	ipRouteMetric1	INTEGER	RW	Die primäre Routingmetrik für diese Route
1.3.6.1.2.1.4.21.1.4	ipRouteMetric2	INTEGER	RW	Eine alternative Routingmetrik für diese Route
1.3.6.1.2.1.4.21.1.5	ipRouteMetric3	INTEGER	RW	Eine alternative Routingmetrik für diese Route
1.3.6.1.2.1.4.21.1.6	ipRouteMetric4	INTEGER	RW	Eine alternative Routingmetrik für diese Route
1.3.6.1.2.1.4.21.1.7	ipRouteNextHop	IpAddress	RW	Die IP-Adresse des nächsten Hops dieser Route
1.3.6.1.2.1.4.21.1.8	ipRouteType	INTEGER	RW	Die Art der Route
1.3.6.1.2.1.4.21.1.9	ipRouteProto	INTEGER	RO	Der Routing-Mechanismus, über den diese Route erlernt wurde

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.4.21.1.10	ipRouteAge	INTEGER	RW	Die Anzahl der Sekunden, seit diese Route zuletzt aktualisiert oder anderweitig als korrekt eingestuft wurde
1.3.6.1.2.1.4.21.1.11	ipRouteMask	IpAddress	RW	Geben Sie an, dass die Maske logisch mit der Zieladresse verbunden ist, bevor sie mit dem Wert im Feld ipRouteDest verglichen wird
1.3.6.1.2.1.4.21.1.12	ipRouteMetric5	INTEGER	RW	Eine alternative Routingmetrik für diese Route
1.3.6.1.2.1.4.21.1.13	ipRouteInfo	OBJECT IDENTIFIER	RO	Ein Verweis auf MIB-Definitionen, die spezifisch für das jeweilige Routing-Protokoll sind, das für diese Route verantwortlich ist, bestimmt durch den Wert, der im ipRouteProto-Wert der Route angegeben ist
1.3.6.1.2.1.4.22	ipNetToMediaTable	SEQUENCE OF IpNetToMediaEntry		Die Tabelle IP Address Translation, die für die Zuordnung von IP-Adressen zu physischen Adressen verwendet wird
1.3.6.1.2.1.4.22.1	ipNetToMediaEntry	IpNetToMediaEntry		Jeder Eintrag enthält eine IpAddress zu „physischer“ Adressäquivalenz
1.3.6.1.2.1.4.22.1.1	ipNetToMediaIfIndex	INTEGER	RW	Die Schnittstelle, auf der die Äquivalenz dieses Eintrags wirksam ist
1.3.6.1.2.1.4.22.1.2	ipNetToMediaPhysAddress	PhysAddress	RW	Die medienabhängige „physikalische“ Adresse
1.3.6.1.2.1.4.22.1.3	ipNetToMediaNetAddress	IpAddress	RW	Die IpAddress, die der medienabhängigen „physikalischen“ Adresse entspricht
1.3.6.1.2.1.4.22.1.4	ipNetToMediaType	INTEGER	RW	Die Art der Zuordnung
1.3.6.1.2.1.4.23	ipRoutingDiscards	Counter	RO	Die Anzahl der Routing-Einträge, die ausgewählt wurden, um verworfen zu werden, obwohl sie gültig sind
1.3.6.1.2.1.5	icmp			ICMP MIB, see mib-2.my

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.5.1	icmpInMsgs	Counter	RO	Die Gesamtzahl der ICMP-Nachrichten, die die Entität empfangen hat
1.3.6.1.2.1.5.2	icmpInErrors	Counter	RO	Die Anzahl der ICMP-Nachrichten, die die Entität empfangen hat, die aber als ICMP-spezifisch fehlerhaft eingestuft wurde (schlechte ICMP-Prüfsummen, schlechte Länge, etc.)
1.3.6.1.2.1.5.3	icmpInDestUnreachs	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Ziel unerreichbar“
1.3.6.1.2.1.5.4	icmpInTimeExcds	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Zeit überschritten“
1.3.6.1.2.1.5.5	icmpInParmProbs	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Parameterproblem“
1.3.6.1.2.1.5.6	icmpInSrcQuenchs	Counter	RO	Die Anzahl der empfangenen ICMP Source Quench-Nachrichten
1.3.6.1.2.1.5.7	icmpInRedirects	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Umleiten“
1.3.6.1.2.1.5.8	icmpInEchos	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Echo (Anforderung)“
1.3.6.1.2.1.5.9	icmpInEchoReps	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Echo Antwort“
1.3.6.1.2.1.5.10	icmpInTimestamps	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Zeitstempel (Anforderung)“
1.3.6.1.2.1.5.11	icmpInTimestampReps	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Zeitstempel Antwort“
1.3.6.1.2.1.5.12	icmpInAddrMasks	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Adressenmaske-Anforderung“
1.3.6.1.2.1.5.13	icmpInAddrMaskReps	Counter	RO	Die Anzahl der empfangenen ICMP-Nachrichten „Adressenmaske-Antwort“
1.3.6.1.2.1.5.14	icmpOutMsgs	Counter	RO	Die Gesamtzahl der ICMP-Nachrichten, die die Entität versucht hat zu senden

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.5.15	icmpOutErrors	Counter	RO	Die Anzahl der ICMP-Nachrichten, die diese Entität nicht gesendet hat, aufgrund von Problemen, die innerhalb von ICMP entdeckt wurden, wie z. B. ein Mangel an Puffern
1.3.6.1.2.1.5.16	icmpOutDestUnreachs	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Ziel unerreichbar“
1.3.6.1.2.1.5.17	icmpOutTimeExcds	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Zeit überschritten“
1.3.6.1.2.1.5.18	icmpOutParmProbs	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Parameterproblem“
1.3.6.1.2.1.5.19	icmpOutSrcQuenchs	Counter	RO	Die Anzahl der gesendeten ICMP Source Quench-Nachrichten
1.3.6.1.2.1.5.20	icmpOutRedirects	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Umleiten“
1.3.6.1.2.1.5.21	icmpOutEchos	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Echo (Anforderung)“
1.3.6.1.2.1.5.22	icmpOutEchoReps	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Echo Antwort“
1.3.6.1.2.1.5.23	icmpOutTimestamps	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Zeitstempel (Anforderung)“
1.3.6.1.2.1.5.24	icmpOutTimestampReps	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Zeitstempel Antwort“
1.3.6.1.2.1.5.25	icmpOutAddrMasks	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Adressenmaske-Anforderung“
1.3.6.1.2.1.5.26	icmpOutAddrMaskReps	Counter	RO	Die Anzahl der gesendeten ICMP-Nachrichten „Adressenmaske-Antwort“
1.3.6.1.2.1.6	tcp			TCP MIB, siehe mib-2.my
1.3.6.1.2.1.6.1	tcpRtoAlgorithm	INTEGER	RO	Der Algorithmus, der verwendet wird, um den Timeout-Wert zu bestimmen, der für die erneute Übertragung von nicht bestätigten Oktetts verwendet wird

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.6.2	tcpRtoMin	INTEGER	RO	Der von einer TCP-Implementierung zulässige Mindestwert für den Timeout der erneuten Übertragung, gemessen in Millisekunden
1.3.6.1.2.1.6.3	tcpRtoMax	INTEGER	RO	Der von einer TCP-Implementierung zulässige Maximalwert für den Wiederholungs-Timeout, gemessen in Millisekunden
1.3.6.1.2.1.6.4	tcpMaxConn	INTEGER	RO	Die Begrenzung der Gesamtzahl der TCP-Verbindungen, die die Entität unterstützen kann. In Entitäten, bei denen die maximale Anzahl von Verbindungen dynamisch ist, sollte dieses Objekt den Wert -1 enthalten
1.3.6.1.2.1.6.5	tcpActiveOpens	Counter	RO	Die Anzahl der TCP-Verbindungen, bei denen ein direkter Übergang in den Zustand SYN-SENT aus dem Zustand CLOSED erfolgt ist
1.3.6.1.2.1.6.6	tcpPassiveOpens	Counter	RO	Die Anzahl der TCP-Verbindungen, bei denen ein direkter Übergang in den SYN-RCVD-Zustand aus dem Zustand LISTEN erfolgt ist
1.3.6.1.2.1.6.7	tcpAttemptFails	Counter	RO	Die Anzahl der TCP-Verbindungen, die einen direkten Übergang in den Zustand CLOSED entweder aus dem Zustand SYN-SENT oder dem Zustand SYN-RCVD vollzogen haben, sowie die Anzahl der TCP-Verbindungen, die einen direkten Übergang in den Zustand LISTEN aus dem Zustand SYN-RCVD vollzogen haben
1.3.6.1.2.1.6.8	tcpEstabResets	Counter	RO	Die Anzahl der TCP-Verbindungen, bei denen ein direkter Übergang in den Zustand CLOSED entweder aus dem Zustand ESTABLISHED oder dem Zustand CLOSE-WAIT erfolgt ist
1.3.6.1.2.1.6.9	tcpCurrEstab	Gauge	RO	Die Anzahl der TCP-Verbindungen, bei denen der aktuelle Zustand entweder ESTABLISHED oder CLOSE- WAIT ist

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.6.10	tcpInSegs	Counter	RO	Die Gesamtzahl der empfangenen Segmente, einschließlich der fehlerhaft empfangenen Segmente
1.3.6.1.2.1.6.11	tcpOutSegs	Counter	RO	Die Gesamtzahl der gesendeten Segmente, einschließlich derjenigen auf aktuellen Verbindungen, jedoch ohne diejenigen, die nur wieder übertragene Oktette enthalten
1.3.6.1.2.1.6.12	tcpRetransSegs	Counter	RO	Die Gesamtzahl der wieder übertragenen Segmente – d. h. die Anzahl der übertragenen TCP-Segmente, die ein oder mehrere zuvor übertragene Oktette enthalten
1.3.6.1.2.1.6.13	tcpConnTable	SEQUENCE OF TcpConnEntry		Eine Tabelle mit TCP-Verbindungsspezifischen Informationen
1.3.6.1.2.1.6.13.1	tcpConnEntry	TcpConnEntry		Informationen über eine bestimmte aktuelle TCP-Verbindung
1.3.6.1.2.1.6.13.1.1	tcpConnState	INTEGER	RW	Der Status dieser TCP-Verbindung
1.3.6.1.2.1.6.13.1.2	tcpConnLocalAddress	IpAddress	RO	Die lokale IP-Adresse für diese TCP-Verbindung
1.3.6.1.2.1.6.13.1.3	tcpConnLocalPort	INTEGER (0..65535)	RO	Die lokale Portnummer für diese TCP-Verbindung
1.3.6.1.2.1.6.13.1.4	tcpConnRemAddress	IpAddress	RO	Die entfernte IP-Adresse für diese TCP-Verbindung
1.3.6.1.2.1.6.13.1.5	tcpConnRemPort	INTEGER (0..65535)	RO	Die Nummer des Remote-Ports für diese TCP-Verbindung
1.3.6.1.2.1.6.14	tcpInErrs	Counter	RO	Die Gesamtzahl der fehlerhaft empfangenen Segmente (z. B. schlechte TCP-Prüfsummen)
1.3.6.1.2.1.6.15	tcpOutRsts	Counter	RO	Die Anzahl der gesendeten TCP-Segmente, die das RST-Flag enthalten
1.3.6.1.2.1.7	udp			UDP MIB, siehe mib-2.my
1.3.6.1.2.1.7.1	udpInDatagrams	Counter	RO	Die Gesamtzahl der UDP-Datagramme, die an UDP-Benutzer geliefert wurden

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.7.2	udpNoPorts	Counter	RO	Die Gesamtzahl der empfangenen UDP-Datagramme, für die es am Ziel-Port keine Anwendung gab
1.3.6.1.2.1.7.3	udpInErrors	Counter	RO	Die Anzahl der empfangenen UDP-Datagramme, die aus anderen Gründen als dem Fehlen einer Anwendung am Ziel-Port nicht geliefert werden konnten
1.3.6.1.2.1.7.4	udpOutDatagrams	Counter	RO	Die Gesamtzahl der von dieser Entität gesendeten UDP-Datagramme
1.3.6.1.2.1.7.5	udpTable	SEQUENCE OF UdpEntry		Eine Tabelle mit Informationen über den UDP-Listener
1.3.6.1.2.1.7.5.1	udpEntry	udpEntry		Informationen über einen bestimmten aktuellen UDP-Listener
1.3.6.1.2.1.7.5.1.1	udpLocalAddress	IpAddress	RO	Die lokale IP-Adresse für diesen UDP-Listener
1.3.6.1.2.1.7.5.1.2	udpLocalPort	INTEGER (0..65535)	RO	Die lokale Portnummer für diesen UDP-Listener
1.3.6.1.2.1.8	egp			EGP MIB, siehe mib-2.my
1.3.6.1.2.1.8.1	egpInMsgs	Counter	RO	Die Anzahl der fehlerfrei empfangenen EGP-Nachrichten
1.3.6.1.2.1.8.2	egpInErrors	Counter	RO	Die Anzahl der empfangenen EGP-Nachrichten, die sich als fehlerhaft erwiesen haben
1.3.6.1.2.1.8.3	egpOutMsgs	Counter	RO	Die Gesamtzahl der lokal erzeugten EGP-Nachrichten
1.3.6.1.2.1.8.4	egpOutErrors	Counter	RO	Die Anzahl der lokal erzeugten EGP-Nachrichten, die aufgrund von Ressourcenbeschränkungen innerhalb einer EGP-Einheit nicht gesendet wurden
1.3.6.1.2.1.8.5	egpNeighTable	SEQUENCE OF EgpNeighEntry		Die EGP-Nachbarschaftstabelle
1.3.6.1.2.1.8.5.1	egpNeighEntry	EgpNeighEntry		Informationen über die Beziehung dieser Einheit zu einem bestimmten EGP-Nachbarn

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.8.5.1.1	egpNeighState	INTEGER	RO	Der EGP-Zustand des lokalen Systems in Bezug auf den EGP-Nachbarn dieses Eintrags
1.3.6.1.2.1.8.5.1.2	egpNeighAddr	IpAddress	RO	Die IP-Adresse des EGP-Nachbarn dieses Eintrags
1.3.6.1.2.1.8.5.1.3	egpNeighAs	INTEGER	RO	Das autonome System dieses EGP-Peers
1.3.6.1.2.1.8.5.1.4	egpNeighInMsgs	Counter	RO	Die Anzahl der EGP-Nachrichten, die ohne Fehler von diesem EGP-Peer empfangen wurden
1.3.6.1.2.1.8.5.1.5	egpNeighInErrs	Counter	RO	Die Anzahl der von diesem EGP-Peer empfangenen EGP-Nachrichten, die sich als fehlerhaft erwiesen haben (z. B. schlechte EGP-Prüfsumme)
1.3.6.1.2.1.8.5.1.6	egpNeighOutMsgs	Counter	RO	Die Anzahl der lokal erzeugten EGP-Nachrichten an diesen EGP-Peer
1.3.6.1.2.1.8.5.1.7	egpNeighOutErrs	Counter	RO	Die Anzahl der lokal erzeugten EGP-Nachrichten, die aufgrund von Ressourcenbeschränkungen innerhalb einer EGP-Einheit nicht an diesen EGP-Peer gesendet wurden
1.3.6.1.2.1.8.5.1.8	egpNeighInErrMsgs	Counter	RO	Die Anzahl der von diesem EGP-Peer empfangenen EGP-definierten Fehlermeldungen
1.3.6.1.2.1.8.5.1.9	egpNeighOutErrMsgs	Counter	RO	Die Anzahl der von der EGP definierten Fehlermeldungen, die an diesen EGP-Peer gesendet wurden
1.3.6.1.2.1.8.5.1.10	egpNeighStateUps	Counter	RO	Die Anzahl der EGP-Zustände, die mit diesem EGP-Peer in den UP-Zustand übergehen
1.3.6.1.2.1.8.5.1.11	egpNeighStateDowns	Counter	RO	Die Anzahl der EGP-Zustandsübergänge vom UP-Zustand in einen beliebigen anderen Zustand mit diesem EGP-Peer
1.3.6.1.2.1.8.5.1.12	egpNeighIntervalHello	INTEGER	RO	Das Intervall zwischen EGP Hello Befehlswiederholungen (in Hundertstelsekunden)

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.8.5.1.13	egpNeighIntervalPoll	INTEGER	RO	Das Intervall zwischen den Wiederholungen von EGP-Pollbefehlen (in Hundertstelsekunden)
1.3.6.1.2.1.8.5.1.14	egpNeighMode	INTEGER	RO	Der Polling-Modus dieser EGP-Einheit, entweder passiv oder aktiv active(1), passive(2)
1.3.6.1.2.1.8.5.1.15	egpNeighEventTrigger	INTEGER	RW	Eine Steuervariable, die verwendet wird, um vom Bediener initiierte Start- und Stoppereignisse auszulösen start(1), stop(2)
1.3.6.1.2.1.8.6	egpAs	INTEGER	RO	Die autonome Systemnummer dieser EGP-Einheit
1.3.6.1.2.1.10	transmission			Transmission MIB, siehe rfc2127.my
1.3.6.1.2.1.10.20	isdnMib			Das MIB-Modul zur Beschreibung der Verwaltung von ISDN-Schnittstellen
1.3.6.1.2.1.10.20.1	isdnMibObjects			ISDN MIB-Objektdefinitionen
1.3.6.1.2.1.10.20.1.1	isdnBasicRateGroup			Diese Gruppe beschreibt physikalische Basisraten-Schnittstellen
1.3.6.1.2.1.10.20.1.1.1	isdnBasicRateTable	SEQUENCE OF IsdnBasicRateEntry		Tabelle mit Konfigurations- und Betriebsparametern für alle physikalischen Basisraten-Schnittstellen auf diesem verwalteten Gerät
1.3.6.1.2.1.10.20.1.1.1.1	isdnBasicRateEntry	IsdnBasicRateEntry		Ein Eintrag in der ISDN-Basistabelle
1.3.6.1.2.1.10.20.1.1.1.1.1	isdnBasicRateIfType	INTEGER	RW	Der Typ der physikalischen Schnittstelle Für „S/T“-Schnittstellen, auch „Four-wire Basic Access Interface“ genannt, ist der Wert dieses Objekts isdns(75). Für „U“-Schnittstellen, auch „Two-wire Basic Access Interface“ genannt, ist der Wert dieses Objekts isdnu(76)

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.1.1.2	isdnBasicRateLineTopology	INTEGER	RW	Die Leitungstopologie, die für diese Schnittstelle verwendet werden soll pointToPoint(1), pointToMultipoint(2)
1.3.6.1.2.1.10.20.1.1.1.3	isdnBasicRateIfMode	INTEGER	RW	Der physikalische Schnittstellenmodus. Im TE-Modus ist der Wert dieses Objekts te(1). Im NT-Modus ist der Wert dieses Objekts nt(2)
1.3.6.1.2.1.10.20.1.1.1.4	isdnBasicRateSignalMode	INTEGER	RW	Die Betriebsart des Signalkanals für diese Schnittstelle. Wenn aktiv(1), befindet sich auf dieser Schnittstelle ein Signalisierungskanal. Wenn inaktiv(2), ist ein Signalisierungskanal nicht verfügbar.
1.3.6.1.2.1.10.20.1.2	isdnBearerGroup			Diese Gruppe beschreibt physikalische Basisraten-Schnittstellen
1.3.6.1.2.1.10.20.1.2.1	isdnBearerTable	SEQUENCE OF IsdnBearerEntry		Diese Tabelle definiert portspezifische Betriebs-, Statistik- und aktive Anrufdaten für ISDN-B-Kanäle. Jeder Eintrag in dieser Tabelle beschreibt einen B-Kanal (Träger)
1.3.6.1.2.1.10.20.1.2.1.1	isdnBearerEntry	IsdnBearerEntry		Betriebs- und Statistikinformationen für einen Port. Ein Port ist ein einzelner B-Kanal
1.3.6.1.2.1.10.20.1.2.1.1	isdnBearerChannelType	INTEGER	RW	Der B-Kanaltyp. Wenn der B-Kanal mit einer Wählleitung verbunden ist, hat dieses Objekt den Wert dialup(1). In diesem Fall wird sie von einem zugehörigen Signalkanal gesteuert. Wenn der B-Kanal mit einer Standleitung verbunden ist, hat dieses Objekt einen Wert von leased(2). Für Standleitung B-Kanäle ist keine Signalkanalsteuerung verfügbar

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.2.1.1.2	isdnBearerOperStatus	INTEGER	RO	Der aktuelle Zustand der Anrufsteuerung für diesen Port. idle(1): Der B-Kanal ist im Leerlauf, es findet kein Anruf oder Anrufversuch statt. connecting(2): An dieser Schnittstelle wird ein Verbindungsversuch (abgehender Ruf) durchgeführt. connected(3): Ein eingehender Anruf ist im Prozess der Validierung. active(4): Ein Anruf ist auf dieser Schnittstelle aktiv
1.3.6.1.2.1.10.20.1.2.1.1.3	isdnBearerChannelNumber	INTEGER (1..30)	RO	Der Identifikator, der von einem Signalisierungsprotokoll verwendet wird, um diesen B-Kanal zu identifizieren, auch als B-Kanalnummer bezeichnet
1.3.6.1.2.1.10.20.1.2.1.1.4	isdnBearerPeerAddress	DisplayString	RO	Die ISDN-Adresse, an die der aktuelle oder letzte Anruf angeschlossen ist oder war
1.3.6.1.2.1.10.20.1.2.1.1.5	isdnBearerPeerSubAddress	DisplayString	RO	Die ISDN-Subadresse, an der sich der aktuelle oder letzte Anruf befindet oder war
1.3.6.1.2.1.10.20.1.2.1.1.6	isdnBearerCallOrigin	INTEGER	RO	Der Anrufursprung für den aktuellen oder letzten Anruf unknown(1), originate(2), answer(3), callback(4)
1.3.6.1.2.1.10.20.1.2.1.1.7	isdnBearerInfoType	INTEGER	RO	Die Informationsübertragungsfähigkeit für den aktuellen oder letzten Anruf. speech(2) bezieht sich auf eine Nicht-Datenverbindung, während audio31(6) und audio7(7) auf Datenmodusverbindungen verweisen
1.3.6.1.2.1.10.20.1.2.1.1.8	isdnBearerMultirate	TruthValue	RO	Dieses Flag zeigt an, ob der aktuelle oder letzte Anruf eine Multirate verwendet hat
1.3.6.1.2.1.10.20.1.2.1.1.9	isdnBearerCallSetupTime	TimeStamp	RO	Der Wert von sysUpTime, wenn die ISDN-Setup-Nachricht für den aktuellen oder letzten Anruf gesendet oder empfangen wurde

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.2.1.10	isdnBearerCallConnectTime	TimeStamp	RO	Der Wert von sysUpTime, wenn die ISDN-Verbindungsnachricht für den aktuellen oder letzten Anruf gesendet oder empfangen wurde
1.3.6.1.2.1.10.20.1.2.1.11	isdnBearerChargedUnits	Gauge32	RO	Die Anzahl der geladenen Geräte für die aktuelle oder letzte Verbindung
1.3.6.1.2.1.10.20.1.3	isdnSignalingGroup			Konfigurationstabelle für den Signalkanal
1.3.6.1.2.1.10.20.1.3.1	isdnSignalingGetIndex	TestAndIncr	RW	Die empfohlene Vorgehensweise für die Auswahl eines neuen Index für die Erstellung von isdnSignalingTable-Zeilen ist, den Wert dieses Objekts zu erhalten und dann das Objekt mit dem gleichen Wert festzulegen. Wenn der SET-Vorgang erfolgreich war, kann der Manager diesen Wert als Index verwenden, um eine neue Zeile in dieser Tabelle zu erstellen
1.3.6.1.2.1.10.20.1.3.2	isdnSignalingTable	SEQUENCE OF IsdnSignalingEntry		ISDN-Signaltabelle mit Konfigurations- und Betriebsparametern für alle ISDN-Signalkanäle auf diesem verwalteten Gerät
1.3.6.1.2.1.10.20.1.3.2.1	isdnSignalingEntry	IsdnSignalingEntry		Ein Eintrag in der ISDN-Signaltabelle
1.3.6.1.2.1.10.20.1.3.2.1.1	isdnSignalingIndex	INTEGER (1..2147483647)		Der Indexwert, der einen Eintrag in der isdnSignalingTable eindeutig identifiziert
1.3.6.1.2.1.10.20.1.3.2.1.2	isdnSignalingIfIndex	InterfaceIndex	RO	Der ifIndex-Wert der Schnittstelle, die diesem Signalisierungskanal zugeordnet ist
1.3.6.1.2.1.10.20.1.3.2.1.3	isdnSignalingProtocol	IsdnSignalingProtocol	RC	Der jeweilige Protokolltyp, der von dem Switch unterstützt wird, der den Zugang zu dem ISDN-Netz ermöglicht, mit dem dieser Signalisierungskanal verbunden ist
1.3.6.1.2.1.10.20.1.3.2.1.4	isdnSignalingCallingAddress	DisplayString	RC	Die ISDN-Adresse, die diesem Signalisierungskanal zugeordnet werden soll
1.3.6.1.2.1.10.20.1.3.2.1.5	isdnSignalingSubAddress	DisplayString	RC	Zusatzinformationen zu der diesem Signalisierungskanal zugeordneten ISDN-Adresse

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.3.2.1.6	isdnSignalingBchannelCount	Integer32 (1..65535)	RC	Die Gesamtzahl der B-Kanäle (Trägerkanäle), die von diesem Signalisierungskanal verwaltet werden
1.3.6.1.2.1.10.20.1.3.2.1.7	isdnSignalingInfoTrapEnable	INTEGER	RC	Gibt an, ob für Anrufe auf diesem Signalkanal isdnMibCallInformationstraps generiert werden sollen
1.3.6.1.2.1.10.20.1.3.2.1.8	isdnSignalingStatus	RowStatus	RC	Dieses Objekt dient zum Erstellen und Löschen von Zeilen in der isdnSignalingTable
1.3.6.1.2.1.10.20.1.3.3	isdnSignalingStatsTable	SEQUENCE OF IsdnSignalingStatsEntry		ISDN-Signaltabelle mit Statistikinformationen für alle ISDN-Signalkanäle auf diesem verwalteten Gerät
1.3.6.1.2.1.10.20.1.3.3.1	isdnSignalingStatsEntry	IsdnSignalingStatsEntry		Ein Eintrag in der ISDN-Signalisierungsstatistik Tabelle
1.3.6.1.2.1.10.20.1.3.3.1.1	isdnSigStatsInCalls	Counter32	RO	Die Anzahl der eingehenden Anrufe auf dieser Schnittstelle
1.3.6.1.2.1.10.20.1.3.3.1.2	isdnSigStatsInConnected	Counter32	RO	Die Anzahl der eingehenden Anrufe auf dieser Schnittstelle, die tatsächlich verbunden waren
1.3.6.1.2.1.10.20.1.3.3.1.3	isdnSigStatsOutCalls	Counter32	RO	Die Anzahl der ausgehenden Anrufe auf dieser Schnittstelle
1.3.6.1.2.1.10.20.1.3.3.1.4	isdnSigStatsOutConnected	Counter32	RO	Die Anzahl der ausgehenden Anrufe an dieser Schnittstelle, die tatsächlich verbunden waren
1.3.6.1.2.1.10.20.1.3.3.1.5	isdnSigStatsChargedUnits	Counter32	RO	Die Anzahl der Ladeeinheiten an dieser Schnittstelle seit der Inbetriebnahme des Systems
1.3.6.1.2.1.10.20.1.3.4	isdnLapdTable	SEQUENCE OF IsdnLapdEntry		Tabelle mit Konfigurations- und Statistikinformationen für alle LAPD (D-Kanal Data Link) Schnittstellen auf diesem verwalteten Gerät
1.3.6.1.2.1.10.20.1.3.4.1	isdnLapdEntry	IsdnLapdEntry		An entry in the LAPD Table
1.3.6.1.2.1.10.20.1.3.4.1.1	isdnLapdPrimaryChannel	TruthValue	RW	Wenn auf true(1) gesetzt, ist dieser D-Kanal der angegebene primäre D-Kanal, wenn die D-Kanal-Backup-Funktion aktiv ist
1.3.6.1.2.1.10.20.1.3.4.1.2	isdnLapdOperStatus	INTEGER	RO	Der Betriebszustand dieser Schnittstelle

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.3.4.1.3	isdnLapdPeerSabme	Counter32	RO	Die Anzahl der Peer-SABME-Frames, die auf dieser Schnittstelle empfangen wurden
1.3.6.1.2.1.10.20.1.3.4.1.4	isdnLapdRecvdFrmr	Counter32	RO	Die Anzahl der empfangenen LAPD FRMR Antwortrahmen
1.3.6.1.2.1.10.20.1.4	isdnEndpointGroup			Die Gruppe und Tabelle der Terminal-Endpunkte
1.3.6.1.2.1.10.20.1.4.1	isdnEndpointGetIndex			Die empfohlene Vorgehensweise für die Auswahl eines neuen Index für die Erstellung von isdnEndpointTable-Zeilen ist, den Wert dieses Objekts zu erhalten und dann das Objekt mit dem gleichen Wert festzulegen. Wenn der SET-Vorgang erfolgreich war, kann der Manager diesen Wert als Index verwenden, um eine neue Zeile in dieser Tabelle zu erstellen
1.3.6.1.2.1.10.20.1.4.2	isdnEndpointTable	SEQUENCE OF IsdnEndpointEntry		Tabelle mit der Konfiguration für Terminal-Endpunkte
1.3.6.1.2.1.10.20.1.4.2.1	isdnEndpointEntry	IsdnEndpointEntry		Ein Eintrag in der Terminal-Endpunkt-Tabelle
1.3.6.1.2.1.10.20.1.4.2.1.1	isdnEndpointIndex	INTEGER (1..2147483647)		Der Indexwert, der einen Eintrag in der isdnEndpunktTable eindeutig identifiziert
1.3.6.1.2.1.10.20.1.4.2.1.2	isdnEndpointIfIndex	InterfaceIndex	RO	Der ifIndex-Wert der Schnittstelle, die diesem Terminal-Endpunkt zugeordnet ist
1.3.6.1.2.1.10.20.1.4.2.1.3	isdnEndpointIfType	IANAifType	RC	Der Schnittstellentyp für diesen Terminal-Endpunkt. Schnittstellentypen von x25ple(40) und isdn(63) sind erlaubt
1.3.6.1.2.1.10.20.1.4.2.1.4	isdnEndpointTeiType	INTEGER	RC	Der Typ des TEI (Terminal Endpoint Identifier), der für diesen Terminal-Endpunkt verwendet wird. Im Falle von dynamic(1) wird der TEI-Wert durch den Schalter ausgewählt. Im Falle von static(2) muss ein gültiger TEI-Wert in das isdnEndpointTeiValue-Objekt eingetragen werden

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.1.4.2.1.5	isdnEndpointTeiValue	INTEGER (0..255)	RC	Der TEI-Wert (Terminal Endpoint Identifier) für diesen Terminal-Endpunkt
1.3.6.1.2.1.10.20.1.4.2.1.6	isdnEndpointSpid	DisplayString	RC	Die Service-Profil-IDentifier (SPID)-Informationen für diesen Terminal-Endpunkt
1.3.6.1.2.1.10.20.1.4.2.1.7	isdnEndpointStatus	RowStatus	RC	Dieses Objekt wird verwendet, um Zeilen in der isdnEndpointTable zu erstellen und zu löschen
1.3.6.1.2.1.10.20.1.5	isdnDirectoryGroup			Die Gruppe Verzeichnisnummer
1.3.6.1.2.1.10.20.1.5.1	isdnDirectoryTable	SEQUENCE OF IsdnDirectoryEntry		Tabelle mit Verzeichnisnummern
1.3.6.1.2.1.10.20.1.5.1.1	isdnDirectoryEntry	IsdnDirectoryEntry		Ein Eintrag in der Verzeichnisnummerntabelle
1.3.6.1.2.1.10.20.1.5.1.1.1	isdnDirectoryIndex	INTEGER (1..'7fffffff'h)		Der Indexwert, der einen Eintrag in der isdnDirectoryTable eindeutig identifiziert
1.3.6.1.2.1.10.20.1.5.1.1.2	isdnDirectoryNumber	DisplayString	RC	Eine Verzeichnisnummer. Verzeichnisnummern werden verwendet, um eingehende Anrufe auf dem in isdnDirectorySigIndex angegebenen Signalisierungskanal zu identifizieren
1.3.6.1.2.1.10.20.1.5.1.1.3	isdnDirectorySigIndex	INTEGER (1..2147483647)	RC	Ein Index, der auf einen ISDN-Signalkanal zeigt
1.3.6.1.2.1.10.20.1.5.1.1.4	isdnDirectoryStatus	RowStatus	RC	Dieses Objekt wird verwendet, um Zeilen in der isdnDirectoryTable zu erstellen und zu löschen
1.3.6.1.2.1.10.20.2	isdnMibTrapPrefix			
1.3.6.1.2.1.10.20.2.0	isdnMibTraps			

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.10.20.2.0.1	isdnMibCallInformation	TRAP		Dieser Trap/diese Information wird unter den folgenden Bedingungen an den Manager gesendet: - bei eingehenden Anrufen für jeden Anruf, der aus Richtliniengründen abgelehnt wird (z. B. unbekannter Nachbar oder Zugriffsverletzung) - bei ausgehenden Anrufen, wenn festgestellt wird, dass ein Anrufversuch letztendlich fehlgeschlagen ist. Für den Fall, dass die Anrufwiederholung aktiv ist, erfolgt dies, nachdem alle Wiederholungsversuche fehlgeschlagen sind. - wenn sich ein Anruf verbindet. In diesem Fall sollte das Objekt isdnBearerCallConnectTime in den Trap aufgenommen werden.
1.3.6.1.2.1.10.20.3	isdnMibConformance			
1.3.6.1.2.1.10.20.3.1	isdnMibCompliances			
1.3.6.1.2.1.10.20.3.2	isdnMibGroups			
1.3.6.1.2.1.11	snmp			SNMP MIB, siehe mib-2.my
1.3.6.1.2.1.11.1	snmpInPkts	Counter	RO	Die Gesamtzahl der Nachrichten, die vom Transportdienst an die SNMP-Entität übermittelt wurden
1.3.6.1.2.1.11.2	snmpOutPkts	Counter	RO	Die Gesamtzahl der SNMP-Nachrichten, die von der SNMP-Protokoll-Entität an den Transportdienst weitergeleitet wurden
1.3.6.1.2.1.11.3	snmpInBadVersions	Counter	RO	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protokolleinheit übermittelt wurden und für eine nicht unterstützte SNMP-Version bestimmt waren
1.3.6.1.2.1.11.4	snmpInBadCommunityNames	Counter	RO	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protokoll-Entität übermittelt wurden, die einen SNMP-Community-Namen verwendet, der der Entität nicht bekannt ist

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.11.5	snmpInBadCommunityUses	Counter	RO	Die Gesamtzahl der SNMP-Nachrichten, die an die SNMP-Protokolleinheit übermittelt wurden, die eine SNMP-Operation darstellte, die von der in der Nachricht genannten SNMP-Community nicht erlaubt war
1.3.6.1.2.1.11.6	snmpInASNParseErrs	Counter	RO	Die Gesamtzahl der ASN.1 oder BER-Fehler, die bei der Dekodierung empfangener SNMP-Nachrichten von der SNMP-Protokollentität auftreten
1.3.6.1.2.1.11.7				not used
1.3.6.1.2.1.11.8	snmpInTooBigs	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protokoll-Entität geliefert wurden und für die der Wert des Fehlerstatusfeldes „tooBig“ ist
1.3.6.1.2.1.11.9	snmpInNoSuchNames	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protokoll-Entität geliefert wurden und für die der Wert des Fehlerstatusfeldes „noSuchName“ lautet
1.3.6.1.2.1.11.10	snmpInBadValues	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protokoll-Entität geliefert wurden und für die der Wert des Fehlerstatusfeldes „badValue“ lautet
1.3.6.1.2.1.11.11	snmpInReadOnlys	Counter	RO	Die Gesamtzahl der gültigen SNMP-PDUs, die an die SNMP-Protokoll-Entität geliefert wurden und für die der Wert des Fehlerstatusfeldes „ReadOnly“ lautet
f30h++				
1.3.6.1.2.1.11.12	snmpInGenErrs	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die an die SNMP-Protokoll-Entität geliefert wurden und für die der Wert des Fehlerstatusfeldes „genErr“ ist
1.3.6.1.2.1.11.13	snmpInTotalReqVars	Counter	RO	Die Gesamtzahl der MIB-Objekte, die von der SNMP-Protokollentität als Ergebnis des Empfangs gültiger SNMP Get-Request und Get-Next-PDUs erfolgreich abgerufen wurden

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.11.14	snmpInTotalSetVars	Counter	RO	Die Gesamtzahl der MIB-Objekte, die von der SNMP-Protokoll-Entität durch den Empfang gültiger SNMP-Set-Request-PDUs erfolgreich geändert wurden
1.3.6.1.2.1.11.15	snmpInGetRequests	Counter	RO	Die Gesamtzahl der SNMP Get-Request PDUs, die von der SNMP-Protokolleinheit akzeptiert und verarbeitet wurden
1.3.6.1.2.1.11.16	snmpInGetNexts	Counter	RO	Die Gesamtzahl der SNMP Get-Next PDUs, die von der SNMP-Protokolleinheit akzeptiert und verarbeitet wurden
1.3.6.1.2.1.11.17	snmpInSetRequests	Counter	RO	Die Gesamtzahl der SNMP Set-Request PDUs, die von der SNMP-Protokolleinheit akzeptiert und verarbeitet wurden
1.3.6.1.2.1.11.18	snmpInGetResponses	Counter	RO	Die Gesamtzahl der SNMP Get-Response-PDUs, die von der SNMP-Protokolleinheit akzeptiert und verarbeitet wurden
1.3.6.1.2.1.11.19	snmpInTraps	Counter	RO	Die Gesamtzahl der SNMP Trap PDUs, die von der SNMP-Protokolleinheit akzeptiert und verarbeitet wurden
1.3.6.1.2.1.11.20	snmpOutTooBigs	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden und für die der Wert des Fehlerstatusfeldes „tooBig“ ist
1.3.6.1.2.1.11.21	snmpOutNoSuchNames	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden und für die der Wert des Fehlerstatus „noSuchName“ lautet
1.3.6.1.2.1.11.22	snmpOutBadValues	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden und für die der Wert des Fehlerstatusfeldes „badValue“ lautet
1.3.6.1.2.1.11.23				not used
1.3.6.1.2.1.11.24	snmpOutGenErrs	Counter	RO	Die Gesamtzahl der SNMP-PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden und für die der Wert des Fehlerstatusfeldes „genErr“ ist

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.11.25	snmpOutGetRequests	Counter	RO	Die Gesamtzahl der SNMP Get-Request PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden
1.3.6.1.2.1.11.26	snmpOutGetNexts	Counter	RO	Die Gesamtzahl der SNMP Get-Next PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden
1.3.6.1.2.1.11.27	snmpOutSetRequests	Counter	RO	Die Gesamtzahl der SNMP Set-Request PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden
1.3.6.1.2.1.11.28	snmpOutGetResponses	Counter	RO	Die Gesamtzahl der SNMP Get-Response-PDUs, die von der SNMP-Protokoll-Entität erzeugt wurden
1.3.6.1.2.1.11.29	snmpOutTraps	Counter	RO	Die Gesamtzahl der SNMP Trap PDUs, die von der SNMP-Protokolleinheit generiert wurden
1.3.6.1.2.1.11.30	snmpEnableAuthenTraps	INTEGER	RW	Gibt an, ob der SNMP-Agent-Prozess berechtigt ist, Traps für Authentifizierungsfehler zu erzeugen. enabled(1), disabled(2)
1.3.6.1.2.1.16	rmon			RMON MIB, siehe my_rmon2.my
1.3.6.1.2.1.16.19	probeConfig			Diese Gruppe steuert die Konfiguration verschiedener Betriebsparameter der Sonde
1.3.6.1.2.1.16.19.1	probeCapabilities	BITS	RO	Diese Gruppe steuert die Konfiguration verschiedener Betriebsparameter der Sonde
1.3.6.1.2.1.16.19.2	probeSoftwareRev	DisplayString (SIZE(0..15))	RO	Die Software-Revision dieses Gerätes
1.3.6.1.2.1.16.19.3	probeHardwareRev	DisplayString (SIZE(0..31))	RO	Die Hardware-Revision dieses Gerätes
1.3.6.1.2.1.16.19.4	probeDateTime	OCTET STRING	RW	Aktuelles Datum und Uhrzeit der Sonde

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.16.19.5	probeResetControl	INTEGER	RW	Wenn Sie dieses Objekt auf warmBoot(2) setzen, startet das Gerät die Anwendungssoftware neu, wobei die aktuellen Konfigurationsparameter im nichtflüchtigen Speicher gespeichert sind. Das Setzen dieses Objekts auf coldBoot(3) bewirkt, dass das Gerät die Konfigurationsparameter im nichtflüchtigen Speicher auf Standardwerte zurücksetzt und die Anwendungssoftware neu startet. Wenn das Gerät normal läuft, hat diese Variable den Wert running(1)
1.3.6.1.2.1.16.19.6	probeDownloadFile	DisplayString (SIZE(0..127))	RW	Der Dateiname, der bei der nächsten Anforderung eines Downloads über diese MIB vom TFTP-Server heruntergeladen werden soll
1.3.6.1.2.1.16.19.7	probeDownloadTFTPServer	IpAddress	RW	Die IP-Adresse des TFTP-Servers, der das Boot-Image enthält, das bei der nächsten Anforderung eines Downloads über diese MIB geladen werden soll

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.16.19.8	probeDownloadAction	INTEGER	RW	Wenn dieses Objekt auf downloadToRAM(2) oder downloadToPROM(3) eingestellt ist, beendet das Gerät seinen normalen Betrieb und beginnt den Download des durch probeDownloadFile spezifizierten Bildes von dem durch probeDownloadTFTPServer spezifizierten Server über das TFTP-Protokoll. Wenn downloadToRAM(2) angegeben ist, wird das neue Bild nur ins RAM kopiert (das alte Bild bleibt im Flash-EPROM unverändert). Wenn downloadToPROM(3) angegeben ist, wird das neue Image in den Flash-EPROM-Speicher geschrieben, nachdem seine Prüfsumme auf Richtigkeit überprüft wurde. Wenn der Download-Vorgang abgeschlossen ist, startet das Gerät warm, um die neu geladene Anwendung neu zu starten. Wenn das Gerät nicht heruntergeladen wird, hat dieses Objekt den Wert notDownloading(1).
1.3.6.1.2.1.16.19.9	probeDownloadStatus	INTEGER	RO	Der Status des letzten Download-Vorgangs, falls vorhanden. Dieses Objekt hat den Wert downloadStatusUnknown(2), wenn kein Download-Prozess durchgeführt wurde
1.3.6.1.2.1.16.19.13	trapDestTable	SEQUENCE OF TrapDestEntry		Eine Liste von Trap-Zieleinträgen
1.3.6.1.2.1.16.19.13.1	trapDestEntry	TrapDestEntry		Dieser Eintrag enthält eine Ziel-IP-Adresse, an die Traps für diese Community gesendet werden sollen
1.3.6.1.2.1.16.19.13.1.1	trapDestIndex	Integer32 (1..65535)		Ein Wert, der diesen trapDestEntry eindeutig identifiziert
1.3.6.1.2.1.16.19.13.1.2	trapDestCommunity	OCTET STRING (SIZE(0..127))	RC	Eine Community, zu der diese Zieladresse gehört

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.16.19.13.1.3	trapDestProtocol	INTEGER	RC	Das Protokoll, mit dem diese Trap gesendet werden kann ip(1), ipx(2)
1.3.6.1.2.1.16.19.13.1.4	trapDestAddress	OCTET STRING	RC	Die Adresse, an die Traps im Namen dieses Eintrags gesendet werden sollen
1.3.6.1.2.1.16.19.13.1.5	trapDestOwner	DisplayString	RC	Die Entität, die diesen Eintrag konfiguriert hat und somit die ihr zugeordneten Ressourcen verwendet
1.3.6.1.2.1.16.19.13.1.6	trapDestStatus	RowStatus	RC	Der Status dieses Trap-Zieleintrags
1.3.6.1.2.1.30	ianaifType			IANA MIB, siehe iana.my Das MIB-Modul, das die textuelle Konvention IANAifType und damit die aufgezählten Werte des ifType-Objekts definiert, das in MIB-IIs ifTable definiert ist
1.3.6.1.2.1.31	ifMIB			IF MIB, siehe rfc2233.my Das MIB-Modul zur Beschreibung generischer Objekte für Unterebenen der Netzwerkschnittstelle. Diese MIB ist eine aktualisierte Version der ifTable von MIB-II und enthält die in RFC 1229 definierten Erweiterungen.
1.3.6.1.2.1.31.1	ifMIBObjects			
1.3.6.1.2.1.31.1.1	ifXTable	SEQUENCE OF IfXEntry		Eine Liste der Interface-Einträge. Die Anzahl der Einträge wird durch den Wert von ifNumber angegeben. Diese Tabelle enthält zusätzliche Objekte für die Interfacetabelle.
1.3.6.1.2.1.31.1.1.1	ifXEntry	IfXEntry		Ein Eintrag, der zusätzliche Verwaltungsinformationen enthält, die für eine bestimmte Schnittstelle gelten.
1.3.6.1.2.1.31.1.1.1.1	ifName	DisplayString	RO	Der textuelle Name der Schnittstelle.
1.3.6.1.2.1.31.1.1.1.2	ifInMulticastPkts	Counter	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die an eine Multicast-Adresse in dieser Unterschicht adressiert wurden.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.31.1.1.1.3	ifInBroadcastPkts	Counter	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die an eine Broadcast-Adresse in dieser Unterschicht adressiert wurden.
1.3.6.1.2.1.31.1.1.1.4	ifOutMulticastPkts	Counter	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die an eine Multicast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.
1.3.6.1.2.1.31.1.1.1.5	ifOutBroadcastPkts	Counter	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die an eine Broadcast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.
1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	Counter64	RO	Die Gesamtzahl der auf der Schnittstelle empfangenen Oktette, einschließlich Framingzeichen.
1.3.6.1.2.1.31.1.1.1.7	ifHCInUcastPkts	Counter64	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die nicht an eine Multicast- oder Broadcast-Adresse in dieser Unterschicht adressiert wurden.
1.3.6.1.2.1.31.1.1.1.8	ifHCInMulticastPkts	Counter64	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die an eine Multicast-Adresse in dieser Unterschicht adressiert wurden.
1.3.6.1.2.1.31.1.1.1.9	ifHCInBroadcastPkts	Counter64	RO	Die Anzahl der Pakete, die von dieser Unterschicht an eine höhere (Unter-)Schicht geliefert werden, die an eine Broadcast-Adresse in dieser Unterschicht adressiert wurden.
1.3.6.1.2.1.31.1.1.1.10	ifHCOutOctets	Counter64	RO	Die Gesamtzahl der über die Schnittstelle übertragenen Oktette, einschließlich Framingzeichen.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.31.1.1.1.11	ifHCOutUcastPkts	Counter64	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die nicht an eine Multicast- oder Broadcast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.
1.3.6.1.2.1.31.1.1.1.12	ifHCOutMulticastPkts	Counter64	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die an eine Multicast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.
1.3.6.1.2.1.31.1.1.1.13	ifHCOutBroadcastPkts	Counter64	RO	Die Gesamtzahl der Pakete, die von übergeordneten Protokollen angefordert wurden und die an eine Broadcast-Adresse auf dieser Unterschicht adressiert wurden, einschließlich derjenigen, die verworfen oder nicht gesendet wurden.
1.3.6.1.2.1.31.1.1.1.14	ifLinkUpDownTrapEnable	INTEGER	RW	Gibt an, ob für diese Schnittstelle linkUp/linkDown-Traps generiert werden sollen. enabled(1), disabled(2)
1.3.6.1.2.1.31.1.1.1.15	ifHighSpeed	Gauge	RO	Eine Schätzung der aktuellen Bandbreite der Schnittstelle in Einheiten von 1.000.000 Bit pro Sekunde.
1.3.6.1.2.1.31.1.1.1.16	ifPromiscuousMode	TruthValue	RW	true(1), wenn die Station alle Pakete/Frames akzeptiert, die auf den Medien übertragen werden. false(2), wenn diese Schnittstelle nur Pakete/Frames akzeptiert, die an diese Station adressiert sind.
1.3.6.1.2.1.31.1.1.1.17	ifConnectorPresent	TruthValue	RO	true(1), wenn die Schnittstellenunterschicht einen physikalischen Verbinder aufweist andernfalls false(2).

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.31.1.1.1.18	ifAlias	DisplayString	RW	Dieses Objekt ist ein Alias-Name für die Schnittstelle, wie von einem Netzwerkmanager angegeben, und stellt ein nichtflüchtiges Handle für die Schnittstelle bereit.
1.3.6.1.2.1.31.1.1.1.19	ifCounterDiscontinuityTime	TimeStamp	RO	Der Wert von sysUpTime bei der letzten Gelegenheit, bei der einer oder mehrere Zähler dieser Schnittstelle eine Diskontinuität erlitten haben.
1.3.6.1.2.1.31.1.2	ifStackTable	SEQUENCE OF IfStackEntry		Die Tabelle, die Informationen über die Beziehungen zwischen den verschiedenen Teilschichten von Netzwerkschnittstellen enthält.
1.3.6.1.2.1.31.1.2.1	ifStackEntry	IfStackEntry		Informationen über eine bestimmte Beziehung zwischen zwei Unterebenen, wobei angegeben wird, dass eine Unterschicht auf der „Oberschicht“ der anderen Unterschicht läuft.
1.3.6.1.2.1.31.1.2.1.1	ifStackHigherLayer	Integer32		Der Wert von ifIndex, der der höheren Teilschicht der Beziehung entspricht, d. h. der Teilschicht, die auf der „obersten“ Teilschicht läuft, die durch die entsprechende Instanz von ifStackLowerLayer identifiziert wird.
1.3.6.1.2.1.31.1.2.1.2	ifStackLowerLayer	Integer32		Der Wert von ifIndex, der der unteren Unterschicht der Beziehung entspricht, d. h. der Unterschicht, die unter der Unterschicht läuft, die durch die entsprechende Instanz von ifStackHigherLayer identifiziert wurde.
1.3.6.1.2.1.31.1.2.1.3	ifStackStatus	RowStatus	RC	Der Status der Beziehung zwischen zwei Unterschichten.
1.3.6.1.2.1.31.1.3	ifTestTable	SEQUENCE OF IfTestEntry		Diese Tabelle enthält einen Eintrag pro Schnittstelle. Es definiert Objekte, die es einem Netzwerkmanager ermöglichen, einen Agenten anzuweisen, eine Schnittstelle auf verschiedene Fehler zu testen. Veraltet

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.31.1.3.1	ifTestEntry	IfTestEntry		Ein Eintrag, der Objekte zum Aufrufen von Tests auf einer Schnittstelle enthält. Veraltet
1.3.6.1.2.1.31.1.3.1.1	ifTestId	TestAndIncr	RW	Dieses Objekt identifiziert den aktuellen Aufruf des Schnittstellentests Veraltet
1.3.6.1.2.1.31.1.3.1.2	ifTestStatus	INTEGER	RW	Dieses Objekt gibt an, ob ein Manager derzeit über die erforderliche „Eigentümerschaft“ verfügt, um einen Test auf dieser Schnittstelle aufzurufen Veraltet
1.3.6.1.2.1.31.1.3.1.3	ifTestType	AutonomousType	RW	Eine Steuervariable, die zum Starten und Stoppen von vom Bediener initiierten Schnittstellentests verwendet wird Veraltet
1.3.6.1.2.1.31.1.3.1.4	ifTestResult	INTEGER	RO	Dieses Objekt enthält das Ergebnis des zuletzt angeforderten Tests oder den Wert none(1), wenn seit dem letzten Zurücksetzen keine Tests angefordert wurden Veraltet
1.3.6.1.2.1.31.1.3.1.5	ifTestCode	OBJECT IDENTIFIER	RO	Dieses Objekt enthält einen Code, der spezifischere Informationen über das Testergebnis enthält, z. B. einen Fehlercode nach einem fehlgeschlagenen Test Veraltet
1.3.6.1.2.1.31.1.3.1.6	ifTestOwner	OwnerString	RW	Die Entität, die derzeit die „Eigentümerschaft“ hat, die erforderlich ist, um einen Test auf dieser Schnittstelle durchzuführen Veraltet
1.3.6.1.2.1.31.1.4	ifRcvAddressTable	SEQUENCE OF IfRcvAddressEntry		Diese Tabelle enthält einen Eintrag für jede Adresse (Broadcast, Multicast oder Uni-Cast), für die das System Pakete/Frames auf einer bestimmten Schnittstelle empfängt.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.2.1.31.1.4.1	ifRcvAddressEntry	IfRcvAddressEntry		Eine Liste von Objekten, die eine Adresse identifizieren, für die das System Pakete/Frames auf der jeweiligen Schnittstelle akzeptiert, die durch den Indexwert ifIndex identifiziert wird.
1.3.6.1.2.1.31.1.4.1.1	ifRcvAddressAddress	PhysAddress		Eine Adresse, für die das System Pakete/Frames auf der Schnittstelle dieses Eintrags akzeptiert.
1.3.6.1.2.1.31.1.4.1.2	ifRcvAddressStatus	RowStatus	RC	Mit diesem Objekt werden Zeilen in der ifRcvAddressTable erstellt und gelöscht.
1.3.6.1.2.1.31.1.4.1.3	ifRcvAddressType	INTEGER	RC	Dieses Objekt hat den Wert nonVolatile(3) für diejenigen Einträge in der Tabelle, die gültig sind und beim nächsten Neustart des verwalteten Systems nicht gelöscht werden. Einträge mit dem Wert volatile(2) sind gültig und vorhanden, wurden aber nicht gespeichert, sodass sie nach dem nächsten Neustart des verwalteten Systems nicht existieren. Einträge mit dem Wert other(1) sind gültig und vorhanden, werden aber nicht klassifiziert, ob sie auch nach dem nächsten Neustart bestehen bleiben.
1.3.6.1.2.1.31.1.5	ifTableLastChange	TimeTicks		Der Wert von sysUpTime zum Zeitpunkt der letzten Erstellung oder Löschung eines Eintrags in der ifTable. Wenn die Anzahl der Einträge seit der letzten Neuinitialisierung des lokalen Netzwerkmanagementsubsystems unverändert geblieben ist, enthält dieses Objekt einen Nullwert.
1.3.6.1.2.1.31.1.6	ifStackLastChange	TimeTicks	RO	Der Wert von sysUpTime zum Zeitpunkt der letzten Änderung des (gesamten) Interface-Stacks.

Tabelle 13: Daten in der SNI-spezifischen MIB

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7	hg3550mib			hg3550 MIB, siehe hg

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.1	errorSigGrouphlb20			Fehlersignalisie MIB mit Ereignis Verwaltungsebe
1.3.6.1.4.1.231.7.2.7.1.1	numberOfTrapHistoryEntries	INTEGER	RW	Enthält die Anza in der Tabelle d zu finden sind. können alle Ein werden (Wert =
1.3.6.1.4.1.231.7.2.7.1.2	hlb20TrapHistoryTable	SEQUENCE OF Hlb20TrapHistoryEntry		Diese Tabelle e über vom Gerät
1.3.6.1.4.1.231.7.2.7.1.2.1	hlb20TrapHistoryEntry	Hlb20TrapHistoryEntry		Die Einträge de Tabelle.
1.3.6.1.4.1.231.7.2.7.1.2.1.1	trapIndex	INTEGER	RO	Identifikation ei Index aktivierter
1.3.6.1.4.1.231.7.2.7.1.2.1.2	trapDateTime	DateAndTime	RO	Zeit, zu der das eingetreten ist.
1.3.6.1.4.1.231.7.2.7.1.2.1.3	trapSeverity	INTEGER	RO	Enthält Informat Schweregrad de - normal(1) - warning(2) - minor(3) - major(4) - critical(5)
1.3.6.1.4.1.231.7.2.7.1.2.1.4	trapErrorClass	INTEGER	RO	Enthält die Num Fehlerklasse (T - general(1) - voice(2) - data(3) - security(4) - client(5)
1.3.6.1.4.1.231.7.2.7.1.2.1.5	trapErrorCode	INTEGER	RO	Enthält den Feh
1.3.6.1.4.1.231.7.2.7.1.2.1.6	trapDescription	DisplayString	RO	Detaillierte Infor Trapereignis.
1.3.6.1.4.1.231.7.2.7.1.2.1.7	trapHandling	INTEGER	RO	Forwarded(1), w Trap ausgelöst Stored(2), wenn gespeichert wu zu senden.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.1.3	numberOfErrorTableEntries	INTEGER	RW	Enthält die Anzahl de in der Tabelle der Tra zu finden sind. Mit die können alle Einträge werden (Wert = 0). veraltet
1.3.6.1.4.1.231.7.2.7.1.4	hlb20ErrorTable	SEQUENCE OF Hlb20ErrorEntry		Diese Tabelle enthält über Fehlerereignisse Expertenebene, die a hg3550-Gerät auftrete veraltet
1.3.6.1.4.1.231.7.2.7.1.4.1	hlb20ErrorEntry	Hlb20ErrorEntry		Die Einträge der Trap Tabelle. veraltet
1.3.6.1.4.1.231.7.2.7.1.4.1.1	errorIndex	INTEGER	RO	Enthält die Fehler-/Tr veraltet
1.3.6.1.4.1.231.7.2.7.1.4.1.2	errorTimeStamp	OCTET STRING	RO	Systemspezifischer Z den Fehler. veraltet
1.3.6.1.4.1.231.7.2.7.1.4.1.3	errorClass	INTEGER	RO	Enthält die Fehler-/Tr veraltet
1.3.6.1.4.1.231.7.2.7.1.4.1.4	errorDescription	DisplayString	RO	Detaillierte Informatio Fehlern. veraltet
1.3.6.1.4.1.231.7.2.7.2	controlGrouphlb20			Steuerungsgruppe M
1.3.6.1.4.1.231.7.2.7.2.1	indexOfLastTrapSent	INTEGER	RO	Enthält den Index der gesendeten Trap.
1.3.6.1.4.1.231.7.2.7.2.2	trapTypesToBeSent	INTEGER	RW	Definiert, welche Feh als Trap signalisiert w
1.3.6.1.4.1.231.7.2.7.2.3	sysState	INTEGER	RW	Der aktuelle Fehlerzu hg3550-Geräts. - normal(1) - warning(2) - minor(3) - major(4) - critical(5)

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.2.4	sysConnectionState	INTEGER	RO	Gibt an, ob die V zwischen Hicom hg3550 / Hicom erfolgreich herg - disconnected(- connected(2)
1.3.6.1.4.1.231.7.2.7.2.5	sysMacAddress	DisplayString	RO	Enthält die MAC Geräts. (Objekt in hg35 1.0 nicht verfüg
1.3.6.1.4.1.231.7.2.7.2.6	sysSoftwareVersion	DisplayString	RO	Enthält den Ver Systemsoftware (Objekt in HG15 1.0 nicht verfüg
1.3.6.1.4.1.231.7.2.7.2.7	sysSnmpAgentVersion	DisplayString	RO	Versionsnumme Agenten des Sy (Formatierung:
1.3.6.1.4.1.231.7.2.7.2.8	sysShadowSoftwareVersion	DisplayString	RO	Enthält den Ver inaktiven Softwa Bild), die kürzlic übertragen wur HG1500 / Xpres verfügbar) veraltet
1.3.6.1.4.1.231.7.2.7.2.9	sysHardwareVersion	DisplayString	RO	Hardware-Versi Gerätes. (Objek Xpress @LAN 1
1.3.6.1.4.1.231.7.2.7.2.10	sysOperatingMode	INTEGER	RO	Betriebsart des Standardmodus Gerät als norma Gatekeeper-Mo er zusätzlich als Voice over IP-E HG1500 / Xpres verfügbar)
1.3.6.1.4.1.231.7.2.7.2.11	sysSwitchoverDateTime	DateAndTime	RW	Date and time fo the new system

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.2.1.1.9	sysDownloadAction	INTEGER	RW	Wenn dieses Objekt a downloadAndImmedia (2) eingestellt ist, lädt Gerät die neue Softw konfigurierten Host he Nach Abschluss des startet das Gerät auto der neuen Software n downloadAndDelayed (3) angegeben ist, wi Bild auf das Gerät ko der tftpDateTime-Wer wird, beendet das Ge normalen Betrieb und Softwareumschaltung Nach einem automati Reset beginnt es mit Systemsoftware. Eins downloadWithoutSwit (4) startet einen Dow ohne auf die neue So umzusteigen. Wenn d nicht heruntergeladen hat dieses Objekt den notDownloading(1).
1.3.6.1.4.1.231.7.2.7.2.1.1.10	sysSwitchoverState	INTEGER	RW	Die Werte readyForS (1) und notReadyForS (2) geben an, ob das bereit ist, auf die neue umgestellt zu werden in den Schattenblitzbe heruntergeladen wurd nicht. Wenn dies nich ist, gibt h150eShadow Details über den Grun Wenn Sie dieses Obje switchoverNow (3) se das Gerät sofort auf d Software umgeschalte zuvor in den Schatten heruntergeladen wurd das System neu start initSwitchoverDelayed eine verzögerte Umsc veraltet
1.3.6.1.4.1.231.7.2.7.2.1.1.14	sysFirmwareVersion	DisplayString	RO	Versionsnummer der Firmware.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.2.15	sysHlbSymbolSubInfo	DisplayString	RO	Enthält neben d gemeinsamen M deviceSymbolIn Symbolinformat eine URL zu de Symbolinformat
1.3.6.1.4.1.231.7.2.7.2.16	sysHlbBranding	DisplayString	RO	Enthält den Bra Geräts.
1.3.6.1.4.1.231.7.2.7.3	monitoringGroupHlb20			Überwachungsg
1.3.6.1.4.1.231.7.2.7.3.1	numberOfIdleMonTableEntries	INTEGER	RO	Enthält die Anza Überwachungst Last.
1.3.6.1.4.1.231.7.2.7.3.2	hlb20IdleMonTable	SEQUENCE OF Hlb20IdleMonTableEntry		Diese Tabelle e über die Leerlau Systems (alle 5 für die letzten 2
1.3.6.1.4.1.231.7.2.7.3.2.1	hlb20IdleMonTableEntry	Hlb20IdleMonTableEntry		Die Tabelleneint Lastüberwachu
1.3.6.1.4.1.231.7.2.7.3.2.1.1	idle1Index	INTEGER	RO	Identifikation ei Tabelleneintrags
1.3.6.1.4.1.231.7.2.7.3.2.1.2	idle2Value	INTEGER	RO	Der Wert des La
1.3.6.1.4.1.231.7.2.7.3.3	numberOfIdleLatestTableEntries	INTEGER	RO	Enthält die Anza Tabelleneinträg Lastüberwachu
1.3.6.1.4.1.231.7.2.7.3.4	hlb20IdleLatestTable	SEQUENCE OF Hlb20IdleLatestTableEntry		Diese Tabelle e über die Leerlau Systems (jede M die letzten 10 M
1.3.6.1.4.1.231.7.2.7.3.4.1	hlb20IdleLatestTableEntry	Hlb20IdleLatestTableEntry		Die präzise Lee Lastüberwachu zehn neuesten
1.3.6.1.4.1.231.7.2.7.3.4.1.1	idle1LatestIndex	INTEGER	RO	Identifikation ei Tabelleneintrags
1.3.6.1.4.1.231.7.2.7.3.4.1.2	idle2LatestValue	INTEGER	RO	Identifikation ei
1.3.6.1.4.1.231.7.2.7.3.5	numberOfIdleMonYellowAlarms	INTEGER	RO	Enthält die Anza Lastüberwachu
1.3.6.1.4.1.231.7.2.7.3.6	numberOfIdleMonRedAlarms	INTEGER	RO	Enthält die Anza Lastüberwachu

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.3.7	flagIdleMonYellowAlarm	INTEGER	RO	1, wenn die Lastüberw gelben Alarm steht. ansonsten 0
1.3.6.1.4.1.231.7.2.7.3.8	flagIdleMonRedAlarm	INTEGER	RO	1, wenn die Lastüberw rotem Alarm steht. ansonsten 0
1.3.6.1.4.1.231.7.2.7.3.9	thresholdIdleMonYellowAlarm	INTEGER (0..100)	RW	Leerlauf-Schwellenwe Erzeugung eines gelb
1.3.6.1.4.1.231.7.2.7.3.10	thresholdIdleMonRedAlarm	INTEGER (0..100)	RW	Leerlauf-Schwellenwe Erzeugung des roten
1.3.6.1.4.1.231.7.2.7.3.11	idleMonHighWaterMark	INTEGER	RO	Enthält den Lastspitze Gerätes.
1.3.6.1.4.1.231.7.2.7.3.12	idleMonLastValue	INTEGER	RO	Enthält den neuesten Lastüberwachung.
1.3.6.1.4.1.231.7.2.7.3.13	numberOfFreeMemBuffersTableEntries	INTEGER	RO	Enthält die Anzahl de Tabelleneinträge der Speicherpufferung. A neueren Versionen ve devices veraltet
1.3.6.1.4.1.231.7.2.7.3.14	freeMemBuffersTable	SEQUENCE OF FreeMemBuffersTableEntry	Key	Diese Tabelle enthält über die Anzahl der fr Speicherpuffer für die verschiedenen Puffer Tabelle verfügbar in n Versionen. 1.1 device veraltet
1.3.6.1.4.1.231.7.2.7.3.14.1	freeMemBuffersTableEntry	FreeMemBuffersTableEntry	Key	Die freien Speicherpu Geräts. veraltet
1.3.6.1.4.1.231.7.2.7.3.14.1.1	buffIndex	INTEGER	RO	Identifikation eines Tabelleneintrags. veraltet
1.3.6.1.4.1.231.7.2.7.3.14.1.2	buffType	DisplayString	RO	Typ/Größe dieses Pu veraltet
1.3.6.1.4.1.231.7.2.7.3.14.1.3	numOfFreeBuffers	INTEGER	RO	Die Anzahl der freien Typs. veraltet

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.3.15	loadBalanceMeasureControl	INTEGER	RW	Die Messung de der Prozesse de durch dieses Ob Das Setzen des (2) startet die M (1) stoppt sie. A Versionen verfü
1.3.6.1.4.1.231.7.2.7.3.16	numberOfLoadBalanceTableEntries	INTEGER	RO	Enthält die Anza die Lastausgleic veraltet
1.3.6.1.4.1.231.7.2.7.3.17	loadBalanceTable	SEQUENCE OF LoadBalanceTableEntry		Diese Tabelle e Informationen ü Lastverteilung d Prozesse des G veraltet
1.3.6.1.4.1.231.7.2.7.3.17.1	loadBalanceTableEntry	LoadBalanceTableEntry		Die Lastverteilu dieser Vorrichtu veraltet
1.3.6.1.4.1.231.7.2.7.3.17.1.1	loadBalanceIndex	INTEGER	RO	Identifikation ein Tabelleneintrags veraltet
1.3.6.1.4.1.231.7.2.7.3.17.1.2	processDescription	DisplayString	RO	Textuelle Besch Prozesses. veraltet
1.3.6.1.4.1.231.7.2.7.3.17.1.3	loadProportionValue	DisplayString	RO	Lastverhältnis fü veraltet
1.3.6.1.4.1.231.7.2.7.4	statisticsGrouphlb20			Statistikgruppe
1.3.6.1.4.1.231.7.2.7.4.1	globalVcapiClientStatGroup			globale Statistik
1.3.6.1.4.1.231.7.2.7.4.1.1	statVcapiInstalledClients	INTEGER	RO	Enthält die Anza Lastüberwachun veraltet
1.3.6.1.4.1.231.7.2.7.4.1.2	statVcapiLoggedInClients	INTEGER	RO	Enthält die Ges Client-Anmeldu letzten Systemn veraltet

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.4.1.1	statVcapiActiveClients	INTEGER	RO	Enthält die Anzahl de vCAPI-Clients (oder b wenn die Kanalbünde konfiguriert ist). veraltet
1.3.6.1.4.1.231.7.2.7.4.2	globalH323ClientStatGroup			globale Statistikdaten
1.3.6.1.4.1.231.7.2.7.4.2.1	statH323InstalledClients	INTEGER	RO	Enthält die Anzahl de H323-Clients (d. h. si Kundendatenbank ko veraltet
1.3.6.1.4.1.231.7.2.7.4.2.2	statH323ActiveClients	INTEGER	RO	Enthält die Anzahl de Clients in einem aktiv Verbindungszustand. veraltet
1.3.6.1.4.1.231.7.2.7.4.3	globalTfaClientStatGroup			globale Statistikdaten
1.3.6.1.4.1.231.7.2.7.4.3.1	statTfaInstalledClients	INTEGER	RO	Enthält die Anzahl de TFA Clients (d. h. sie Kundendatenbank ko veraltet
1.3.6.1.4.1.231.7.2.7.4.3.2	statTfaActiveClients	INTEGER	RO	Enthält die Anzahl de im aktiven Verbindung veraltet
1.3.6.1.4.1.231.7.2.7.4.3.3	statTfaRegistratedClients	INTEGER	RO	Enthält die Anzahl de Clients, die sich seit d Systemneustart bei ih registriert haben. veraltet
1.3.6.1.4.1.231.7.2.7.4.3.4	statTfaClientLogonSuccess	INTEGER	RO	Enthält die Anzahl de Anmeldungen von TF dem letzten Systemn veraltet
1.3.6.1.4.1.231.7.2.7.4.3.5	statTfaClientLogonFailed	INTEGER	RO	Enthält die Anzahl de fehlgeschlagenen An von TFA-Clients seit d Systemneustart. veraltet
1.3.6.1.4.1.231.7.2.7.4.4	globalVoiceClientCallStatGroup			globale statistische A H323- und TFA-Client

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.4.4.1	statOutgoingRtp	INTEGER	RO	Enthält die Anza ausgehenden R TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.2	statOutgoingLostRtp	INTEGER	RO	Enthält die Anza ausgehenden R TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.3	statIncomingRtp	INTEGER	RO	Enthält die Anza RTP-Pakete (H3
1.3.6.1.4.1.231.7.2.7.4.4.4	statIncomingLostRtp	INTEGER	RO	Enthält die Anza eingehenden RT TFA Clients).
1.3.6.1.4.1.231.7.2.7.4.4.5	statTotalBytesSentRtp	INTEGER	RO	Enthält die Anza Bytes (RTP).
1.3.6.1.4.1.231.7.2.7.4.4.6	statTotalBytesRecvRtp	INTEGER	RO	Enthält die Anza empfangenen B
1.3.6.1.4.1.231.7.2.7.4.5	indivVoiceClientCallStatBuffer			individuelle Stat Client
1.3.6.1.4.1.231.7.2.7.4.5.1	numOfClientStatIndTableEntries	INTEGER	RO	Enthält die Anza Einträge der H3 Tabelle.
1.3.6.1.4.1.231.7.2.7.4.5.2	hlb20ClientStatIndTable	SEQUENCE OF Hlb20ClientStatIndTableEntry		Diese Tabelle e statistische Info H323-Client. No diese Tabelle le das Debugging konzipiert.
1.3.6.1.4.1.231.7.2.7.4.5.2.1	hlb20ClientStatIndTableEntry	Hlb20ClientStatIndTableEntry		Ein einzelnen E statistischen Inf des H323-Clien
1.3.6.1.4.1.231.7.2.7.4.5.2.1.1	statInd1VoiceCliIndex	Hlb20ClientStatIndSnmpIndex	RO	Identifikation ein Index aktivierter
1.3.6.1.4.1.231.7.2.7.4.5.2.1.2	statInd1VoiceCliCallId	OCTET STRING (SIZE (1..21))	RO	Enthält die Rufn (autorisierter Na
1.3.6.1.4.1.231.7.2.7.4.5.2.1.3	statInd1VoiceCliLocalIpAddress	TransportLabel	RO	Enthält die IP-A Endpunktes.
1.3.6.1.4.1.231.7.2.7.4.5.2.1.4	statInd1VoiceCliTimeBegin	DateAndTime	RO	Enthält den Zeit Beginn des Anr
1.3.6.1.4.1.231.7.2.7.4.5.2.1.5	statInd1VoiceCliTimeEnd	DateAndTime	RO	Enthält den Zeit Ende des Anruf

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.6	staVoiceCliEncoder	INTEGER	RO	Enthält Geberinforma
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.7	staVoiceCliDecoder	INTEGER	RO	Enthält Decoderinfor
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.8	staVoiceCliOutgoingRtp	INTEGER	RO	Enthält die Anzahl de ausgehenden RTP-Pa
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.9	staVoiceCliOutgoingLostRtp	INTEGER	RO	Enthält die Anzahl de ausgehenden RTP-Pa
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.10	staVoiceCliIncomingRtp	INTEGER	RO	Enthält die Anzahl de RTP-Pakete.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.11	staVoiceCliIncomingLostRtp	INTEGER	RO	Enthält die Anzahl de eingehenden RTP-Pa
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.12	staVoiceCliTotalBytesSentRtp	INTEGER	RO	Enthält die Anzahl de Byte.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.13	staVoiceCliTotalBytesRcvdRtp	INTEGER	RO	Enthält die Anzahl de empfangenen Byte.
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.14	staVoiceCliDelay	INTEGER	RO	Enthält die durchschn Netzwerkverzögerung
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.15	staVoiceCliJitter	INTEGER	RO	Enthält den durchsch
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.16	staVoiceConnectionCondTable	OCTET STRING (SIZE (1..21))	RO	Enthält die Konferenz (Kanonenname), die Telefonkonferenz ode beteiligten Parteien e
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.17	staVoiceConnectionQuality	INTEGER	RO	Die Gesamtqualität d des Anrufs - Abschnit - normal(1) - warning(2) - minor(3) - major(4) - critical(5)
1.3.6.1.4.1.231.7.2.7.4.5.1.2.1.18	staVoiceCliRemoteIpAddressType	TransportLabel	RO	Enthält die IP-Adress entfernten Endpunkte
1.3.6.1.4.1.231.7.2.7.4.5.3	staIPQualityNotificationCounter	INTEGER	RO	Gesamtzahl der Traps Qualität, die seit dem Agenten gesendet wu
1.3.6.1.4.1.231.7.2.7.4.6	staAudioStreamStatGroup			individuelle Statistikda Client

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.4.11	statAudioStreamSccRxErrors	INTEGER	RO	Enthält die Anza (Pufferunterläuf Kommunikation und den empfar (Objekt in hg35 1.0 nicht verfüg veraltet
1.3.6.1.4.1.231.7.2.7.4.12	statAudioStreamSccTxErrors	INTEGER	RO	Enthält die Anza (Pufferüberläufe Kommunikation und den sender in HG1500 / Xp nicht verfügbar)
1.3.6.1.4.1.231.7.2.7.5	sendAlarmWithValues	TRAP		Tritt ein Fehler a geprüft, ob die e konfiguriert ist, sofortige Signal Wenn ja, wird e Managementsta die oben genan enthält.
1.3.6.1.4.1.231.7.2.7.6	fileOverflowError	TRAP		Informiert den M die Tabelle Trap geworden ist. W der Tabelle nich reduziert wird (d von numberOfT werden die ältes Trapinformation überschrieben.
1.3.6.1.4.1.231.7.2.7.7	allServeGrouphlb20			HiPath AllServe
1.3.6.1.4.1.231.7.2.7.7.1	registrationState	INTEGER	RO	Enthält Informat über den HiPath Registrierungss - registered(1) - notRegistered
1.3.6.1.4.1.231.7.2.7.7.2	numberOfCallAddrTableEntries	INTEGER	RO	Enthält die Anza der Adresstabel
1.3.6.1.4.1.231.7.2.7.7.3	numberOfCallAddrCacheEntries	INTEGER	RO	Enthält die Anza Einträge für die
1.3.6.1.4.1.231.7.2.7.7.4	numberOfNodeIpTableEntries	INTEGER	RO	Enthält die Anza der IP-Tabelle d

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.7.5	hlb20NodeIpTable	SEQUENCE OF Hlb20NodeIpTableEntry		Diese Tabelle enthält über die Zuordnung v Adressen zu HiPath A Knoten.
1.3.6.1.4.1.231.7.2.7.7.5.1	hlb20NodeIpTableEntry	Hlb20NodeIpTableEntry		Der Knoten IP-Tabelle
1.3.6.1.4.1.231.7.2.7.7.5.1.1	nodeIndex	INTEGER	RO	Identifikation eines Tabelleneintrags, iden Knoten-ID.
1.3.6.1.4.1.231.7.2.7.7.5.1.2	nodeIpNumOfIpAddr	INTEGER	RO	Anzahl der IP-Adress diesen Knoten.
1.3.6.1.4.1.231.7.2.7.7.5.1.3	nodeIpAddresses	DisplayString	RO	Zugewiesene IP-Adre diesen Knoten.
1.3.6.1.4.1.231.7.2.7.7.6	numberOfNuPortDataTableEntries	INTEGER	RO	Enthält die Anzahl de der Datentabelle für d Netzwerkgeräte.
1.3.6.1.4.1.231.7.2.7.7.7	hlb20NuPortDataTable	SEQUENCE OF Hlb20NuPortDataTableEntry		Diese Tabelle enthält über die Portdaten de Netzwerkgeräte diese
1.3.6.1.4.1.231.7.2.7.7.7.1	hlb20NuPortDataTableEntry	Hlb20NuPortDataTableEntry		Die Netzwerkeinheit p Datentabelleneinträge
1.3.6.1.4.1.231.7.2.7.7.7.1.1	nuPortDataIndex	INTEGER	RO	Identifikation eines Tabelleneintrags.
1.3.6.1.4.1.231.7.2.7.7.7.1.2	nuCardPort	INTEGER	RO	Die lw_port zum Syst
1.3.6.1.4.1.231.7.2.7.7.7.1.3	nuPortDataProtocol	INTEGER	RO	Das Netzwerkprotoko
1.3.6.1.4.1.231.7.2.7.7.7.1.4	nuPortDataNumOfBchn	INTEGER	RO	Die Anzahl der B-Kar System.
1.3.6.1.4.1.231.7.2.7.7.7.1.5	nuPortDataActiveBchn	INTEGER	RO	Die Anzahl der aktive
1.3.6.1.4.1.231.7.2.7.7.8	numberOfNuTransDataTableEntries	INTEGER	RO	Enthält die Anzahl de der Transaktionsdate Netzwerkeinheit.
1.3.6.1.4.1.231.7.2.7.7.9	hlb20NuTransDataTable	SEQUENCE OF Hlb20NuTransDataTableEntry		Diese Tabelle enthält über die Transaktions Netzwerkeinheit diese
1.3.6.1.4.1.231.7.2.7.7.9.1	hlb20NuTransDataTableEntry	Hlb20NuTransDataTableEntry		Die Einträge der Transaktionsdatentab Netzwerkeinheit.
1.3.6.1.4.1.231.7.2.7.7.9.1.1	nuTransDataIndex	INTEGER	RO	Identifikation eines Tabelleneintrags.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.7.9.1.2	hTransStepState	INTEGER	RO	Der Zustand de
1.3.6.1.4.1.231.7.2.7.7.9.1.3	hTransCallDirection	INTEGER	RO	Die Anrufrichtur - incoming(1) = - outgoing(2) =
1.3.6.1.4.1.231.7.2.7.7.9.1.4	hTransCallRefSys	INTEGER	RO	Die Anrufreferer Mainboard.
1.3.6.1.4.1.231.7.2.7.7.9.1.5	hTransBchnIndex	INTEGER	RO	Der Kanalindex Nachricht.
1.3.6.1.4.1.231.7.2.7.7.9.1.6	hTransTimeSlot	INTEGER	RO	Das Zeitfenster Schnittstelle.
1.3.6.1.4.1.231.7.2.7.7.9.1.7	hTransPartnerIpAddr	IpAddress	RO	Die IP-Adresse AllServe-Partne
1.3.6.1.4.1.231.7.2.7.7.9.1.8	hTransCallRefIp	INTEGER	RO	Die Anrufreferer Netzwerk.
1.3.6.1.4.1.231.7.2.7.8	ethernetStatGrouphlb20			Ethernet Statist
1.3.6.1.4.1.231.7.2.7.8.1	ethernetStatState	INTEGER	RW	Initialisieren Sie Statistikdaten a den Wert 2 eins - counting(1) - reset(2)
1.3.6.1.4.1.231.7.2.7.8.2	goodFramesTransmitted	INTEGER	RO	Erfolgreich gese Frames
1.3.6.1.4.1.231.7.2.7.8.3	goodFramesReceived	INTEGER	RO	Korrigiert empfa Frames
1.3.6.1.4.1.231.7.2.7.8.4	sendRetries	INTEGER	RO	erfolgreiche Eth Sendeversuche
1.3.6.1.4.1.231.7.2.7.8.5	receiveCollisions	INTEGER	RO	Kollisionen bei
1.3.6.1.4.1.231.7.2.7.8.6	sendRetryError	INTEGER	RO	16 fehlgeschlag
1.3.6.1.4.1.231.7.2.7.8.7	macEngineDefer	INTEGER	RO	MAC-Engine m
1.3.6.1.4.1.231.7.2.7.8.8	excessiveDeferral	INTEGER	RO	übermäßige Ver
1.3.6.1.4.1.231.7.2.7.8.9	lossOfCarrier	INTEGER	RO	Trägerverlust
1.3.6.1.4.1.231.7.2.7.8.10	lateCollision	INTEGER	RO	verspätete Kolli
1.3.6.1.4.1.231.7.2.7.8.11	txBufferError	INTEGER	RO	Sendepuffer - fa
1.3.6.1.4.1.231.7.2.7.8.12	underflowError	INTEGER	RO	Unterlauffehler

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.8.1.1	checksumError	INTEGER	RO	Prüfsummenfehler em
1.3.6.1.4.1.231.7.2.7.8.1.1	framingError	INTEGER	RO	Framing-Fehler empfa
1.3.6.1.4.1.231.7.2.7.8.1.1	missedFrames	INTEGER	RO	Verpasste Bilder
1.3.6.1.4.1.231.7.2.7.8.1.1	runtPackets	INTEGER	RO	runt-Pakete
1.3.6.1.4.1.231.7.2.7.8.1.1	frameTooShort	INTEGER	RO	Empfangener Rahme
1.3.6.1.4.1.231.7.2.7.8.1.1	frameTooLong	INTEGER	RO	Empfangener Rahme
1.3.6.1.4.1.231.7.2.7.8.1.1	bufferLimitReached	INTEGER	RO	Untere Puffergrenze e
1.3.6.1.4.1.231.7.2.7.8.2.0	rcvBufferError	INTEGER	RO	Empfangspuffer - fata
1.3.6.1.4.1.231.7.2.7.8.2.1	overflowError	INTEGER	RO	Überlauffehler - Hardw
1.3.6.1.4.1.231.7.2.7.8.2.2	collisionErrorInt	INTEGER	RO	Sender-Empfänger-Te fehlgeschlagen - Hard
1.3.6.1.4.1.231.7.2.7.8.2.3	memoryErrorInt	INTEGER	RO	Systembus-Timeout - Hardwarefehler
1.3.6.1.4.1.231.7.2.7.8.2.4	excessiveInts	INTEGER	RO	Übermäßiges Auftrete Unterbrechungen
1.3.6.1.4.1.231.7.2.7.8.2.5	linkChanged	INTEGER	RO	link changed
1.3.6.1.4.1.231.7.2.7.8.2.6	linkMode	INTEGER	RO	Betriebsart der Ether Verbindung. - halfDuplex10BaseT - halfDuplex100Base - fullDuplex10BaseT(- fullDuplex100BaseT - auto(0)
1.3.6.1.4.1.231.7.2.7.8.2.7	good8021pFramesReceived	INTEGER	RO	Die Anzahl der korrek empfangenen 802.1p
1.3.6.1.4.1.231.7.2.7.8.2.8	babblingReceiveInts	INTEGER	RO	Die Anzahl der empfa Frames mit einer Län ist als die maximal zu Ethernet-Framegröße 1522 Byte).
1.3.6.1.4.1.231.7.2.7.8.2.9	babblingTransmitInts	INTEGER	RO	Die Anzahl der übertr Frames mit einer Län ist als die maximal zu Ethernet-Framegröße 1522 Byte).

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.8.30	unexpectedInts	INTEGER	RO	Die Anzahl der Interrupt-Ereign sind . Das Vorhande unerwarteten U kann auf ein sc Problem auf de
1.3.6.1.4.1.231.7.2.7.9	qosStatGrouphlb20			Quality Of Servi MIB
1.3.6.1.4.1.231.7.2.7.9.1	numOfQosStatTableEntries	INTEGER	RW	Enthält die Anz in der Statistikta Service (qos). D Schreibwert ist Statistikzähler z
1.3.6.1.4.1.231.7.2.7.9.2	qosStatTable	SEQUENCE OF QosStatTableEntry		Diese Tabelle e Informationen ü Mechanismen d Service (QOS).
1.3.6.1.4.1.231.7.2.7.9.2.1	qosStatTableEntry	QosStatTableEntry		Die QOS-Statistikinforma Einträge.
1.3.6.1.4.1.231.7.2.7.9.2.1.1	qosIndex	INTEGER	RO	Identifikation ei Index aktivierte
1.3.6.1.4.1.231.7.2.7.9.2.1.2	interface	DisplayString	RO	Die Schnittstelle Statistikdaten g
1.3.6.1.4.1.231.7.2.7.9.2.1.3	remarkedFrames	INTEGER	RO	Die Anzahl der Rahmen.
1.3.6.1.4.1.231.7.2.7.9.2.1.4	droppedPackets	DisplayString	RO	Die Anzahl der für jede Wartes
1.3.6.1.4.1.231.7.2.7.10	bChannelStatGrouphlb20			B-Channel Stati
1.3.6.1.4.1.231.7.2.7.10.1	numOfBChannelStatTableEntries	INTEGER	RW	Enthält die Anz in der B-Kanal-S Der einzige gült ist 0, was alle B zurücksetzt.
1.3.6.1.4.1.231.7.2.7.10.2	bChannelStatTable	SEQUENCE OF BChannelStatTableEntry		Diese Tabelle e Informationen ü
1.3.6.1.4.1.231.7.2.7.10.2.1	bChannelStatTableEntry	BChannelStatTableEntry		Die Einträge in statistischen Inf Kanals.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.10.2.1.1	b2ChannelStatIndex	INTEGER	RO	Identifikation eines du Index aktivierten Tabe
1.3.6.1.4.1.231.7.2.7.10.2.1.2	b2ChannelIdentifier	DisplayString (SIZE (0..255))	RO	Der B-Kanal-Bezeichn die Summe aller B-Ka
1.3.6.1.4.1.231.7.2.7.10.2.1.3	frmLenViolation	INTEGER	RO	Anzahl der empfange mit ungültiger Länge.
1.3.6.1.4.1.231.7.2.7.10.2.1.4	frmNotOctetAligned	INTEGER	RO	Anzahl der Frames m ungültigen Anzahl vor
1.3.6.1.4.1.231.7.2.7.10.2.1.5	frmAbortSequence	INTEGER	RO	Anzahl der Fälle, in d HDLC-Abbruchseque wurde.
1.3.6.1.4.1.231.7.2.7.10.2.1.6	frmCrcError	INTEGER	RO	Anzahl der empfange mit CRC-Prüfsummer
1.3.6.1.4.1.231.7.2.7.10.2.1.7	qmcBusyInt	INTEGER	RO	Anzahl der empfange wenn kein Empfangsp Deskriptor verfügbar
1.3.6.1.4.1.231.7.2.7.10.2.1.8	qmcMrfInt	INTEGER	RO	Frühindikator für die A Frame-Length-Verletz
1.3.6.1.4.1.231.7.2.7.10.2.1.9	qmcSynInt	INTEGER	RO	Anzahl der qmc-Send
1.3.6.1.4.1.231.7.2.7.10.2.1.10	qmcIqOv	INTEGER	RO	Anzahl der Überläufe Interruptring-Ringbuff
1.3.6.1.4.1.231.7.2.7.10.2.1.31	qmcGlunGov	INTEGER	RO	Dieser kritische Fehle einem Reset. Er tritt a einen Pufferüberlauf i qmc-Fifo-Puffern gibt.
1.3.6.1.4.1.231.7.2.7.10.3	numOfDspChannelsExisting	INTEGER	RO	Enthält die Anzahl de vorhandenen DSP-Ka
1.3.6.1.4.1.231.7.2.7.10.4	numOfDspChannelsAvailable	INTEGER	RO	Enthält die Anzahl de DSP-Kanäle.
1.3.6.1.4.1.231.7.2.7.10.5	numOfDspChannelsInUse	INTEGER	RO	Enthält die Anzahl de verwendeten DSP-Ka
1.3.6.1.4.1.231.7.2.7.11	notificationGrouphlb20			Benachrichtigungsgru Trap-Spezifikationen
1.3.6.1.4.1.231.7.2.7.11.1	sendVoIPQualityNotification	TRAP		Diese Benachrichtigu gesendet, wenn die n Voice over IP-Verbind Qualitätsprobleme ha

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.11.2	sendIpPhoneTableNotification	TRAP		Diese Benachri wird gesendet, der Fehlerstatus Telefontabellen wenn die Konfig Telefonen geän
1.3.6.1.4.1.231.7.2.7.12.20	ipPhoneGroup			IP Phone Group
1.3.6.1.4.1.231.7.2.7.12.1	numOfIpPhoneTableEntries	INTEGER	RO	Enthält die Anz der Tabelle IP P
1.3.6.1.4.1.231.7.2.7.12.2	ipPhoneTable	SEQUENCE OF IpPhoneTableEntry		Diese Tabelle e über alle konfig und OptiCients, Standard H.323
1.3.6.1.4.1.231.7.2.7.12.2.1	ipPhoneTableEntry	IpPhoneTableEntry		Die Tabellenein Telefons.
1.3.6.1.4.1.231.7.2.7.12.2.1.1	ipPhoneIndex	INTEGER	RO	Identifikation ei Index aktivierte
1.3.6.1.4.1.231.7.2.7.12.2.1.2	subscriberNumber	DisplayString	RO	Dem Telefon zu Teilnehmer-Ruf
1.3.6.1.4.1.231.7.2.7.12.2.1.3	ipAddress	IpAddress	RO	Enthält die IP-A Telefons.
1.3.6.1.4.1.231.7.2.7.12.2.1.4	operationalState	INTEGER	RO	Enthält Informat Betriebszustand - installed(1) be Telefon in hg35 wurde, aber es betriebsbereit. - registriert(2) b Telefon in Betrie - active(3) bede Telefon tatsächl
1.3.6.1.4.1.231.7.2.7.12.2.1.5	errorState	INTEGER	RO	Enthält Informat Fehlerstatus de - normal(1) - warning(2) - minor(3) - major(4) - critical(5) - unknown(6)

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.12.3	gwPlatformMibObjects			
1.3.6.1.4.1.231.7.2.7.12.3.1	gwPlatformHardwareGroup			
1.3.6.1.4.1.231.7.2.7.12.3.1.1	gwPlatformHwConfigGroup			Die Hardware-Konfigu
1.3.6.1.4.1.231.7.2.7.12.3.1.1.2	gwPlatformHwDspModuleNumber	INTEGER (0..12)	RO	Die Anzahl der montie Module.
1.3.6.1.4.1.231.7.2.7.12.3.1.1.3	gwPlatformHwCpuType	DisplayString	RO	Der Prozessortyp.
1.3.6.1.4.1.231.7.2.7.12.3.1.1.4	gwPlatformHwCpuSpeed	INTEGER (0..1024)	RO	Die CPU-Geschwindi
1.3.6.1.4.1.231.7.2.7.12.3.2	gwPlatformMibTraps			
1.3.6.1.4.1.231.7.2.7.12.3.2.1	gwPlatformHwTrapGroup			
1.3.6.1.4.1.231.7.2.7.12.3.2.1.1	gwPlatformHwDspModuleStatusChange			Ein Trap wird gesend Status eines DSP-Mo
1.3.6.1.4.1.231.7.2.7.12.3.2.1.1.1	gwPlatformHwDspModuleStatusChangeModuleNumber	INTEGER (0..12)	RO	Die Nummer des DSP- Status sich geändert
1.3.6.1.4.1.231.7.2.7.12.3.2.1.1.2	gwPlatformHwDspModuleStatusChangeModuleStatus	INTEGER	RO	Der neue Status des
1.3.6.1.4.1.231.7.2.7.12.3.2.1.2	gwPlatformHwCpuSpeedChange			Ein Trap wird gesend Geschwindigkeit der
1.3.6.1.4.1.231.7.2.7.12.3.2.1.2.1	gwPlatformHwCpuSpeedChangeNewSpeed	INTEGER (0..1024)	RO	Die neue Geschwindi
1.3.6.1.4.1.231.7.2.7.12.3.2.1.2.2	gwPlatformHwCpuSpeedChangeOldSpeed	INTEGER (0..1024)	RO	Die alte Geschwindig
1.3.6.1.4.1.231.7.2.7.12.3.2.1.3	gwPlatformHwCpuTypeChange			Ein Trap wird gesend Prozessortyps.
1.3.6.1.4.1.231.7.2.7.12.3.2.1.3.1	gwPlatformHwCpuTypeChangeNewType	DisplayString	RO	Der neue Prozessorty
1.3.6.1.4.1.231.7.2.7.12.3.2.1.3.2	gwPlatformHwCpuTypeChangeOldType	DisplayString	RO	Der alte Prozessorty

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.1.1.5	gwPlatformHwFlashMemory	INTEGER (0..1024)	RO	Die Flash-Speic (1024x1024 Byt
1.3.6.1.4.1.231.7.2.7.13.1.1.6	gwPlatformHwDram	INTEGER (0..1024)	RO	Die DRAM-Grö (1024x1024 Byt
1.3.6.1.4.1.231.7.2.7.13.1.1.7	gwPlatformHwDspSlotCount	INTEGER (0..12)	RO	Die Anzahl der
1.3.6.1.4.1.231.7.2.7.13.1.1.10	gwPlatformHwMacAddress	OCTET STRING (SIZE(6))	RO	Die MAC-Adres
1.3.6.1.4.1.231.7.2.7.13.1.1.11	gwPlatformHwBootline	DisplayString	RO	Die Bootline.
1.3.6.1.4.1.231.7.2.7.13.1.1.12	gwPlatformHwSystemSerialNumber	DisplayString	RO	Die Seriennumm
1.3.6.1.4.1.231.7.2.7.13.1.1.13	gwPlatformHwMotherboardVersion	DisplayString	RO	Die Motherboar
1.3.6.1.4.1.231.7.2.7.13.1.1.14	gwPlatformHwPartListVersion	DisplayString	RO	Die Stücklistenv
1.3.6.1.4.1.231.7.2.7.13.1.1.15	gwPlatformHwBootromVersion	DisplayString	RO	Die Boot-ROM-
1.3.6.1.4.1.231.7.2.7.13.1.1.17	gwPlatformHwDspModuleTable	SEQUENCE OF GwPlatformHwDspModuleEntry		Tabelle mit den installierten DSI
1.3.6.1.4.1.231.7.2.7.13.1.1.17.1	gwPlatformHwDspModuleEntry	GwPlatformHwDspModuleEntry		Ein Eintrag in d Tabelle.
1.3.6.1.4.1.231.7.2.7.13.1.1.17.1.1	gwPlatformHwDspModuleIndex	INTEGER (1..12)	RO	Der Index in die
1.3.6.1.4.1.231.7.2.7.13.1.1.17.1.2	gwPlatformHwDspModuleType	DisplayString	RO	Die Typanzeige
1.3.6.1.4.1.231.7.2.7.13.1.1.17.1.3	gwPlatformHwDspModuleDescription	DisplayString	RO	Der beschreiben dsp-Moduls, z.B geschriebenen dsp und die Grö dem Modul.
1.3.6.1.4.1.231.7.2.7.13.1.1.18	gwPlatformHwResourceGroup			Die Hardware R
1.3.6.1.4.1.231.7.2.7.13.1.1.18.1	gwPlatformHwDramFree	Unsigned32	RO	Der freie DRAM sysMemPart+sa
1.3.6.1.4.1.231.7.2.7.13.1.1.18.2	gwPlatformHwFlashFree	Unsigned32	RO	Der freie Flash-
1.3.6.1.4.1.231.7.2.7.13.1.2	gwPlatformSwConfigGroup			Die Software-K
1.3.6.1.4.1.231.7.2.7.13.1.2.1	gwPlatformSwBuild	DisplayString	RO	Die berichtete B der geladenen S

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.2	gwManagementMib			Die Management MIB Kommunikationsgatew des Unternehmens. Siehe ar2500_manag
1.3.6.1.4.1.231.7.2.7.13.2.1	gwManagementMibObjects			
1.3.6.1.4.1.231.7.2.7.13.2.1.1	gwManagementMgmtGroup			Die Management-Gru
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1	gwManagementRouterPropertiesGroup	SEQUENCE OF GwManagementRouterPropertiesGroupEntry		Die Gruppe der Gatew Eigenschaftseinstellu
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1	gwManagementRouterPropertiesGroupEntry	GwManagementRouterPropertiesGroupEntry		Der Eintrag (Zeilentyp Tabelle der Gateway- settings.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1.1	gwManagementRouterPropertiesGroupIndex	INTEGER	RO	Der Index für die Tabe Einstellungen der Ga Eigenschaften.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1.2	gwManagementRouterPropertiesSystemName	DisplayString (SIZE(0..20))	RW	Ermöglicht die Einste Namens des Gateway
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1.3	gwManagementRouterPropertiesSystemLocation	DisplayString (SIZE(0..20))	RW	Ermöglicht die Einste Standorts des Gatewa
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1.4	gwManagementRouterPropertiesIpAddress	DisplayString (SIZE(0..20))	RO	IP-Adresse
1.3.6.1.4.1.231.7.2.7.13.2.1.1.1.1.5	gwManagementRouterPropertiesSubnetMask	DisplayString (SIZE(0..20))	RO	Subnetzmaske
1.3.6.1.4.1.231.7.2.7.13.2.1.3	gwManagementMgmtConfigGroup			Die Gruppe Managem Konfiguration
1.3.6.1.4.1.231.7.2.7.13.2.1.3.14	gwManagementCommConfigTable	SEQUENCE OF GwManagementCommConfigEntry		Die Gruppe der SNM Einstellungen für die
1.3.6.1.4.1.231.7.2.7.13.2.1.3.14.1	gwManagementCommConfigEntry	GwManagementCommConfigEntry		Der Eintrag (Zeilentyp der Tabelle der SNMP Konfigurationseinstell Verwaltung.
1.3.6.1.4.1.231.7.2.7.13.2.1.3.14.1.1	gwManagementCommConfigIndex	INTEGER	RO	Der Index für die Tabe SNMP-Konfigurations für die Verwaltung.
1.3.6.1.4.1.231.7.2.7.13.2.1.3.14.1.2	gwManagementCommConfigSetting	DisplayString	RO	Diese Spalte enthält d gemäß dem in der vo Spalte angegebenen interpretieren ist.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.4.1.3	gwManagementCommConfigIpAddr	GwSettingIpAddr	RC	DisplayString Der Teil der Ein Adresse enthält
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.4.1.4	gwManagementCommConfigType	GwSettingType	RC	MgmtConfigEntryType Typkennzeichnet Zeile der Tabelle Daten. - readCommuni - writeCommuni - trapReceiver(3
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.4.1.5	gwManagementCommConfigStatus	RowStatus	RC	Der Zeilenstatus SNMP-Konfigur für die Verwaltu
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6	gwManagementStaticRouteConfigTable	SEQUENCE OF GwManagementStaticRouteConfigEntry		Die Tabelle der Konfigurationen zur Konfiguration beim Systemsta
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1	gwManagementStaticRouteConfigEntry	GwManagementStaticRouteConfigEntry		Der Eintrag (Ze der Tabelle der Konfigurationen
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.1	gwManagementStaticRouteConfigIndex	GwManagementStaticRouteConfigIndex	RC	Der Konfigurati StaticRoute Co
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.2	gwManagementStaticRouteConfigName	DisplayString	RC	Die Bezeichnung dem Manager b
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.3	gwManagementStaticRouteDest	IpAddress	RC	ipRouteDest aus ipRouteTable.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.4	gwManagementStaticRouteGateway	IpAddress	RC	ipRouteNextHop ipRouteTable.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.5	gwManagementStaticRouteMask	IpAddress	RC	ipRouteMask aus ipRouteTable.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.6	gwManagementStaticRouteTos	INTEGER	RC	ipRouteAge aus
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.1.6.1.7	gwManagementStaticRouteStatus	RowStatus	RC	Der Status dies Routeneintrags.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.4	globalDataTable	SEQUENCE OF GlobalDataEntry		Tabelle mit glob Gateway rg250
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.4.1	globalDataEntry	GlobalDataEntry		Eintrag in der gl Datentabelle.
1.3.6.1.4.1.231.7.2.7.13.2.1.1.8.4.1.1	globalDataID	Integer32 (0..1)	RC	Index, um einen der globalen Da nachzuschlagen

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.2	system1Location	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.3	system1Name	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.4	system1IPAddress	DisplayString (SIZE(0..20))	RO	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.5	system1SubnetMask	DisplayString (SIZE(0..20))	RO	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.6	system1DateTime	DisplayString (SIZE(14..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.7	system1CountryCode	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.8	system1UpTime	TimeTicks	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.9	gwEnableGatekeeperUsage	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.10	gwEnableSCNProtocolTunneling	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.11	gwEnableH323TerminalSupport	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.12	gwEnablePreH450CallForward	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.13	gwEnablePreH450CallTransfer	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.14	gwEnableH450FeatureSupport	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.15	gwEnableH235Profile1Support	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.16	u2OnlineHelp	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.17	u2DocumentationLocation	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.18	server1SystemID	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.19	server1IntegrOnOff	BooleanValue	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.20	server1AuthIpAddress	DisplayString (SIZE(0..20))	RW	
1.3.6.1.4.1.231.7.2.7.13.2.1.4.1.21	server1AuthPort	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.3	gwMSCandApplications			HG3550 V2 / HiPath 4 Siehe cg2500.my
1.3.6.1.4.1.231.7.2.7.13.3.1	mscTable			
1.3.6.1.4.1.231.7.2.7.13.3.1.1	mscStats			

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.1.1	mscStatsOverall			msc Gesamtsta
1.3.6.1.4.1.231.7.2.7.13.3.1.1.1	mscOutgoingRTPpackets	Counter	RO	Ausgehende RT (insgesamt).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.2	mscOutgoingRTPLostpackets	Counter	RO	Ausgehende RT (insgesamt).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.3	mscIncomingRTPpackets	Counter	RO	Eingehende RT (insgesamt).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.4	mscIncomingRTPLostpackets	Counter	RO	Eingehende RT (insgesamt).
1.3.6.1.4.1.231.7.2.7.13.3.1.1.5	mscTotalBytesSent	Counter	RO	Gesamtzahl der
1.3.6.1.4.1.231.7.2.7.13.3.1.1.6	mscTotalBytesReceived	Counter	RO	Gesamtzahl der Bytes.
1.3.6.1.4.1.231.7.2.7.13.3.1.2	mscStatsPerCallTable	SEQUENCE OF MscStatsPerCallEntry		Die Tabelle der Anruf.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1	mscStatsPerCallEntry	MscStatsPerCallEntry		Die Msc-Statisti Ressource.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.1	mscStatsPerCallInd	INTEGER		Der Tabellenind
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.2	mscPeerCanonicalName	OCTET STRING (SIZE (0..64))	RO	Der Verbindung angerufenen Nu
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.3	mscDestIP	OCTET STRING (SIZE (0..15))	RO	Die Ziel-IP-Adre
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.4	mscBeginTime	OCTET STRING (SIZE (0..64))	RO	Uhrzeit, zu der gestartet wurde
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.5	mscEncoder	INTEGER	RO	Encoder, der be verwendet wird. - g711ULaw(0) - g723(4) - g711ALaw(8) - g729(18)

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.6	mscCsp2dDecoder	INTEGER	RO	Decoder, der bei dies verwendet wird. - g711ULaw(0) - g723(4) - g711ALaw(8) - g729(18)
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.7	mscCsp2dOutgoingRTPpackets	Counter	RO	Ausgehende RTP-Pa Anruf).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.8	mscCsp2dOutgoingRTPpacketsLost	Counter	RO	Ausgehende RTP-Pa (pro Anruf).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.9	mscCsp2dIncomingRTPpackets	Counter	RO	Eingehende RTP-Pak Anruf).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.10	mscCsp2dIncomingRTPpacketsLost	Counter	RO	Eingehende RTP-Pak (pro Anruf).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.11	mscCsp2dBytesSent	Counter	RO	Gesamtzahl der gese
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.12	mscCsp2dBytesReceived	Counter	RO	Gesamtzahl der empf Bytes.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.13	mscCsp2dRndTripNetworkDelay	Integer32	RO	Round Trip Network D für diese Verbindung.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.14	mscCsp2dActualJitter	Integer32	RO	Der aktuelle Jitter (in Verbindung.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.15	mscCsp2dJitterBufferDepth	Integer32	RO	Aktuelle Größe des D Jitterpuffers (in ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.16	mscCsp2dRtpEncodings	Integer32	RO	Anzahl der gesamme einem RTP-Paket, die Gateway gesendet w
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.17	mscCsp2dAverageNetworkDelay	Integer32	RO	Durchschnittliche Net für diesen Anruf (in m
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.18	mscCsp2dJitterLan	Integer32	RO	Jitter im LAN dieser V
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.19	mscCsp2dFractionLostOutgoing	Integer32	RO	Bruchteil der RTP-Da einer bestimmten Qu seit dem Senden des Empfängerberichts ve gegangen sind.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.20	mscCsp2dMaxFractionLostOutgoing	Integer32	RO	Maximaler fraktioniert Paketverlust unter all teilnehmenden Sitzun außer uns selbst.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.21	mscSpeech2TooLatePacketCount	Counter32	RO	Die Anzahl der seit Beginn der
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1.22	mscEnc2TimePerPacket	Integer32	RO	Kodierungszeit
1.3.6.1.4.1.231.7.2.7.13.3.1.2	mscConfig			Msc-Konfigurati
1.3.6.1.4.1.231.7.2.7.13.3.1.2.1	mscRtpPortLow	INTEGER (1024..65535)	RW	Die niedrige Po RTCP-Ports.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.2	mscRtpPortHigh	INTEGER (1024..65535)	RW	Die hohe Portgr RTCP-Ports.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.3	mscT38PortLow	INTEGER (1024..65535)	RW	Die niedrige Po Ports (T38-fax).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.4	mscT38PortHigh	INTEGER (1024..65535)	RW	Die hohe Portgr (T38-fax).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.5	mscTrafficStatistic	BooleanValue	RW	TrafficStatistic e Generierung de (durch das GW oder deaktiviert
1.3.6.1.4.1.231.7.2.7.13.3.1.2.9	mscJitterBufferAdaptation	BooleanValue	RW	Wenn dies vom wird, passt der seine Tiefe basi Statistiken an. der Host die Jitt zur Laufzeit exp basierend auf d generierten Sta
1.3.6.1.4.1.231.7.2.7.13.3.1.2.10	mscJitterType	INTEGER	RW	Jitterpuffer-Anp (0..TIS, 1..HLB2
1.3.6.1.4.1.231.7.2.7.13.3.1.2.11	mscJitterCacheUpdateInterval	INTEGER (5..10)	RW	Aktualisierungsi Cache: 5 - 10 S
1.3.6.1.4.1.231.7.2.7.13.3.1.2.15	mscJitterTotalFractionLostWeight	INTEGER (0..1000)	RW	Faktor zur Glätt variierenden An eingehender RT Jitter in 10 Proz 100,0 %. Defau
1.3.6.1.4.1.231.7.2.7.13.3.1.2.16	mscJitterMinFractionLost	INTEGER (0..1000)	RW	Unterer Schwel die adaptive Ste Jitterpuffergröß RTP-Pakete in 1000 ist 100,0 % (0,5 %).

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.1.2.17	mscJitterMaxFractionLost	INTEGER (0..1000)	RW	Oberer Schwellenwer die adaptive Steueru Jitterpuffergröße für e RTP-Pakete in 10 Pro 1000 ist 100,0 %. Def
1.3.6.1.4.1.231.7.2.7.13.3.1.2.18	mscJitterFactor	INTEGER (0..1000)	RW	Faktor für die Größen des Jitterpuffers in Be durchschnittlichen Jitt 4.
1.3.6.1.4.1.231.7.2.7.13.3.1.2.19	mscJitterIncrement	INTEGER (100..300)	RW	Schrittweite des Jitter wenn jitterMinFraction 100 Mikrosekundensc überschritten wird: St (20 ms).
1.3.6.1.4.1.231.7.2.7.13.3.1.2.20	mscJitterDecrement	INTEGER (100..300)	RW	Verringerung des Jitte wenn der geglättete durchschnittliche Jitte jitterMaxFractionLost Mikrosekundenschritt Standard: 100 (10 ms
1.3.6.1.4.1.231.7.2.7.13.3.1.2.21	mscJitterBufferAvarageDelay	INTEGER (0..300)	RW	Die Tiefe des Jitterpu in ms. Wird vom Host Konfigurationszeit fes Der DSP rundet den V Vielfaches von 10 ms - 300 ms
1.3.6.1.4.1.231.7.2.7.13.3.1.3	mscDspConfig			Msc DSP-Konfiguratio
1.3.6.1.4.1.231.7.2.7.13.3.1.3.1	mscVadEnable	BooleanValue	RW	Sprachaktivitätserken aus; VAD wird explizit durchgeführt.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.4	mscEchoCancellerEnable	BooleanValue	RW	Echounterdrückung e Kompensation für Ech bei einer Verbindung das Sprachportal zu a Telefonen auftreten k
1.3.6.1.4.1.231.7.2.7.13.3.1.3.5	mscDtmfReceiveEnable	BooleanValue	RW	Dtmf Outband Signali aus.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.6	mscDtmfDefaultToneLength	INTEGER (50..300)	RW	Standardlänge des Im DTMF-Töne.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.7	mscG711MaxRecvBytes	INTEGER (80..960)	RW	Max. Bytes von G711 RTP-Daten.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.8	mscG723MaxRecvBytes	INTEGER (24..96)	RW	Max. Bytes von G723 RTP-Daten.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.1.3.7	mscG729MaxRecvBytes	INTEGER (20..120)	RW	Max. Bytes von kodierten RTP-I
1.3.6.1.4.1.231.7.2.7.13.3.1.3.8	mscG711EncTimePerPacket	INTEGER (10..120)	RW	Definiert die Ko pro Paket für di G711.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.9	mscG723EncTimePerPacket	INTEGER (30..120)	RW	Definiert die Ko pro Paket für di G723.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.10	mscG729EncTimePerPacket	INTEGER (20..120)	RW	Definiert die Ko pro Paket für di G729.
1.3.6.1.4.1.231.7.2.7.13.3.1.3.11	mscDtmfDefaultPauseLength	INTEGER (50..300)	RW	Standard-Pause gesendeten DM
1.3.6.1.4.1.231.7.2.7.13.3.2	gwApplications			
1.3.6.1.4.1.231.7.2.7.13.3.2.1	deviceConfiguration			
1.3.6.1.4.1.231.7.2.7.13.3.2.2	deviceResourceStatistics			
1.3.6.1.4.1.231.7.2.7.13.3.2.2.1	deviceResourceMgmtTable	SEQUENCE OF DeviceResourceMgmtEntry		Statistiktabelle f von Geräteress
1.3.6.1.4.1.231.7.2.7.13.3.2.2.1.1	deviceResourceMgmtEntry	DeviceResourceMgmtEntry		

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.2.2.1.1	devId	INTEGER	RO	eindeutige ID eines G - devIdISDNSubs(0) - devIdISDNTrunk(1) - devIdHFA(2) - devIdPayload(3) - devIdMoH(4) - devHXG3RTP(5) - devHXG3Fax(6) - devHXG3PPP(7) - devHXG3Vcapi(8) - devIdWAML(10) - devIdISDNTrunk1(1 - devIdISDNTrunk2(1 - devIdISDNTrunk3(1 - devIdISDNTrunk4(1 - devIdDMC(15) - devIdRTP(100) - devIdFax(101) - devIdPPP(102) - devIdVcapi(103) - devIdNu(104) - devIdLegk(105) - devIdUnused(106) - deviceId_Rtp_H323 - deviceId_Fax_H323 - deviceId_Rtp_SIP(1 - deviceId_Fax_SIP(1
1.3.6.1.4.1.231.7.2.7.13.2.2.1.2	devMaxCh	Integer32	RO	Effektive max. Anzah verwendbaren Kanäle eindeutige ID eines G - deviceId_Rtp_H323 - deviceId_Fax_H323 - deviceId_Rtp_SIP(1 - deviceId_Fax_SIP(1

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.2.1.13	devSerializedChannels	Integer32	RO	Anzahl der derz Kanäle. Eindeut - deviceId_Rtp_ - deviceId_Fax_ - deviceId_Rtp_ - deviceId_Fax_
1.3.6.1.4.1.231.7.2.7.13.3.2.2	gwParameters			Gateway-Param
1.3.6.1.4.1.231.7.2.7.13.3.2.3	gwGlobalTrace			
1.3.6.1.4.1.231.7.2.7.13.3.2.3.1	gwGlobalTraceID	Integer32	RW	
1.3.6.1.4.1.231.7.2.7.13.3.2.3.2	gwConsoleTraceOnOff	BooleanValue	RW	Schaltet die Abl gesamten Kons
1.3.6.1.4.1.231.7.2.7.13.3.2.3.3	gwFileTraceOnOff	BooleanValue	RW	Schaltet die ges Dateiverfolgung
1.3.6.1.4.1.231.7.2.7.13.3.2.3.4	gwTraceMaxFileSize	Integer32	RO	Maximale Größ
1.3.6.1.4.1.231.7.2.7.13.3.2.3.5	gwTraceTimerValue	Integer32	RO	Timer für die Ve
1.3.6.1.4.1.231.7.2.7.13.3.2.3.6	gwTraceMaxBuffSize	Integer32	RO	Maximale Puffe Ablaufverfolgun
1.3.6.1.4.1.231.7.2.7.13.3.2.4	gwEventLog			
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1	gwTrapGenerationTbl	SEQUENCE OF GwTrapGenerationEntry		Die Tabelle zur von Traps zeigt Ereignisse Trap und für welche
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1	gwTrapGenerationEntry	GwTrapGenerationEntry		Ein Eintrag in d Generierung vo bestimmtes Ere
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.1	gwTrapEventID	Integer32	RC	Dieser Index de Generierung vo ein bestimmtes
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.2	gwTrapEventName	OCTET STRING (SIZE (0..64))	RC	
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.3	gwTrapType	Integer32	RC	Dies bestimmt, Ereignis ein Tra nicht.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.4	gwTrapFlag	BooleanValue	RC	
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.1.5	gwRebootFlag	BooleanValue	RC	

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.6	gwTrapEntType	Integer32	RC	Dies bestimmt, ob für Ereignis ein Trap erze nicht.
1.3.6.1.4.1.231.7.2.7.13.3.2.4.1.7	gwTrapEntRowCmd	RowCmd	RC	Wenn Sie dies so ein es zerstört wird, wird gelöscht.
1.3.6.1.4.1.231.7.2.7.13.3.2.5	gwStatistics			Gateway-Statistik
1.3.6.1.4.1.231.7.2.7.13.3.2.5.1	gwStatNumLANVoiceCallsRcvd1H	Counter32	RO	Anzahl der eingehend Sprachanrufe, die in Stunde empfangen w
1.3.6.1.4.1.231.7.2.7.13.3.2.5.2	gwStatNumLANVoiceCallsRcvd24H	Counter32	RO	Anzahl der eingehend Sprachanrufe, die in Stunden empfangen w
1.3.6.1.4.1.231.7.2.7.13.3.2.5.3	gwStatNumLANFaxCallsRcvd1H	Counter32	RO	Anzahl der in der letz empfangenen eingeh Faxanrufe.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.4	gwStatNumLANFaxCallsRcvd24H	Counter32	RO	Anzahl der eingehend die in den letzten 24 S empfangen wurden.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.5	gwStatNumLANVoiceCallsConn1H	Counter32	RO	Anzahl der eingehend Sprachanrufe, die in Stunde verbunden wa
1.3.6.1.4.1.231.7.2.7.13.3.2.5.6	gwStatNumLANVoiceCallsConn24H	Counter32	RO	Anzahl der eingehend Sprachanrufe, die in Stunden verbunden w
1.3.6.1.4.1.231.7.2.7.13.3.2.5.7	gwStatNumLANFaxCallsConn1H	Counter32	RO	Anzahl der eingehend die in der letzten Stu waren.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.8	gwStatNumLANFaxCallsConn24H	Counter32	RO	Anzahl der eingehend die in den letzten 24 S verbunden waren.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.9	gwStatNumPBXVoiceCallsRcvd1H	Counter32	RO	Anzahl der in der letz empfangenen ausgeh Sprachanrufe.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.10	gwStatNumPBXVoiceCallsRcvd24H	Counter32	RO	Anzahl der in den letz 24 Stunden empfange ausgehenden Sprach
1.3.6.1.4.1.231.7.2.7.13.3.2.5.11	gwStatNumPBXFaxCallsRcvd1H	Counter32	RO	Anzahl der in der letz empfangenen ausgeh Faxanrufe.

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.2.5.12	gwStatsNumPBXFaxCallsCounter24H	Counter	RO	Anzahl der in de 24 Stunden emp ausgehenden F
1.3.6.1.4.1.231.7.2.7.13.3.2.5.13	gwStatsNumPBXVoiceCallsCounter1H	Counter	RO	Anzahl der in de verbundenen au Sprachanrufe.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.14	gwStatsNumPBXVoiceCallsCounter24H	Counter	RO	Anzahl der in de 24 Stunden verb ausgehenden S
1.3.6.1.4.1.231.7.2.7.13.3.2.5.15	gwStatsNumPBXFaxCallsCounter1H	Counter	RO	Anzahl der in de verbundenen au
1.3.6.1.4.1.231.7.2.7.13.3.2.5.16	gwStatsNumPBXFaxCallsCounter24H	Counter	RO	Anzahl der ausg Faxanrufe, die i Stunden verbun
1.3.6.1.4.1.231.7.2.7.13.3.2.5.17	gwStatsCumLANCallDuration1H	Counter	RO	Kumulative Ges Sekunden in de
1.3.6.1.4.1.231.7.2.7.13.3.2.5.18	gwStatsCumLANCallDuration24H	Counter	RO	Kumulative Ges in Sekunden in Stunden.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.19	gwStatsCumPBXCallDuration1H	Counter	RO	Kumulative Ges Sekunden in de
1.3.6.1.4.1.231.7.2.7.13.3.2.5.20	gwStatsCumPBXCallDuration24H	Counter	RO	Kumulative Ges in Sekunden in Stunden.
1.3.6.1.4.1.231.7.2.7.13.3.2.5.25	gwStatsNumCurCalls	Counter	RO	Kumulierte Anz Anrufe
1.3.6.1.4.1.231.7.2.7.13.3.2.5.30	gwStatsNumLANDataCallsCounter1H	Counter	RO	Anzahl der eing Datenanrufe, di Stunde empfang
1.3.6.1.4.1.231.7.2.7.13.3.2.5.31	gwStatsNumLANDataCallsCounter24H	Counter	RO	Anzahl der eing Datenanrufe, di Stunden empfa
1.3.6.1.4.1.231.7.2.7.13.3.2.5.32	gwStatsNumLANDataCallsCounter1H	Counter	RO	Anzahl der eing Datenanrufe, di Stunde verbund
1.3.6.1.4.1.231.7.2.7.13.3.2.5.33	gwStatsNumLANDataCallsCounter24H	Counter	RO	Anzahl der eing Datenanrufe, di Stunden verbun
1.3.6.1.4.1.231.7.2.7.13.3.2.5.34	gwStatsNumPBXDataCallsCounter1H	Counter	RO	Anzahl der eing Datenanrufe, di Stunde empfang

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.2.5.35	gwv2tab35	NumPBXDataCallCounter24H	RO	Anzahl der eingehend Datenanrufe, die in de Stunden empfangen w
1.3.6.1.4.1.231.7.2.7.13.3.2.5.36	gwv2tab36	NumPBXDataCallCounter1H	RO	Anzahl der eingehend Datenanrufe, die in de Stunde verbunden wa
1.3.6.1.4.1.231.7.2.7.13.3.2.5.37	gwv2tab37	NumPBXDataCallCounter24H	RO	Anzahl der eingehend Datenanrufe, die in de Stunden verbunden w
1.3.6.1.4.1.231.7.2.7.13.3.7.2	gwv2TrapGroup			The HXG3 SNMP Tra
1.3.6.1.4.1.231.7.2.7.13.3.7.2.1	gwv2Trap1	TRAP		Weist auf ein Problem RG2500-Software hin gesendet, wenn der A ein überwindbares Er Ereignisprotokoll erke
1.3.6.1.4.1.231.7.2.7.13.3.7.2.3	gwv2Startup	TRAP		Zeigt das Hochfahren V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.4	gwv2Reboot	TRAP		Zeigt den Neustart vo an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.5	gwv2Threshold	TRAP		Zeigt an, dass ein Sch HG3550 V2 erreicht is
1.3.6.1.4.1.231.7.2.7.13.3.7.2.6	gwv2WanLinkUp	TRAP		Zeigt eine WAN-Verbi HG1500 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.7	gwv2WanLinkDown	TRAP		Zeigt eine WAN-Verbi HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.8	gwv2IpLinkUp	TRAP		Zeigt eine IP-Verbindu HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.9	gwv2IpLinkDown	TRAP		Zeigt einen IP Linkdo HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.2.10	gwv2AuxTrap	TRAP		Zeigt einen Hilfstrap d V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.7.3.2.1	trap2Num	DisplayString	RO	Definiert eine Softwar Fehlernummer - Verw Trap-Typ und Informa Software-Komponent Baugruppe/Port, um d Fehler zu isolieren.
1.3.6.1.4.1.231.7.2.7.13.3.7.3.2.2	trap2Text	DisplayString	RO	Definiert den Text, de hochgeladen werden

Objekt-ID	Objektname	Syntax	Access	Beschreibung
1.3.6.1.4.1.231.7.2.7.13.3.2.1	trapType	INTEGER	RO	Die Art des aufg - software(1) - hardware(2) - startup(3) - reboot(4) - threshold(5) - wanLinkUp(6) - wanLinkDown - ipLinkUp(8) - ipLinkDown(9) - auxTrap(10)
1.3.6.1.4.1.231.7.2.7.13.3.2.2	trapSeverity	DisplayString	RO	Definiert den Sc Traps.

Tabelle 14: Definitionen in der Firmen-spezifischen MIB

Objekt-ID	Objektname	Beschreibung
1.3.6.1.4.1.4329	siemens	HG3550-V11 MIB, siehe hg3500_v11.my
1.3.6.1.4.1.4329.2	iandcAdmin	
1.3.6.1.4.1.4329.2.24	hg3550v11	Definition der System-OID für hg3550 V2

Tabelle 15: Gesammelte Liste der Traps (wiederholt)

Objekt-ID	Objektname	Beschreibung
1.3.6.1.2.1.10.20.2.0.1	isdnMibCallInformation	Dieser Trap/diese Information wird unter den folgenden Bedingungen an den Manager gesendet: - bei eingehenden Anrufen für jeden Anruf, der aus Richtliniengründen abgelehnt wird (z. B. unbekannter Nachbar oder Zugriffsverletzung) - bei ausgehenden Anrufen, wenn festgestellt wird, dass ein Anrufversuch letztendlich fehlgeschlagen ist. Für den Fall, dass die Anrufwiederholung aktiv ist, erfolgt dies, nachdem alle Wiederholungsversuche fehlgeschlagen sind. - wenn sich ein Anruf verbindet. In diesem Fall sollte das Objekt isdnBearerCallConnectTime in den Trap aufgenommen werden.

Objekt-ID	Objektname	Beschreibung
1.3.6.1.4.1.231.7.2.7.5	sendAlarmWithValues	Tritt ein Fehler auf, wird geprüft, ob die errorClass so konfiguriert ist, dass sie eine sofortige Signalisierung auslöst. Wenn ja, wird ein Trap an die Managementstation gesendet, die die oben genannten Informationen enthält.
1.3.6.1.4.1.231.7.2.7.6	fileOverflowError	Informiert den Manager, dass die Tabelle Trap Hystory zu groß geworden ist. Wenn die Größe der Tabelle nicht vom Manager reduziert wird (durch Zurücksetzen von numberOfTrapHistoryEntries), werden die ältesten Trapinformationen von nun an überschrieben.
1.3.6.1.4.1.231.7.2.7.11.1	sendVoIPQualityNotification	Diese Benachrichtigung wird gesendet, wenn die neueste Voice over IP-Verbindung Qualitätsprobleme hatte.
1.3.6.1.4.1.231.7.2.7.11.2	sendIpPhoneTableNotification	Diese Benachrichtigung wird gesendet, wenn sich der Fehlerstatus eines IP-Telefontabelleneintrags ändert oder wenn die Konfiguration von IP-Telefonen geändert wird.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.1	gw2Trap1	Weist auf ein Problem mit der RG2500-Software hin. Wird gesendet, wenn der Admin-Server ein überwindbares Ereignis im Ereignisprotokoll erkennt.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.3	gw2Startup	Zeigt das Hochfahren von HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.4	gw2Reboot	Zeigt den Neustart von HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.5	gw2Threshold	Zeigt an, dass ein Schwellenwert in HG3550 V2 erreicht ist.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.6	gw2WanLinkUp	Zeigt eine WAN-Verbindung des HG1500 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.7	gw2WanLinkDown	Zeigt eine WAN-Verbindung des HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.8	gw2IpLinkUp	Zeigt eine IP-Verbindung des HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.9	gw2IpLinkDown	Zeigt einen IP Linkdown des HG3550 V2 an.
1.3.6.1.4.1.231.7.2.7.13.3.2.8.10	gw2AuxTrap	Zeigt einen Hilfstrap des HG3550 V2 an.

2.21 IP-Ports

2.21.1 Allgemeine Informationen

Die Port-Zuordnungen finden sie in der Interface Management Database (IFMDB).

Der Zugriff auf die IFMDB kann über das Intranet oder Partner Portal erfolgen:

- Intranet
- Homepage > Index „I“ > IFMDB (Interface Management DataBase)
- Partner Portal

- Support > Interface Management (IFMDB)

2.21.2 Port-Bereich

2.21.2.1 Masterverbindungen IP-Trunking + DMC (IP-Trunking und IPDA)

Port-Wertebereich mit AMO CGWB

Für die Masterverbindungen für IP-Trunking und für die DMC-Slaveverbindungen bei denen die HG 3500 ein DMC-Endpunkt ist (d.h. bei IP-Trunking oder IPDA) wird der UDP-Portbereich mit dem **AMO CGWB** eingerichtet. Der entsprechenden Parameter ist **UDPPRTLO** im Zweig **TYP=ASC**. **UDPPRTHI** ist nicht änderbar. Er wird berechnet aus dem Wert von **UDPPRTLO** + 999 Ports.

Der Default-Wert für **UDPPRTLO** ist 29100.

Wichtig: Da Verbindungen mit/ohne DMC oder/und SPE geschalten werden können (abhängig von der Konfiguration), muss immer die maximal benötigte Portanzahl vom Gateway reserviert werden, auch wenn eventuell nur eine geringere Anzahl von Ports verwendet wird!

2.21.2.2 Master-Verbindungen IPDA (HG 3575/HG 3500) + DMC (HG 3575)

- Masterverbindungen IPDA

  Der Paramerter **UDPPORT** im AMO SIPCO wird für den Payloadstream der IPDA-Masterverbindung verwendet, d.h. für Verbindungen der IPDA-HG 3500 zur HG 3575 und umgekehrt und für Verbindungen von HG 3575 zu HG 3575.

  Für IPDA-Master-Verbindungen wird lediglich der Startwert im AMO SIPCO, **TYP=DIFFSERV**, **UDPPORT=<4352 ... 65083>** definiert. Der obere Wert (=tatsächlich maximal verwendete Ports) berechnet sich aus der Anzahl der B-Kanäle der verwendeten Baugruppe.

  Der niederwertigste Port ist im Bereich [4352 ... 65280] auf geraden Werten einstellbar.
- DMC-Slaveverbindungen

  Für DMC-Slave-Verbindungen, bei denen die NCUI2+/NCUI4 der DMC-Endpunkt ist, gilt der Parameter **UDPPORT** im AMO SIPCO ebenfalls. Es werden automatisch die nachfolgenden Ports verwendet.

  Für DMC-Slaveverbindungen, bei denen die STMI2/STMI4 der DMC-Endpunkt ist, gilt der Portbereich aus AMO CGWB (**UDPPRTLO**-**UDPPRTHI**).

  Wichtig: Verwendete Ports können nicht geändert werden, mit Ausnahme von Ports für „UDP-Payload“!

2.21.3 Hinweise für Netzwerkadministratoren

Wichtig: IP-Pakete mit den verwendeten Ports (hard-coded und per AMO konfiguiert) müssen im IP-Netzwerk transparent geroutet werden, d.h. es darf keine Manipulation (z.B. durch Firewall) vorgenommen werden. Ohne transparentes Routing kommt es zu funktionalen Problemen!

2.21.4 Beispiele

Zur Verdeutlichung der Verkehrsbeziehungen, auf denen bestimmte Ports genutzt werden folgen einige Beispiele.

2.21.4.1 Payload

Die verwendeten Ports werden je beteiligter HG 3500 bzw. HG 3575 aus dem durch den Parameter UDPPORT (AMO SIPCO) bestimmten Portbereich genommen. Der Portbereich für RTP/RTCP ist durch folgendes Intervall bestimmt: [UDPPORT .. UDPPORT + 960].

Port 4007 wird zum Streckentest bei schlechter Payload-Qualität verwendet. Siehe dazu Abschnitt 2.9.1, „Wann wird Payload Survivability genutzt?“ im Dokument „IP Distributed Architecture (IPDA)“ - Stichwort „UDP-Ping“.

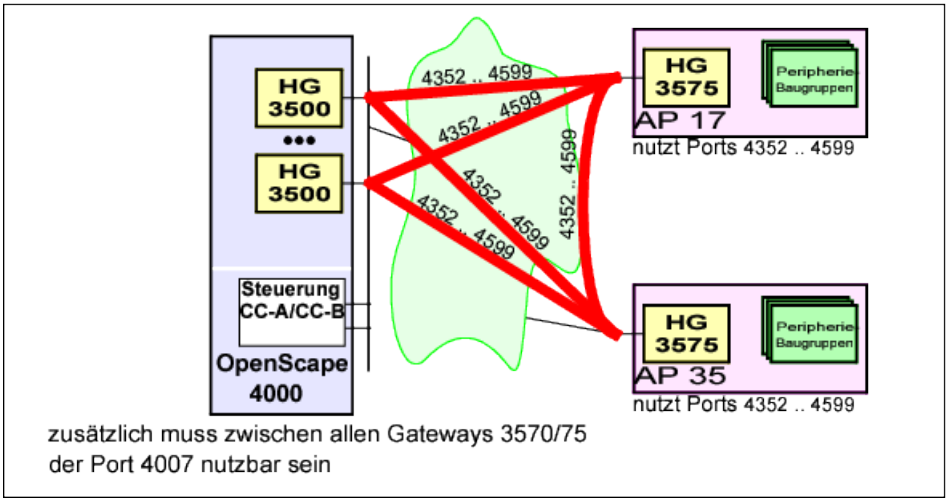


Abbildung 40: Beispiel: Port-Nutzung für Payload

2.21.4.2 Signalisierung

Unter dem Begriff Signalisierung wird der gesamte Datenaustausch zwischen CC und Access Point behandelt. Das beinhaltet das Laden und Steuern von Peripheriebaugruppen, sicherheitstechnische Meldungen, Routinetests und natürlich auch alle Call-Processing Meldungen bis zu den Displaytexten der Telefone.

Jeder Access Point, d.h. jede HG 3575 hat eine **Signalisierungsverbindung** zum aktiven CC. Diese Verbindung wird immer vom CM aufgebaut. Als Source Port werden abwechselnd 1124 bzw. 1125 verwendet. Destination Port (auf HG 3575) ist 4000.

Das Laden der Loadware der HG 3575 geschieht über FTP. Dazu meldet sich die HG 3575 am FTP-Server des CM an. Dieser erlaubt ausschließlich Lesezugriffe von eingerichteten HG 3575 und erlaubt zu einem Zeitpunkt nur einen Download.

Ist Signaling Survivability eingerichtet werden zusätzliche Verbindungen genutzt.

Die **Überwachungsverbindung** überwacht die prinzipielle Verfügbarkeit des Wegs vom CM zur HG 3575 im IP-Netz - parallel zur Signalisierungsverbindung. Diese Verbindung wird immer vom CC aufgebaut. Als Source Port werden abwechselnd 1126 bzw. 1127 verwendet. Destination Port (auf HG 3575) ist 4001.

Ist die Überwachungsverbindung unterbrochen, wird die Signalisierungsverbindung über PSTN-Router und Modem umgeroutet. Die IP-Adressen und Ports der Signalisierungsverbindung bleiben dabei erhalten.

Die Erreichbarkeit einer HG 3575 mit Signaling Survivability über Modem wird im Normalbetrieb zyklisch getestet. Diese Verbindung wird immer vom CM aufgebaut. Als Source Port werden abwechselnd 1128 bzw. 1129 verwendet. Destination Port (auf HG 3575) ist 4002.

Wichtig: Für SURVPATH-Test: Vom aktiven CC (physische Linux-Adresse von V6) ergeht eine ARP-Anforderung für die WAML-MAC. In der Folge werden Pakete an Port 4002 mit der IP-Adresse der WAML MAC NCUI an WAML geroutet.
Für normale Signalisierungs-Survivability: Die normale Signalisierung geschieht an Port 4000. Wenn das Keep Alive für den Supervisory-Port 4001 fehlschlägt, ergeht vom aktiven CC (physische Linux-Adresse von V4001) eine ARP-Anforderung für die WAML-MAC. In der Folge werden Pakete mit der IP-Adresse der NCUI aber der WAML-MAC direkt in derselben TCP-Sitzung an WAML-Port 4000 geroutet, d.h. es wird keine neue TCP-Sitzung hergestellt, sondern nur die MAC-Zieladresse durch die WAML-MAC ersetzt.

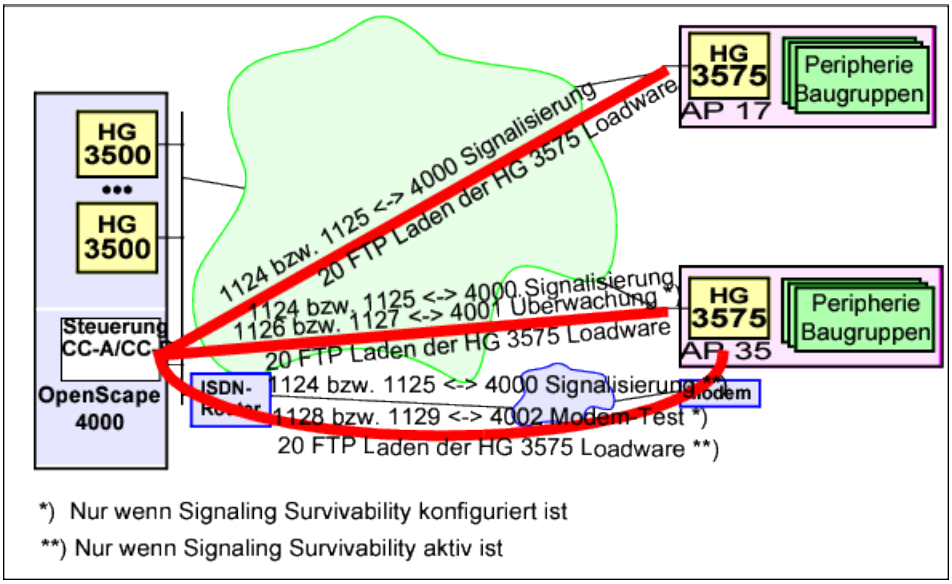


Abbildung 41: Port-Nutzung für Signalisierung

2.21.4.3 SNMP

Die Gateways HG 3500 und HG 3575 sind mit einem SNMP Agenten ausgestattet, der den Lesezugriff auf Daten der MIB-2 und einer Gateway-spezifischen MIB erlaubt. Siehe dazu Kapitel 20, „SNMP Support HG 3500 / HG 3575“. Es werden ausschließlich Lesezugriffe unterstützt. Es können keine Parameter verändert werden. Es werden keine Traps übermittelt.

Der SNMP-Agent wartet standardgemäß an Port 161.

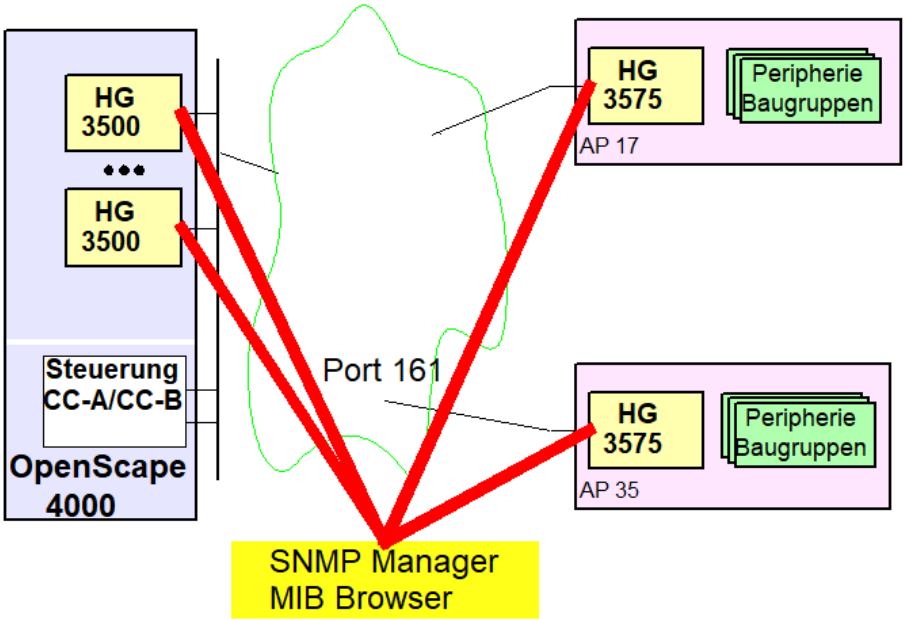


Abbildung 42: Port-Nutzung für SNMP-Zugriffe

2.21.4.4 Diagnose

Zur Fehlerdiagnose können auf den Gateways HG 3500 und HG 3575 zusätzliche Dienste aktiviert werden, die normalerweise unzugänglich sind (Ports gesperrt).

Dies sind

SSH	Port 22	TCP
HTTPS/WBM	Port 443	Web-Server zum Abruf von Diagnosedaten

Für die HG 3575 ist der Zugang über einrichtbare Logons mit Passwort geschützt. Die HG 3500 verwendet feste Werte dafür.

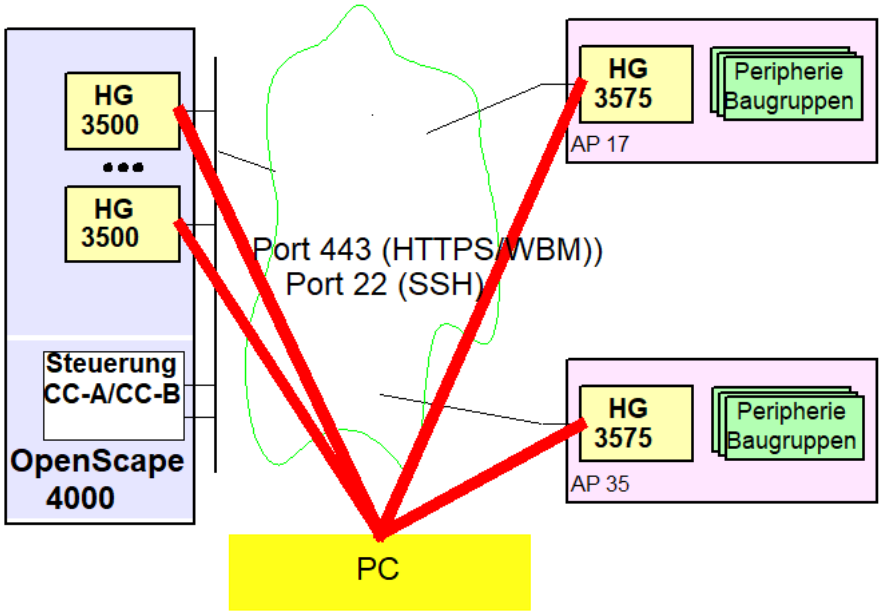


Abbildung 43: Port-Nutzung für Diagnose

2.22 WBMs der Baugruppen

Sie finden eine Oberflächenbeschreibung der WBMs zu HG 3500 und HG 3575 unter folgenden Link:

http://apps.g-dms.com:8081/techdoc/de/P31003H31A0M1030100A9/index.htm

2.23 Diagnosemöglichkeiten HG 3500 / HG 3575

Die Diagnosemöglichkeiten der Gateways HG 3500 und HG 3575 werden über das WBM aufgerufen. Die Tracekomponenten sind im WBM konfigurierbar. Mehr Inforamtionen finden Sie in der Online-Hilfe des WBM.

- Event-Protokoll im **T**rue **F**lash **F**ile **S**ystem (TFFS) über WBM abholen / löschen

  Wartung -> Events -> Event-Protokoll -> Laden über HTTP

  Wartung -> **Events** -> **Even-Protokoll** -> **Event-Protokoll löschen**
- Trace-Protokoll im **T**rue **F**lash **F**ile **S**ystem (TFFS) über WBM abholen / löschen

  Wartung -> **Traces** -> **Trace-Protokoll** -> **Laden über HTTP**

  Wartung -> **Traces** -> **Trace-Protokoll** -> **Trace-Protokoll löschen**
- Kunden-Trace-Protokoll im **T**rue **F**lash **F**ile **S**ystem (TFFS) über WBM abholen / löschen

  Wartung -> **Traces** -> **Kunden-Trace-Protokoll** -> **Laden über HTTP**

  Wartung -> **Traces** -> **Kunden-Trace-Protokoll** -> **Trace-Protokoll löschen**
- V24 Trace / Consoletrace
- LAN Trace für XTracer Client
- Service Center
- Bei einem Absturz muss das DDC log über WBM abgeholt werden
- Belegte Ressourcen abfragen

2.24 Gateways HG 3500 und HG 3575 - Ändern von Gateway UI MODUS

IP-Gateways-Zugriff kann mithilfe von Parameter `UIMODE`, gesichert werden, auf die in `AMO CGWB` und `STMIB` oder über Assistant (**Zugriffsmanagement -> Sicherheitsmodus-Konfiguration**) zugegriffen werden kann.

UIMODE:

1) CLASSIC

Wenn sich die Platine im Modus CLASSIC befindet, können Sie über die Gateway Manager-Seite schnell auf die Schaltflächen SSH, WBM und SFTP (Fernzugriff) zugreifen. Sie können auch Browser oder SSH-Clients wie Putty und WinSCP verwenden, um direkt auf die Gateways zuzugreifen. Weitere Vorgänge, die Sie im CLASSIC-Modus durchführen können, enthalten Backup & Restore, OS-Upgrades, Loadware-Upgrades, Plattform-HF-Upgrades, Bootstrapping (DLS SPE), SNMP und mehr.

Es gibt **keine Filterung** basierend auf der Ursprungs-/Quelladresse des HTTPS- und SSH-Clients.

2) MAINTAIN

Wenn die Funktion der Platine vom Modus CLASSIC in den Modus MAINTAIN geändert wird, können dieselben Vorgänge, die im Modus

CLASSIC durchgeführt werden können, auch im Assistant Gateway Manager durchgeführt werden.

Anmerkung: Im MAINTAIN-Modus ist **direkter** Zugriff von Browsern und SSH-Clients wie Putty, WinSCP nicht mehr möglich, sondern nur noch über Assistant Gateway Manager.

Der Unterschied zwischen Modus **CLASSIC** und **MAINTAIN** in Gateway Manager besteht darin, dass ein Schloss im Menü neben der Platine erscheint (siehe Abbildung 44: Gateway Manager – Vorhängeschloss-Symbol nach Aktivierung des MAINTAIN-Modus auf Seite 283) und durch Klicken auf das Schloss von **MAINTAIN** können Sie die Platine auf **SECURE**umschalten.

3) **HOHE SICHERHEIT**

Wenn die Platine den Modus **SECURE** aktiviert hat, kann nicht einmal Gateway Manager auf die HTTPS- oder SSH-Funktionen zugreifen. Die Fernzugriffstasten im Gateway Manager sind nicht mehr verfügbar, und es gibt keinen Zugriff mehr auf die im Modus **CLASSIC/MAINTAIN** dargestellten Vorgänge (Backup & Restore, OS-Upgrade, LW-Upgrade, Plattform-HF-Upgrade usw.) (siehe Abbildung 45: Gateway Manager – Vorhängeschloss-Symbol nach Aktivierung des SECURE-Modus auf Seite 284).

Wichtig:

Die aktuelle Konfiguration `UIMODE` einer beliebigen Platine wird während des Updates nicht geändert.
Ab V11 wird der Standard-UIMODE von “**CLASSIC**” auf “**MAINTAIN**” gewechselt.

Sie können eine Platine von **CLASSIC UIMODE** auf **MAINTAIN UIMODE** von`CGWB -> MTYPE (CGW) -> MGNTDATA -> UIMODE -> MAINTAIN`wechseln.

Assistant – GW Manager:

Ein Gateway in Modus **MAINTAIN/SECURE** wird als ein Vorhängeschloss-Symbol angezeigt (nachdem die Platine aktualisiert wurde):

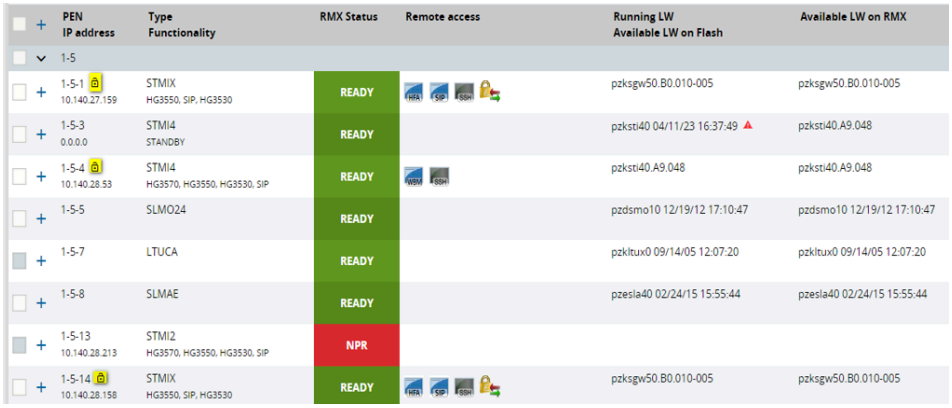
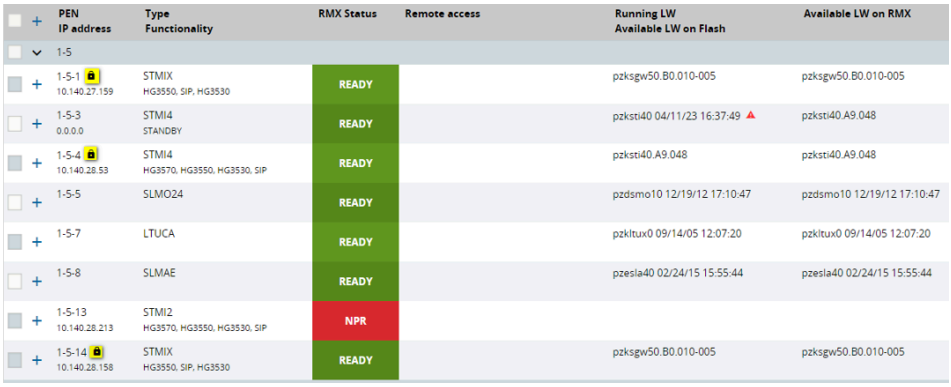


Abbildung 44: Gateway Manager – Vorhängeschloss-Symbol nach Aktivierung des MAINTAIN-Modus



PEN IP address	Type Functionality	RMX Status	Remote access	Running LW Available LW on Flash	Available LW on RMX
1-5					
1-5-1 10.140.27.159	STMIX HG3550, SIP, HG3530	READY		pzksgw50.B0.010-005	pzksgw50.B0.010-005
1-5-3 0.0.0.0	STMI4 STANDBY	READY		pzksti40 04/11/23 16:37:49	pzksti40.A9.048
1-5-4 10.140.28.53	STMI4 HG3570, HG3550, HG3530, SIP	READY		pzksti40.A9.048	pzksti40.A9.048
1-5-5	SLMO24	READY		pzdsmo10 12/19/12 17:10:47	pzdsmo10 12/19/12 17:10:47
1-5-7	LTUCA	READY		pzkltux0 09/14/05 12:07:20	pzkltux0 09/14/05 12:07:20
1-5-8	SLMAE	READY		pzesla40 02/24/15 15:55:44	pzesla40 02/24/15 15:55:44
1-5-13 10.140.28.213	STMI2 HG3570, HG3550, HG3530, SIP	NPR			
1-5-14 10.140.28.158	STMIX HG3550, SIP, HG3530	READY		pzksgw50.B0.010-005	pzksgw50.B0.010-005

Abbildung 45: Gateway Manager – Vorhängeschloss-Symbol nach Aktivierung des SECURE-Modus

2.25 FAQ - Häufig gestellte Fragen

1) **Frage**: Werden HG 3500-Gateways in der Hicom 300 H unterstützt?

   Antwort: Nein. Um HG 3500 Gateways nutzen zu können, müssen Kunden auf HiPath 4000 V4 oder höher hochrüsten.

2) **Frage**: Warum wird für die HG 3500 eine statische IP-Adresse benötigt?

   Antwort: Vom IP-Netzwerk her gesehen, handelt es sich bei der HG 3500 um ein Gateway bzw. einen Sprach-Router. Gateways/Router benötigen grundsätzlich eine statische IP-Adresse. Auf diese Weise wird gewährleistet, dass IP-Geräte jederzeit das zugehörige Gateway bzw. den Router finden, ohne immer wieder neu programmiert werden zu müssen. Die Verwendung von dynamischen IP-Adressen bei Gateways/Routern ist vom praktischen Standpunkt her nicht sinnvoll.

3) **Frage**: Wird die HG 3500 an IPDA Access Points unterstützt?

   Antwort: Ja. HG 3500 wird an IPDA Access Points unterstützt. Übermäßige Verzögerungen infolge mehrmaliger TDM-IP-Umwandlung bei Verbindungen zwischen IP-Benutzern an verschiedenen IPDA Access Points bzw. am Host werden mit Hilfe von DMCs eliminiert.

4) **Frage:** Warum unterstützen die HG 3500 und HG 3575 kein DHCP?

   Antwort: Betrachten Sie die HG 3500/3575 als Sprach-Router. Diese Sprach-Router müssen immer alle verfügbar sein und müssen sich gegenseitig kennen. Wie bei den Ports von IP-Routern ist es zweckmäßig, mit festen IP Adressen zu arbeiten. Für die Gesamtverfügbarkeit des Systems ist es zudem vorteilhaft, Abhängigkeiten zu DHCP und/oder DNS Servern zu vermeiden.

5) **Frage**: Warum unterstützt die HG 3500 den Codec G.722 nicht?

   Antwort: Hierfür besteht keine Notwendigkeit, weil auf der TDM-Seite keine Breitband-Qualität vorhanden ist. G.722 findet bei Verbindungen zwischen IP-Clients Anwendung, wobei der jeweilige Codec von den Clients ausgehandelt wird. Die HG 3500 gibt die Signalisierungsdaten zwischen IP-Clients weiter, die G.722 unterstützen, und sorgt so für eine hohe Sprachqualität.

6) **Frage:** Warum ist der Default-Wert für den Jitterbuffer auf HG 3500/75 auf 60 Millisekunden eingestellt? Kann ich gefahrlos auch geringere Werte einstellen?

Anwort: Die Default-Einstellung soll einen relativ problemlosen Ersthochlauf gewährleisten. 60 ms sind sicherlich zu viel für moderne Campus-LAN-Installationen, die ausschließlich Geräteanschlüsse an Layer 2 Switch Ports nutzen und hinreichend Bandbreitereserven haben. Hier hat sich eine Jitter-Buffer-Tiefe von 20 ms bewährt. Andererseits sind 60 ms manchmal auch zu wenig für Installationen über WAN-Links mit extrem geringer Bandbreite und ohne Reserve. Eine zu großzügige Einstellung der Jitter-Buffer-Tiefe führt zu unnötig hoher Sprachverzögerung. Eine zu knappe Einstellung führt zu schlechter Übertragungsqualität auf Grund hoher Paketverlustrate.

7) **Frage:** Der maximal einstellbare Wert für den Jitter-Buffer liegt bei 210 ms. Ich unterstelle, dass das System mit dieser Einstellung gut funktioniert. Kann ich diesen Wert als Anforderung für die Ausschreibung meines WAN an die Carrier geben?

Anwort: Das System hat mit 210 ms Jitter-Buffer keinerlei Probleme. Mit dieser Einstellung wird ein extrem hoher Jitter von bis zu 210 ms ausgeglichen, ohne dass es zu Störungen in der Sprachverständlichkeit kommt. Es muss aber auch berücksichtigt werden, dass die Größe des Jitter-Buffer unmittelbaren Einfluss auf die Sprachverzögerung hat. Siehe auch Abschnitt 1.4, „Sprachqualität“. Auf die Sprachverzögerung (Mouth-to-Ear-Delay) haben 5 Komponenten Einfluss:

- Paketgröße / Sample Size / wieviele Millisekunden Audio pro Paket
- Verarbeitungszeit auf der Empfängerseite
- Übertragungszeit im LAN/WAN
- Jitter-Buffer
- Verarbeitungszeit auf der Empfängerseite

Bild 3 „Sprachqualität in Abhängigkeit vom Delay“ zeigt die Zufriedenheit der Anwender in Abhängigkeit vom Mouth-to-Ear-Delay. Ab etwa 150 ms nimmt die Zufriedenheit der Anwender stark ab. Ab 250 ms fühlen sich Anwender bereits gestört und sind unzufrieden.

Hierbei muss berücksichtigt werden, dass bei Amtsgesprächen auf der „anderen Seite“ der Amtsleitung eine ähnliche Installation ebenfalls Delay verursachen kann, d.h. je Seite nur die Hälfte des tolerierbaren Delays je Seite verursacht werden darf.

Die folgende Tabelle zeigt ein paar Berechnungsbeispiele (alle Werte in ms)

Sample-Größe	20	60	20	20	60	60	60	20
Übertragungszeit im LAN/ WAN	10	10	10	40	40	40	60	0
Verarbeitungszeit Sende+Empfangsrichtung	32	32	32	32	32	32	32	32
Jitter-Buffer	20	20	60	60	60	120	**210**	**210**

Mouth to Ear Delay	82	122	122	152	192	252	**362**	**262**

Mit 210 ms Jitter-Buffer können keine Verzögerungen unter 262 ms erreicht werden.

8) **Frage:** Sowohl die HG 3500, als auch die HG 3575 haben eine fix der Baugruppe zugeordnete MAC-Adresse des Ethernet-Ports. Die IP-Adressen werden jedoch aus der System-Datenbasis an Hand der „Lage“ der Baugruppe zugeordnet. Tausche ich z.B. eine HG 3500 auf einem bestimmten Steckplatz gegen eine andere Baugruppe des gleichen Typs, so bleibt aus Sicht des IP-Netzes die IP-Adresse erhalten. Die MAC-Adresse, unter der letztlich die Pakete zugestellt werden, ändert sich aber. Führt das nicht dazu, dass die neue Baugruppe wegen der geänderten MAC-Adresse solange nicht erreichbar ist, bis in den IP-Stacks der Kommunikatonspartner die ARP-Einträge durch *Aging* herausfallen?

Antwort: Für dieses prinzipielle Problem mit der Address Resolution gibt es eine Standard-Lösung, die auch auf den Gateways HG 3500 und HG 3575 implementiert ist. Nach Aktivierung der IP-Schnittstelle schickt das Gateway einen ARP-Request auf die eigene IP-Adresse „Gratituous-ARP“. Dadurch lernen alle IP-Geräte am LAN-Segment die neue Zuordnung IP-<-> MAC-Adresse.

9) **Frage:** In einer Kundeninstallation haben wir immer wieder Probleme mit Statistik-Overflow. Einzelne HG 3500/75 Baugruppen werden kurzzeitig vorübergehend außer Betrieb genommen. Das löst alle Gespräche über diese Baugruppen aus und bringt sonst keinen sichtbaren Effekt. Was ist die Ursache, was kann man dagegen tun?

Antwort: Für die HG 3500/75 wird wie für andere Baugruppen auch eine statistische Bewertung von Fehlermeldungen durchgeführt. Dies umfasst unter anderem auch den Verlust der Signalisierungsverbindung bei der HG 3575 und „Bad Quality“ Meldungen für die Payload-Verbindungen der HG 3500/75.

Nachhaltig schlechte Qualität der IP-Verbindungen zwischen den HG 3500/75 Gateways bzw. der OpenScape 4000 Zentrale und den HG 3575 kann zu einer hohen Zahl von Fehlermeldungen in einem kurzen Zeitraum führen, was letztlich zum Statistik-Overflow und zum Rücksetzen der Baugruppen führt.

Durch das Rücksetzen der Baugruppe soll ausgeschlossen werden, dass ein temporärer Fehler auf der Baugruppe zu dem Problem führt.

Liegt der Fehler eindeutig im Netz, so kann durch Rücksetzen der Baugruppe keinerlei Verbesserung herbeigeführt werden.

Sie haben die Möglichkeit mittels AMO PSTAT die Schwellwerte der Zähler für STMI und NCUI über den Standardwert hinaus zu erhöhen, oder die statistische Bewertung durch Setzen der Schwellwerte auf Null ganz abzuschalten.

```
AENDERN-
PSTAT:TYP=CTRLTAB,EBENE=BOARD,BOARD=NCUI,STUFE=1 bzw. 2,
MAXCOUNT=xxx;
```

Wichtig ist es, sowohl die Stufe 1 (`COUNT1`, zählt „sogenannte Pärchen von In- und Außerbetriebnahmemeldungen“) als auch die Stufe 2 (`COUNT2`,

zählt „Meldungen die sich als „Meldungsfluten“ entpuppen können“) zu betrachten.

Für NCUI/STMI und NCUI2/STMI2 werden separate Zähler verwendet

```
+----------+--------+----------+----------+----------
+----------+----------+
! NCUI     ! COUNT1 !   BYTE1  !      61  !      10  !
      2  !       4  !
! STMI     +--------+----------+----------+----------
+----------+----------+
!          ! COUNT2 !   BYTE2  !      61  !       6  !
      2  !       2  !
!          +--------+----------+----------+----------
+----------+----------+
!          ! COUNT3 !   BYTE3  !      21  !      10  !
      2  !       4  !
!          +--------+----------+----------+----------
+----------+----------+
!          ! COUNT4 !   BYTE4  !      19  !      10  !
      2  !       4  !
+----------+--------+----------+----------+----------
+----------+----------+
! NCUI2    ! COUNT1 !   BYTE1  !     241  !      10  !
      2  !       4  !
! STMI2    +--------+----------+----------+----------
+----------+----------+
!          ! COUNT2 !   BYTE2  !     241  !       6  !
      2  !       2  !
!          +--------+----------+----------+----------
+----------+----------+
!          ! COUNT3 !   BYTE3  !      21  !      10  !
      2  !       4  !
!          +--------+----------+----------+----------
+----------+----------+
!          ! COUNT4 !   BYTE4  !      19  !      10  !
      2  !       4  !
+----------+--------+----------+----------+----------
+----------+----------+
```

Details zum AMO PSTAT finden Sie in der AMO-Beschreibung im OpenScape 4000 Servicehandbuch.

Die Modifikation der Statistik verhindert dann das Rücksetzen der Baugruppen auf Grund von Qualitätsproblemen im IP-Netz, welche Einfluss auf die Gesamtfunktion der Anlage haben. Das Ziel muss sein, diese Probleme in Griff zu kriegen!

10) **Frage:** Wo kann ich hören, wie sich Packet Loss Concealment bei G.711 bzw. G.729 Codec auswirkt?

Der Vorschlag, Hörbeispiele in die elektronische Version des Handbuch einzubinden wurde von Service und Vertrieb abgelehnt, da diese Information für Service-Techniker und Vertriebsbeauftragte nicht relevant ist. Sorry

11) **Frage :** Was ist der Unterschied zwischen **TOSLAN**, **TOSSIGNL** und **TOSPL**?

AMO SIPCO	
TOSSIGNL	QoS-Wert für den TCP-Stream von HSR > NCUIs
TOSPL	QoS-Wert für den abgehenden Payload-Stream von IPDA-STMI (OpenScape 4000 Host-System)
AMO STMIB	
TOSLAN	QoS-Wert für den TCP-Stream von NCUI > HSR
TOSPL	QoS-Wert für den abgehenden Payload-Stream NCUI
AMO CGWB	
TOSSIGNL	QoS-Wert für den TCP-Stream von STMI > STMI (IP-Trunking) oder STMI > IP-Telefon
TOSPL	QoS-Wert für den abgehenden Payload-Stream von STMI (HFA/IP-Trunking)

Anmerkung:

Wenn MFS mit IPDA-Funktionalität verwendet wird, müssen die TOSPL (AMO SIPCO & AMO CWGB) identisch sein.

Die TOS-Werte für die vom IP-Telefon gesendeten Pakete können nur im IP-Telefon selbst festgelegt werden.

3 OpenScape 4000 SoftGate

3.1 Überblick

3.1.1 Funktionsüberblick

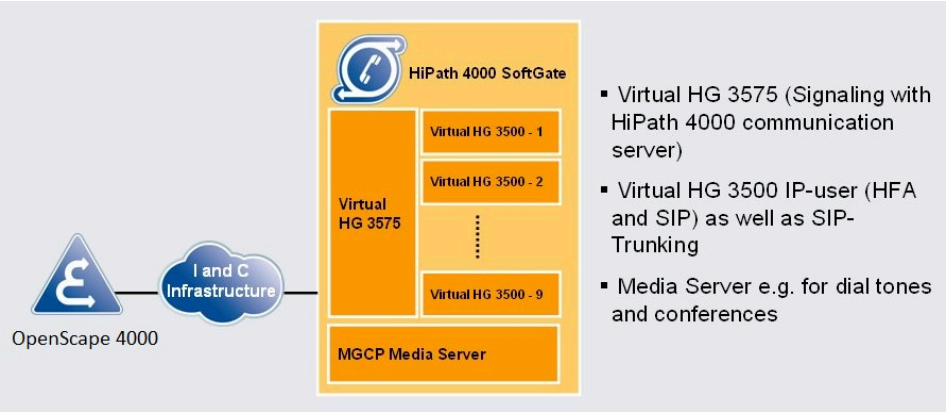


Abbildung 46: Topologie

Das OpenScape 4000 SoftGate ermöglicht kostengünstige Zweigstellen mit zuverlässigen OpenScape 4000 Survivability-Optionen in ein Netzwerk einzubinden sowie eine einfache IT-Integration in die OpenScape 4000 Lösungs- und Management-Suite. Diese Softwareanwendung bietet vollen HiPath Feature Access (HFA) für IP-Endpunkte, Verbindung zu SIP-Service-Providern sowie „Native SIP“-Konnektivität für Trunking und Teilnehmer, das auf einem x86-Standardserver mit Linux basiert.

Ein OpenScape 4000 SoftGate-Standort integriert sich hinsichtlich Leistungsmerkmalen und Administration nahtlos wie ein IPDA Access Point (AP 3700 IP) in das Kommunikationssystem und -netzwerk.

Mit dieser Anwendung können Kunden Investitionskosten (CAPEX) und Betriebskosten (OPEX) reduzieren und zentralisierte Anwendungen mit einheitlichem Benutzererlebnis bereitstellen.

3.1.2 Varianten

Mit OpenScape 4000 V8 ist nur eine SoftGate Application-Bestellnummer verfügbar.

Die älteren SoftGate-Varianten OpenScape 4000 SoftGate können weiterhin im System gesehen und konfiguriert werden, z. B. beim Upgrade von V7 auf V8:

– OpenScape 4000 SoftGate 50 Bis zu 50 Ports für IP-Teilnehmer (HFA- und SIP-Teilnehmer) oder SIP-Trunking (Native SIP/SIP-Q).

– OpenScape 4000 SoftGate 500 Bis zu 500 Ports für IP-Teilnehmer (HFA- und SIP-Teilnehmer) oder SIP-Trunking (Native SIP/SIP-Q).

- OpenScape 4000 SoftGate 1000 Bis zu 1000 Ports für IP-Teilnehmer (HFA- und SIP-Teilnehmer) oder SIP-Trunking (Natives SIP/SIP-Q)/maximale Anzahl von 256 aktiven Ports.

Mit OpenScape 4000 V8 R2 ist es möglich, eine SoftGate-Instanz auf einem laufenden Enterprise Gateway oder Survivable Enterprise Gateway zu konfigurieren und zu starten. Dieses zusätzliche SoftGate heißt „Integriertes SoftGate“ oder kurz „iSoftGate“, läuft in einem Linux-Container und wirkt und unterstützt die meisten Funktionen wie jedes eigenständige SoftGate.

3.1.3 Leistungsmerkmale

Folgende Leistungsmerkmale kennzeichnen das OpenScape 4000 SoftGate:

- Läuft auf Standard-Server-Hardware.
- Betrieb mit Standard-Betriebssystem Suse Linux Enterprise Server (SLES).
- Integrierter Media Server.
- Administration über OpenScape 4000 Assistant/Manager.
- Integration in OpenScape 4000 Netze.
- Unterstützt alle Funktionen von IP Distributed Architecture (IPDA) (siehe Kapitel 1, „Leistungsmerkmalbeschreibung IPDA“).
  - Unterstützung der IPDA Survivability Optionen: Signaling Survivability und Verbindung zu existierenden AP-Emergency Server.
  - Unterstützt a-/µ-Law-Konvertierung pro OpenScape 4000 SoftGate. Mehr Information zu a-/µ-Law-Konvertierung finden Sie im Servicehandbuch **„OpenScape 4000, Band 4- IP-Lösungen > IP Distributed Architecture“**.
- Die folgenden Ressourcen stehen an jedem OpenScape 4000 SoftGate zur Verfügung:
  - 64 TSLs für Konferenz
  - 32 Empfänger für DTMF-Signalisierung (CR)
  - 32 Sender für DTMF-Signalisierung (CS)
  - 2 Dauerton Wähltonempfänger (DTR-DT)
  - 2 Wähltonempfänger für rhytmische Töne (DTR-TT)
  - 2 Test-Empfänger (TESTR)
  - 1 Test-Sender (TESTS)
  - bis zu 18 verschiedene Töne, 6 verschiedene Ansagen (für eine detaillierte Beschreibung siehe **IP Distributed Architecture >** Abschnitt 2.16, „Verschiedene Ansagen, Töne und DTMF DialTone Empfänger pro Access Point“)
  - 5 verschiedene Display-Sprachen/nationale Zeichensätze unterschiedlich zum Host System und/oder unterschiedlich für jedes OpenScape 4000 SoftGate (für eine detaillierte Beschreibung siehe **IP Distributed Architecture >** Abschnitt 2.17, „Verschiedene Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point“)
  - 1 Wartemusik
  - 1 TDS Port
- Maximale Anzahl der parallelen Sprachkanäle: 250
- Unterstützt DMC - Das OpenScape 4000 SoftGate ist DMC-Endpunkt (siehe „Payload Switching DMC, Kapitel 4, „Direct Media Connect (DMC) in Verbindung mit OpenScape 4000 SoftGate“).
- Unterstützt T.38 Fax (siehe T.38 Fax).

- Unterstützt Signalisierungs- und Sprachverschlüsselung
- Mehr Informationen zum Leistungsmerkmal „Signalisierungs- und Sprachverschlüsselung (SPE)“ finden Sie im entsprechenden Abschnitt.
- Unterstützt ISDN Anrufe ins öffentliche Netz. PSTN-Verbindung über Mediatrix SIP Gateways.
- Analog- und Fax-Verbindung:
  - über AP 3700 beim Einsatz von OpenScape 4000 SoftGate 1000.
  - über Mediatrix 41xx SIP-Gateway beim Einsatz von OpenScape 4000 SoftGate 50 (siehe Abschnitt 3.3.5, „Analoge Teilnehmer (Mediatrix 41xx)“).
- S0-Verbindung über Mediatrix 44xx SIP Gateways:
  - S0-Teilnehmer: Abschnitt 3.3.1, „ISDN (S0) Teilnehmer (Mediatrix 44xx)“
  - S0-Trunking: Abschnitt 3.3.2, „S0-Trunking (Mediatrix 44xx)“
  - S0-Daten-Verbindungen: Abschnitt 3.3.3, „ISDN (S0) Daten-Verbindungen (Mediatrix 44xx)“
- Mediatrix 35xx für PRI-Schnittstelle T1.
- Mediatrix 36xx für PRI-Schnittstelle (siehe Abschnitt 3.3.4, „S2-Schnittstelle (Mediatrix 36xx)“ für E1.
- Mediatrix 1204 für anaolges Trunking (siehe Abschnitt 3.3.6, „Analog Trunking (Mediatrix 1204)“).
- Videointegration mit Lifesize Endgeräten (siehe Kapitel 5, „Videoverbindungen“).
- Unterstützung von native SIP- und SIP-Q-Trunking.
- IPv6 für SIP-Q und native SIP Trunking mit OpenScape 4000 SoftGate (siehe Kapitel 12, „IPv6“).
- End-to-end Payload-Verbindungen zwischen native SIP-Trunks und SIP-Teilnehmern.
- Native SIP Trunking Erweiterungen:
  - konfigurierbare Voice Codecs im HG 3500 pro Zielgateway oder IP Subnetzwerk
  - Native SIP Trunking Leistungsmerkmale: Briefkastenlampe, Anrufübergabe, Namensanzeige und Anrufumleitung
- SIP Service Provider-Verbindungen sind möglich.

  Anmerkung: Die Auslegung von Firewall und SBC (Session Border Control) sind von Kundennetz und NAT (Network Address Translation) abhängig.

- HiPath Cordless IP V1 ist zur Anschaltung an das OpenScape 4000 SoftGate freigegeben (siehe).
- Für eine erhöhte Ausfallsicherheit kann das OpenScape 4000 SoftGate über zwei LAN-Kabel an zwei verschiedene Switches/Router angeschlossen werden (siehe Kapitel 6, „LAN-Redundanz“).
- Gatekeeperredundanz für HFA-Teilnehmer (siehe Kapitel 10, „Gatekeeper-Redundanz für HFA/SIP-Teilnehmer“).
- Survivable OpenScape 4000 SoftGate (siehe Kapitel 11, „Survivable OpenScape 4000 SoftGate“).
- SIP Load Balancing für ankommende native SIP-Verbindungen. Damit wird die Leistung der beteiligten SIP-Server skaliert, eine Überlastung der Server vermieden und eine hohe Verfügbarkeit der SIP-Dienste erreicht (siehe Kapitel 13, „Load Balancing“).

- An das OpenScape 4000 SoftGate können direkt OpenScape Access Module angeschlossen werden. Für Informationen über Lizenzen siehe OpenScape Access Servicedokumentation.
- Mit der Einführung von OpenScape Access kann sich die vNCUI nun auch als secure DMC-Endpunkt verhalten.
- QDC wird unterstützt.
- OpenScape Cordless E Integration (siehe Kapitel 17, „OpenScape Cordless E-Integration“).
- MFC-R2-Unterstützung (siehe Kapitel 16, „MFC-R2“)
- 16 periphere Einbauteilungen für virtuelle Baugruppen und OpenScape Access Module

  Jede virtuelle Baugruppe in einem OpenScape 4000 SoftGate benötigt eine Einbauteilung. Auf Grund der Erhöhung der Anzahl der Einbauteilungen, verbraucht die Installation von virtuellen Baugruppe bei OpenScape Access und OpenScape 4000 SoftGate keine Hardware-Einbauteilungen mehr.

  Beim tracen muss darauf geachtet werden, dass die Zuordnung von Einbauteilung und PBC-Nummer stimmt (siehe Abschnitt 1.8, „Diagnosehinweise bezüglich peripherer Einbauteilungen“).

3.1.4 LAN Interfaces

Das OpenScape 4000 SoftGate bietet folgende LAN-Schnittstellen:

- IPDA LAN

  Für den Anschluss an das OpenScape 4000-Hostsystem.
- Management-LAN

  Das Leistungsmerkmal „Separate LAN-Konnektivität für Administration und VoIP“ wird unterstützt. Das Voice-LAN kann jetzt vollständig vom Management-LAN getrennt werden.
- WAN

  Das OpenScape 4000 SoftGate bietet eine WAN-Schnittstelle zum Internet.

  Ein Szenario, in dem die WAN-Schnittstelle des OpenScape 4000 SoftGate verwendet wird, finden Sie in Kapitel 14, „Secure Remote Subscriber“.
- Signaling Survivability

  Eine LAN-Schnittstelle für Signaling Survivability wird unterstützt.
- XLINK

  Die XLINK-Schnittstelle wird für OpenScape Access und RG 8350 A verwendet.

  Der einzige offizielle Weg LAN-Schnittstellen zu konfigurieren/ rekonfigurieren ist die firstinstall XML Datei zu verwenden. Diese beinhaltet Bitraten-, Bond-, VLAN- und IP-Konfiguration. Die XML-Datei wird während der Erst-Installation oder wenn das Recovery Tool aufgerufen wird verwendet. Für weitere Details siehe Dokumentation „OpenScape 4000 V8, Installation, Konfiguration und Migration, Installationsanleitung“.

Anmerkung: Sollten für einzelne vSTMI-Karten des SoftGate verschiedene VLANs erforderlich sein, muss die SoftGate-LAN-Schnittstelle als eth<n> oder bond<n> ausgewählt sein. Anschließend muss unter der AMO-

Schnittstelle ein entsprechendes LAN-Schnittstellen-Tagging konfiguriert werden. Die SoftGate-LAN-Schnittstelle kann entweder über das Portal (SoftGate-LAN-Assistent) oder über die XML-Konfiguration ausgewählt werden. Wenn der gesamte Datenverkehr von SoftGate innerhalb desselben VLANs verwendet werden soll, kann auch vlan<n> als SoftGate-Schnittstelle ausgewählt werden. Für diesen zweiten Anwendungsfall ist keine AMO-VLAN-Konfiguration erforderlich. Voraussetzung ist jedoch, dass das VLAN als Schnittstelle in der XML-Installationsdatei angegeben sein muss.

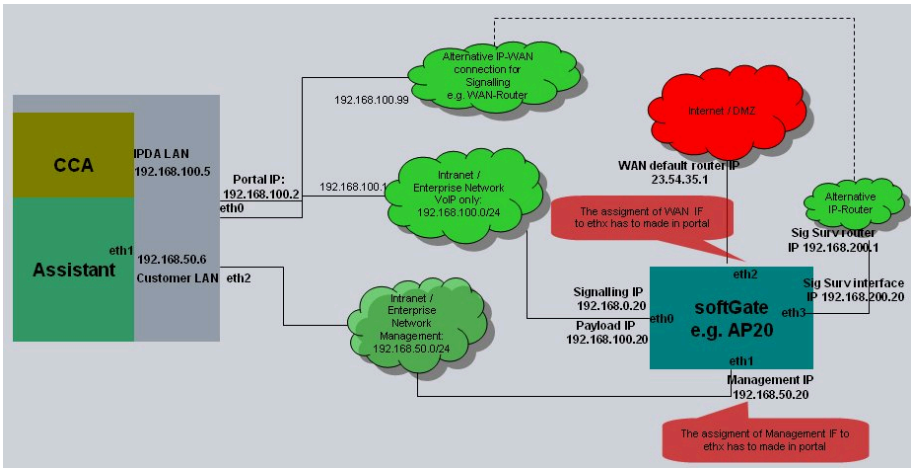


Abbildung 47: LAN-Schnittstellen des OpenScape 4000 SoftGate

3.1.5 Ports

siehe „Gateways HG 3500 und HG 3575 > Kapitel 21, „IP-Ports““.

3.1.6 Vorteile

Nutzen von OpenScape 4000 SoftGate im Vergleich mit bestehenden Zweigstellenszenarien:

Tabelle 16: OpenScape 4000 SoftGate Vorteile im vergleichmit bestehenden Zweigstellenszenarien

Bestehende Zweigstellenszenarien	OpenScape 4000 SoftGate Vorteile
Entfernte IP-Endpunkte	• Lokaler Festnetzanschluss, lokale a/b-Verbindung • Signaling Survivability (Hot-Standby) • Geringere WAN-Bandbreite zwischen Zentrale und Zweigstelle

Bestehende Zweigstellenszenarien	OpenScape 4000 SoftGate Vorteile
Kleiner entfernter Standort mit HiPath 2000 oder HiPath 3000	• Zentralisierte-Switch-Architektur • Homogene Verwaltung mit OpenScape 4000 Administration • Homogene Anwendungen • Geringere WAN-Bandbreite zwischen Zentrale und Zweigstelle
IPDA Access Point	• Keine proprietäre Hardware • Niedrigere TCO • Video-Endpunkte

3.1.7 Einschränkungen

Für alle Varianten des OpenScape 4000 SoftGate:

- Für Signaling Survivability sind nur die ISDN-Modems freigegeben, die auch für OpenScape 4000 unterstützt werden.
- Analoge Modemverbindungen werden nicht unterstützt.
- Codec G.723 wird nicht unterstützt.
- Die folgenden Einschränkungen gelten bei Verbindungen zum Amt über Mediatrix-Gateways:
  - Gebührenerfassung (Accounting) wird nicht unterstützt.
  - Rückruf-Funktionalität wird nicht unterstützt.
- Höchstens 83 OpenScape 4000 SoftGates 50/1000 oder IP Access Points können an einem OpenScape 4000 System angeschlossen werden.
- Einschränkungen für DMC (siehe „Payload Switching DMC“, Kapitel 4, „Direct Media Connect (DMC) in Verbindung mit OpenScape 4000 SoftGate“):
  - Auch zu einem native SIP Trunk kann End-to-End Payload erreicht werden (abhängig vom Trunk-Profil).
  - Zwischen SIP-Partnern (am OpenScape 4000 SoftGate) können die MediaCapabilities (z.B. Codecs) auch nach dem Aufbau der DMC-Verbindung nachverhandelt / geändert werden.
  - Kommuniziert ein SIP-Device oder SIP native Trunk am OpenScape 4000 SoftGate mit einem DMC-Endpunkt (nicht DMC-Proxy!), dann wird immer ein MediaRelay am OpenScape 4000 SoftGate dazwischen geschaltet. Dies entspricht einem RTP-Proxy der den Media-Stream (RTP) immer über das OpenScape 4000 SoftGate leitet.
  - Kommuniziert ein SIP-Device oder SIP native Trunk am OpenScape 4000 SoftGate mit einem DMC-Proxy am Common Gateway, dann werden die MediaCapabilities transparent weitergereicht und es entsteht eine End-to-End-Payloadverbindung. Allerdings kann aufgrund der Einschränkung des DMC-Proxies am CGW keine Codec-Nachverhandlung stattfinden.

Nur für OpenScape 4000 SoftGate 50:

- Provider-Zugang benötigt OpenScape Access Module oder direkte SIP-Provider-Verbindungen.

Nur für OpenScape 4000 SoftGate 1000:

- Signaling Survivability über das öffentliche Amt wird für OpenScape 4000 SoftGate 1000 nicht unterstützt.
- Provider-Zugang benötigt AP 3700 IP oder direkte SIP-Provider-Verbindungen.

Für integriertes SoftGate auf Enterprise Gateway:

- XLink wird nicht unterstützt.
- Datum, Uhrzeit und Zeitzone sind identisch mit dem Enterprise Gateway, auf dem das integrierte SoftGate läuft
- Signaling Survivability wird nicht unterstützt
- iSG muss den gleichen Verbindungstyp wie EntGW/SurvEntGW haben (AMO-UCSU: CONNTYPE =APNW/APDL).

3.1.8 Diagnosehinweise bezüglich peripherer Einbauteilungen

Einbauteilung und PBC-Nummern unterscheiden sich. Bitte nutzen Sie die folgenden Tabellen für ein korrekte Zuordnung.

Slot	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
PBC	1	2	3	4	5	21	9	10	11	12	13	14	15	16	6	7	8
Quarter	1.				2.	---	3				4				2.		

PBC	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	21
Slot	1	2	3	4	5	15	16	17	9	10	11	12	13	14	15	16	6
Quarter	1.				2.				3.				4.				---

3.1.9 Hardware-Voraussetzungen

Die aktuellen Hardware-Voraussetzungen für einen OpenScape 4000 SoftGate Server finden Sie in der White List. Diese ist Bestandteil der aktuellen Release Note.

3.2 OpenScape 4000 SoftGate Upgrade

Im OpenScape 4000 SoftGate Image ist sowohl die Funktionalität der virtuellen HG 3575 als auch die der virtuellen HG 3500 (HFA/SIP) enthalten. Mit einem OpenScape 4000 SoftGate Upgrade werden daher immer alle Funktionalitäten gleichzeitig hochgerüstet.

Der Upgrade erfolgt entweder über den **LW Update Manager** (siehe Abschnitt 2.1, „Upgrade über Loadware Update Manager“) oder über das loakel **WBM** (siehe Abschnitt 2.2, „Upgrade über lokales WBM des OpenScape 4000 SoftGate“) der Baugruppe.

3.2.1 Upgrade über Loadware Update Manager

Das OpenScape 4000 SoftGate Image kann mit dem LW Update Manager oder wahlweise mit dem PCHI-Tool auf die RMX-Harddisk übertragen werden.

- OpenScape 4000 SoftGate Image (RPM-Format mit OMF 386 Header):

  `softgate-5.0-0.i586.rpm.abs`
- Verzeichnis auf der RMX-Harddisk:

  `:A1H1E:/APSP/LTG/LGA0/`

  unter:

  `PZKSGW50`

LW Update Manager

1) Starten Sie den File-Transfer über den Loadware Update Manager des OpenScape 4000 Assistant:

OpenScape 4000 Assistant > Expertenmodus > LW Update Manager

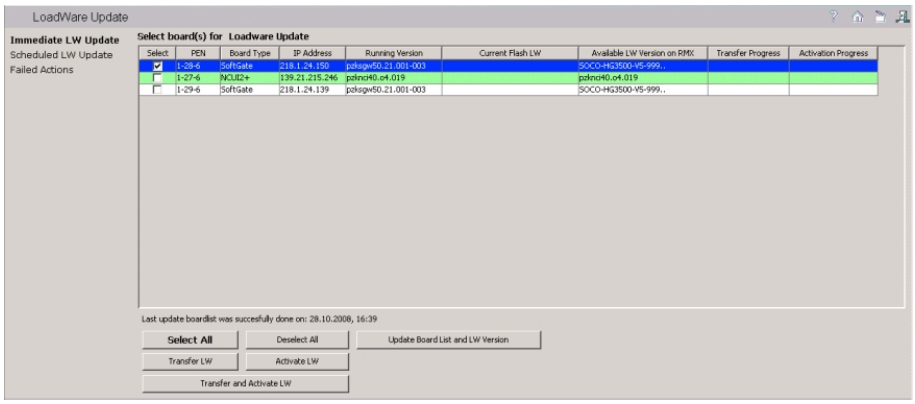


Abbildung 48: OpenScape 4000 Assistant: Loadware Update

2) Wählen Sie in der Liste das OpenScape 4000 SoftGate aus, das Sie upgraden wollen.

3) Sie haben nun folgende Möglichkeiten:

- Schaltfläche **Transfer LW**: Die Loadware wird übertragen aber nicht aktiviert. Für die Aktivierung müssen Sie im Anschluss oder später mit der Schaltfläche **Activate LW** die Loadware auf den gewünschten Baugruppen aktivieren.
- Schaltfläche **Transfer and Activate LW**: Die Loadware wird übertragen und aktiviert.

Wichtig: Bitte beachten Sie, dass beid er Aktivierung der Loadware die Baugruppe kurzzeitig ausser Betrieb genommen wird!

3.2.2 Upgrade über lokales WBM des OpenScape 4000 SoftGate

1) Lokales Web Based Management aufrufen

   Entweder über **OpenScape 4000 Assistant > Expertenmodus > Gateway Manager** oder Aufruf im Browser mit der IP-Adresse des OpenScape 4000 SoftGates, z.B. https://218.1.24.139.

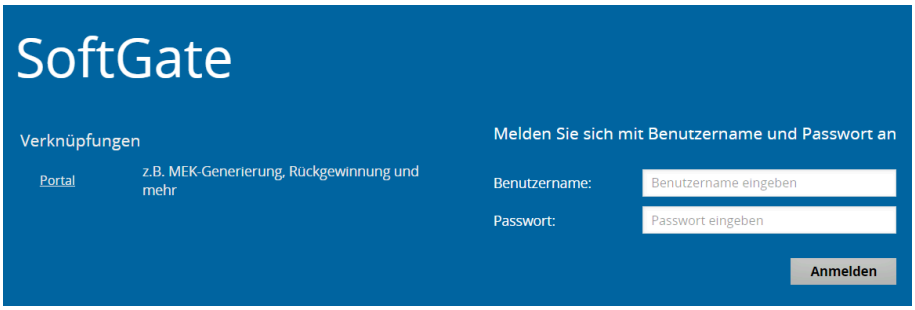


Abbildung 49: WBM - Login

2) Einloggen mit user: **TRM**, ... und entsprechendem Passwort.

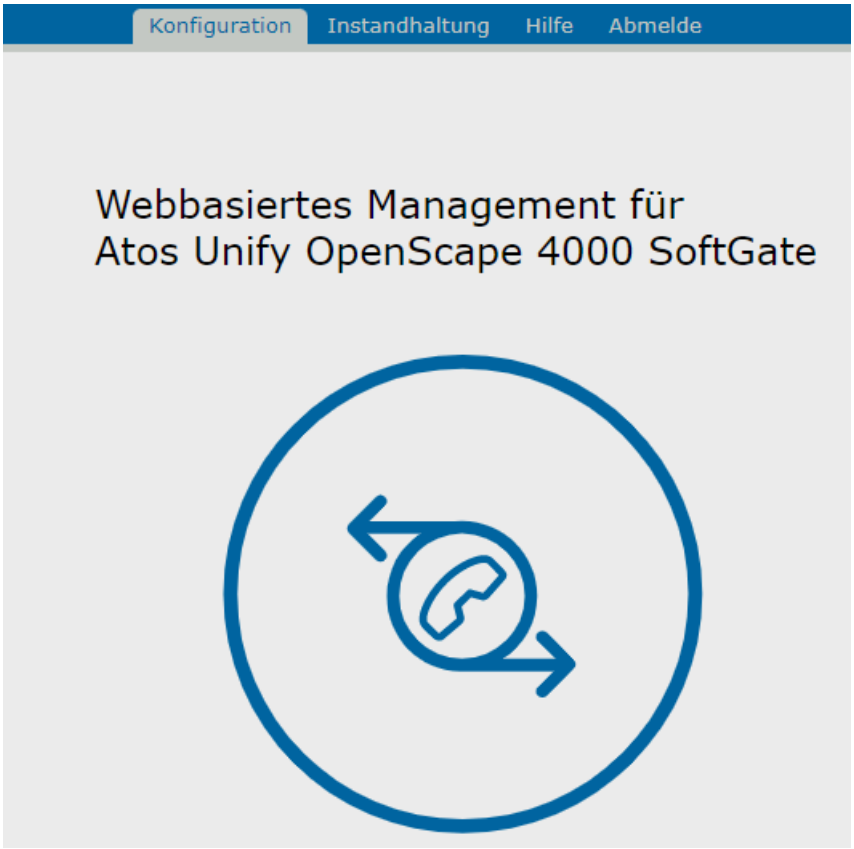


Abbildung 50: WBM - Startseite

3) Wählen Sie ds Menü **SW-Update** aus

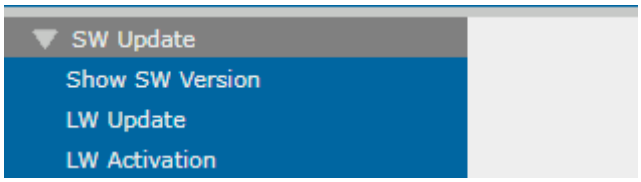


Abbildung 51: WBM - Software Update

4) Übertragen des OpenScape 4000 SoftGate Images mit OMF 386 Header:

`softgate-5.0-0.i586.rpm.abs`

Funktion **Software Update** auswählen.

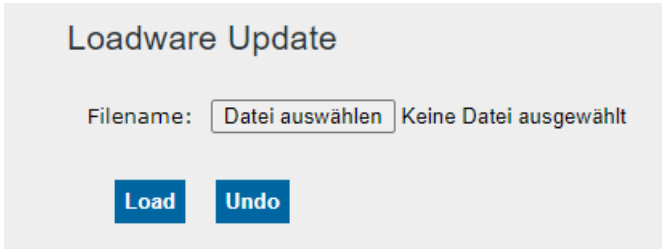


Abbildung 52: WBM - Software Update

5) Mit der Schaltfläche **Durchsuchen** das OpenScape 4000 SoftGate Image in das Feld „Filename“ eintragen.

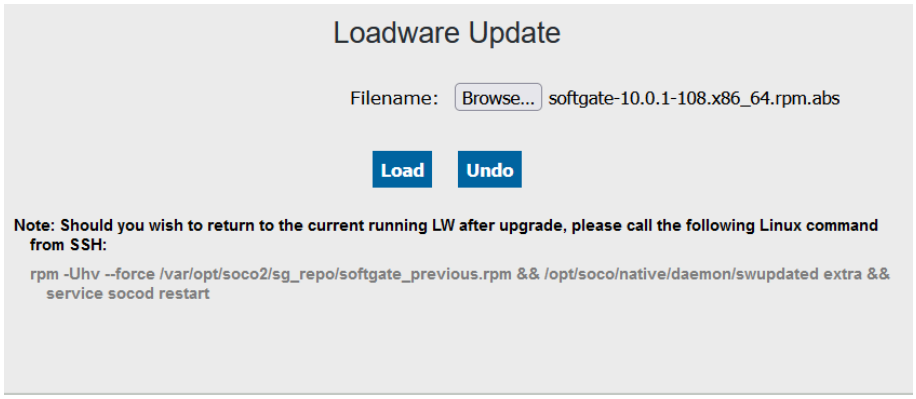


Abbildung 53: WBM - Software Update: Datei eintragen

6) Mit der Schaltfläche **Load** das OpenScape 4000 SoftGate Image laden.

7) Neue Software aktivieren.

Nachdem das Image fertig geladen wurde, erscheint die maske für die Aktivierung der neuen Software.

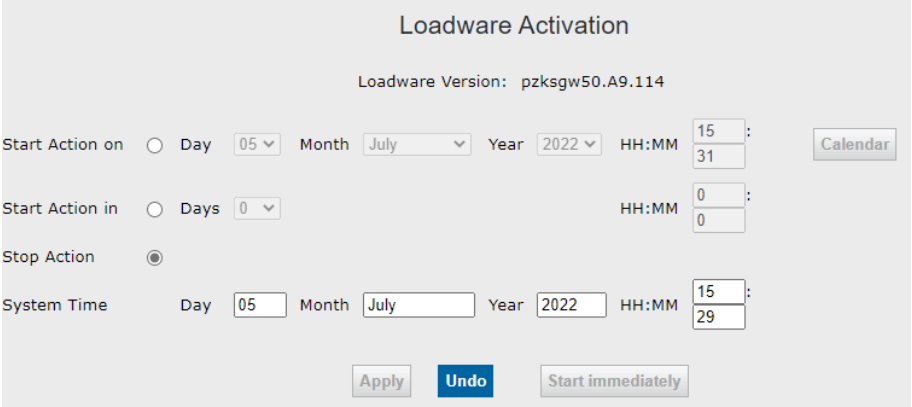


Abbildung 54: WBM - Software Activation

Sie haben nun die Möglichkeit das neue OpenScape 4000 SoftGate Image sofort zu aktivieren (mit der Schaltfläche Start Immediately) oder es auf einen späteren Zeitpunkt zu planen (Einstellungen in der Maske durchführen und mit **Apply** bestätigen).

3.3 Mediatrix Gateways

3.3.1 Freigegebene Mediatrix Gateways

- Mediatrix 4402 Advance: 2x BRI (Basic Rate Interface = ISDN S0) (native SIP Trunking)
  - Abschnitt 3.3.1, „ISDN (S0) Teilnehmer (Mediatrix 44xx)“
  - Abschnitt 3.3.2, „S0-Trunking (Mediatrix 44xx)“
  - Abschnitt 3.3.3, „ISDN (S0) Daten-Verbindungen (Mediatrix 44xx)“
- Mediatrix 4404 Advance: 4x BRI (Basic Rate Interface = ISDN S0) (native SIP Trunking)
  - Abschnitt 3.3.1, „ISDN (S0) Teilnehmer (Mediatrix 44xx)“
  - Abschnitt 3.3.2, „S0-Trunking (Mediatrix 44xx)“
  - Abschnitt 3.3.3, „ISDN (S0) Daten-Verbindungen (Mediatrix 44xx)“
- Mediatrix 35xx (2x ISDN PRI = Primary Rate Interface) für T1
- Mediatrix 3631 (1x ISDN PRI = Primary Rate Interface) für E1
  - Abschnitt 3.3.4, „S2-Schnittstelle (Mediatrix 36xx)“
- Mediatrix 3632 (2x ISDN PRI = Primary Rate Interface) für E1
  - Abschnitt 3.3.4, „S2-Schnittstelle (Mediatrix 36xx)“
- Mediatrix analog Adapter 4104, 4108, 4116, 4124 (analoge Teilnehmer)
  - Abschnitt 3.3.5, „Analoge Teilnehmer (Mediatrix 41xx)“
- Mediatrix 1204 (analog Trunking)
  - Abschnitt 3.3.6, „Analog Trunking (Mediatrix 1204)“

3.3.2 Hinweise zur Konfiguration

Wichtig: Die Ersteinrichtung der Gateways mit Konfiguration der IP-Adresse usw. ist der Dokumentation der Mediatrix-Gateways zu entnehmen. Die abgebildeten Screenshots beziehen sich auf das Web Interface der Mediatrix Gateways. Weiterführende Informationen können auch direkt von Mediatrix bezogen werden unter: http://www.mediatrix.com oder https://support.mediatrix.com/DownloadPlus/Download.asp

Wichtig: G.711 muss immer konfiguriert werden unbahängig davon, ob T.38 oder G.729 verwendet wird. Diese Einschränkung gilt für alle Mediatrix-Gateways, die direkt an ein OpenScape 4000 System oder über ein OpenScape Voice System an ein OpenScape 4000 System angeschlossen sind.

3.3.3 Konfigurationsbeispiele

Dieses Kapitel informiert anhand von Screenshots über die Konfiguration bestimmter Parameter der Mediatrix-Gateways, abgestimmt auf den jeweiligen Anwendungsfall.

3.3.3.1 ISDN (S0) Teilnehmer (Mediatrix 44xx)

Ein Mediatrix 4400 Gateway kann gleichzeitig eine ISDN-Teilnehmerleitung und eine Leitung zum öffentlichen Netz unterstützen.

3.3.3.1.1 Anforderungen

- Jeder Teilnehmer an einem Mediatrix-Gateway muss in der OpenScape 4000 als SIP-Teilnehmer eingerichtet sein.
- Mediatrix 44xx-Gateways unterstützen keine Telefonie-Leistungsmerkmale für die ISDN-Telefone.
- Das Aktualisieren der Anzeige für die ISDN-Telefone wird ebenfalls nicht unterstützt.
- ISDN-Verbindungen werden nur unterstützt, wenn Mediatrix-Gateways der Serie 44xx verwendet werden.
- ISDN-Sprach-Verbindungen werden nur für Teilnehmer oder Trunks unterstützt, die an dem selben OpenScape 4000 SoftGate eingerichtet sind.
- Im Falle von Subscriber Calls (d.h. für kommende Rufe von Mediatrix-Gateway-Teilnehmern) gilt, dass diese stets ihre Calling-Number (interne/Extension-Number) mitliefern müssen.
  - Falls das ISDN-Endgerät dies nicht leistet, kann ein Hinzufügen der Calling-Number ggf. auch im Mediatrix-Gateway konfiguriert werden. Eine solche Konfiguration ist im Mediatrix-Gateway (z.B. ISDN-port bezogen) möglich.
  - Sind mehrere ISDN-Teilnehmer über ISDN-Bus an einem Mediatrix-Gateway-ISDN-Port angeschlossen, ist dies unter Umständen nicht mehr eindeutig möglich – es sei denn, es lassen sich die Teilnehmer anhand des Call-Typs (Bearer-Type) unterscheiden).

3.3.3.1.2 Beispiel-Szenario mit Mediatrix 4402 Gateway

In diesem Beispiel-Szenario wird ein Mediatrix-Gateway für S0-Teilnehmer verwendet.

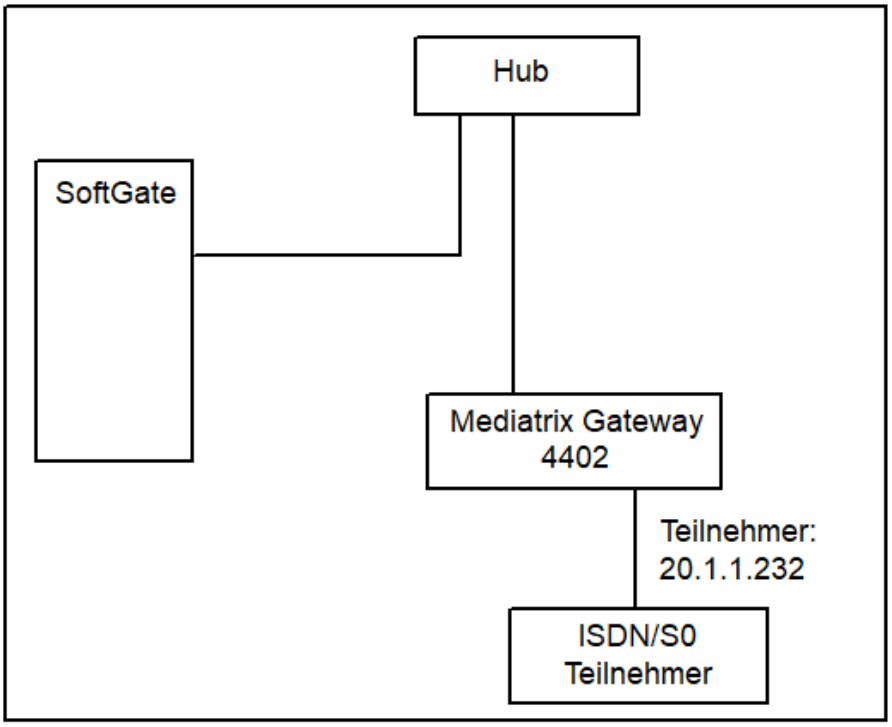


Abbildung 55: Szenario OpenScape 4000 SoftGate mit Mediatrix 4402 Gateway - S0-Teilnehmer

3.3.3.1.3 Konfiguration

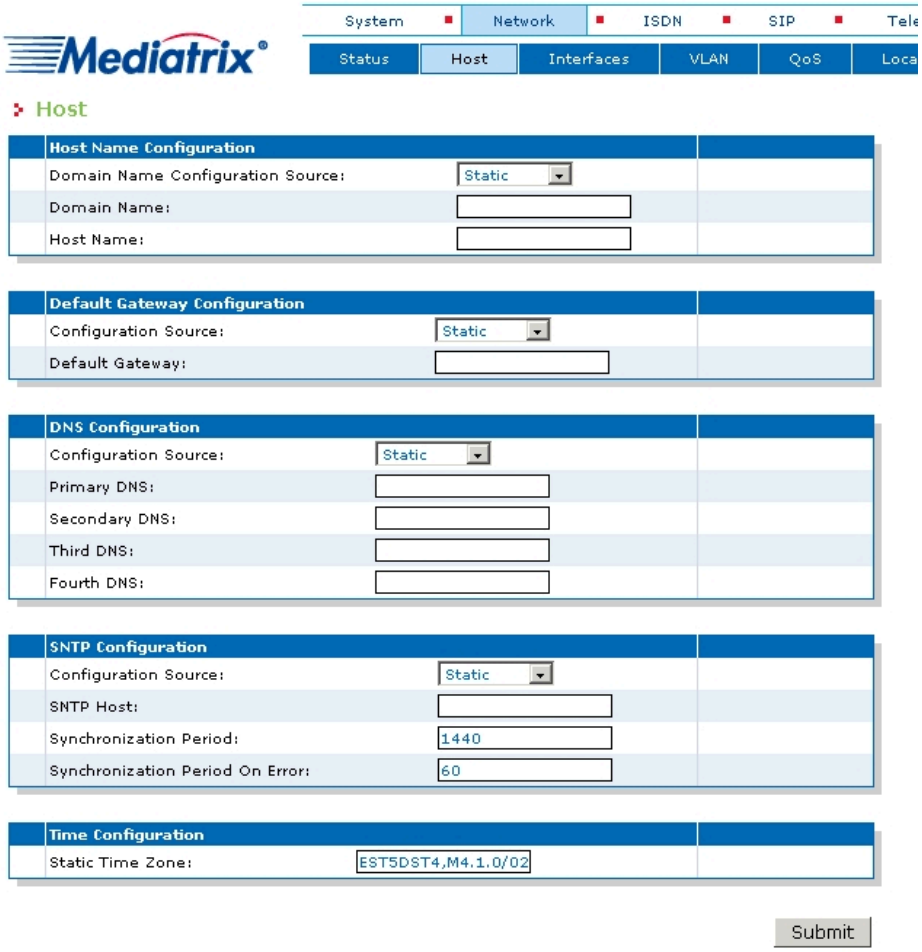
Die Abbildungen in diesem Abschnitt beziehen sich auf die Konfiguration im Beispielszenario.

Überblick

- Netzwerk -> Host
- Network -> Interfaces
- SIP -> Gateways
- SIP -> Servers
- SIP -> Registrations
- ISDN -> Basic Rate Interface
- Telephony -> Call Routing Config

Netzwerk -> Host

Richten Sie die Host Domain, das Default-Gateway, DNS Source und SNTP Source alle als **static** ein.



Mediatrix 44xx Gateway (Teiln.) - Network -> Host

Network -> Interfaces

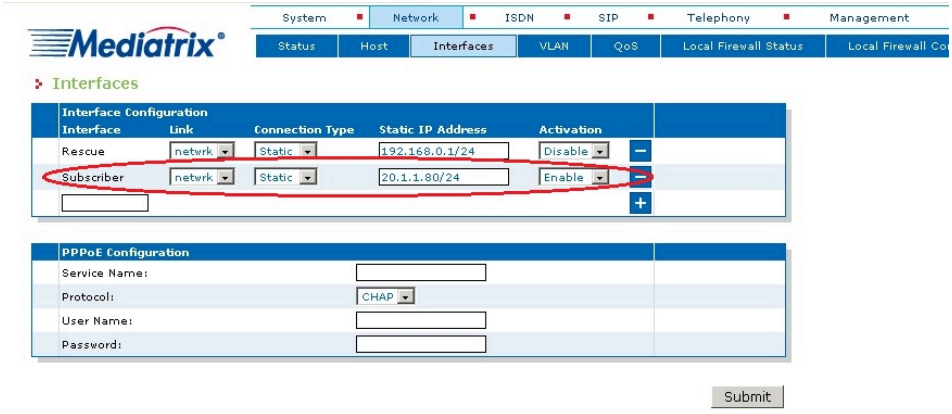
Die Netzwerk-Schnittstellen sollten mit eindeutigen LAN IP-Adressen eingerichtet werden. Ein Mediatrix 4400 Gateway kann bis zu 48 Netzwerk-Schnittstellen unterstützen.

Wichtig: Die IP-Adressen müssen sorgfältig vergeben werden, damit sichergestellt ist, dass das OpenScape 4000 SoftGate sie auch erreichen kann!

Mit einem OpenScape 4000 SoftGate (bzw. vHG3500) kann nur eine Netzwerkschnittstelle des Mediatrix-Gateways bedient werden. Gegebenenfalls müssen Teilnehmer- und Trunking-Szenario über eine Netzwerkschnittstelle konfiguriert werden.

Richten Sie in diesem Fenster ein „Subscriber-Interface“ ein.

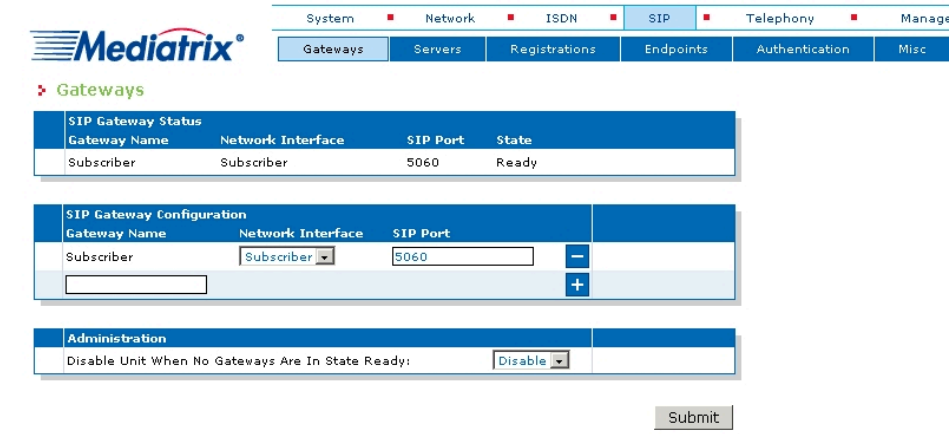
Wichtig: Der Name „Subscriber“ ist frei wählbar und legt noch nicht die Nutzung fest.



Mediatrix 44xx Gateway (Teiln.) - Network -> Interfaces

SIP -> Gateways

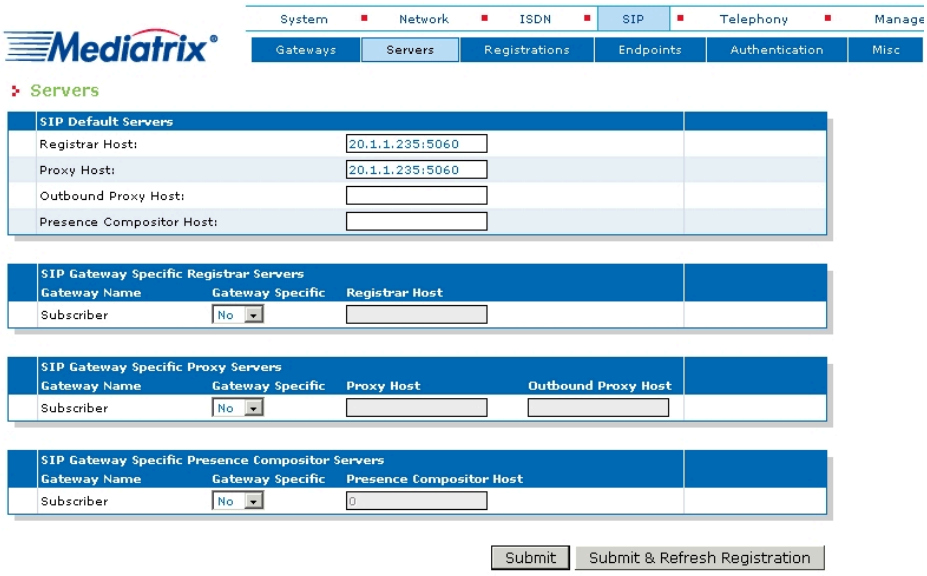
Wählen Sie im Feldbereich „SIP Gateway Configuration“ den Wert **Subscriber** aus.



Mediatrix 44xx Gateway (Teiln.) - SIP -> Gateways

SIP -> Servers

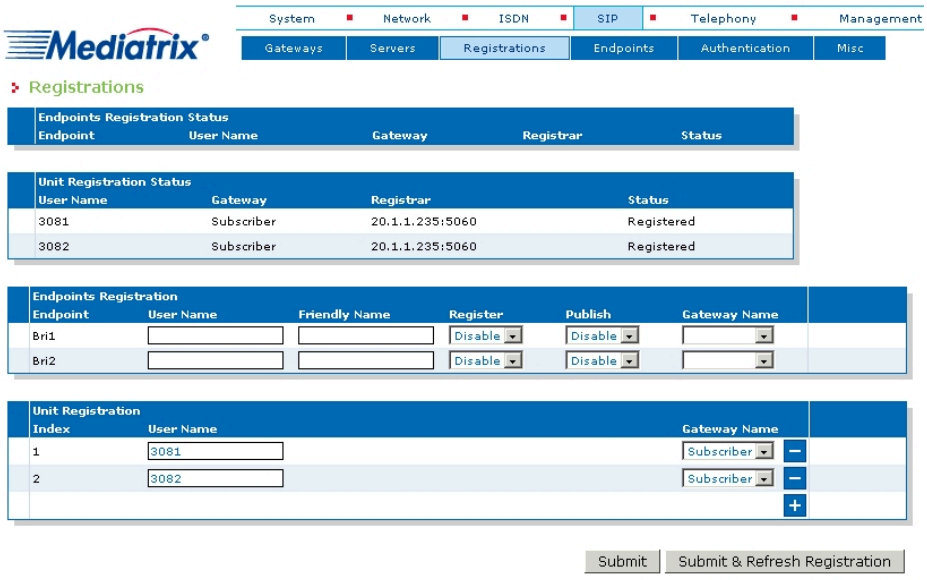
Geben Sie die Werte im Feldbereich „SIP-Default Servers“ ein, „Registrar Host“ und „Proxy.



Mediatrix 44xx Gateway (Teiln.) - SIP -> Servers

SIP -> Registrations

Geben Sie die Rufnummern der ISDN-Teilnehmer zur Registrierung am SIP-Server ein. Fügen Sie die Teilnehmer-Endgeräte hinzu und wählen Sie das Teilnehmer-SoftGate aus. Das Feld „User Name“ bezieht sich auf die Telefonnummer.



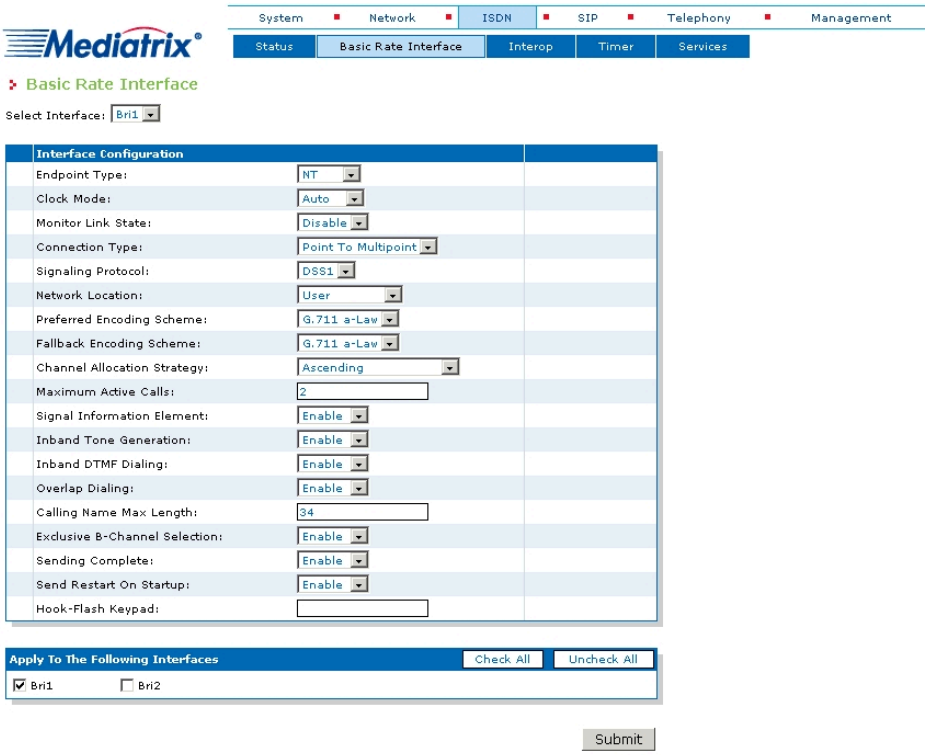
Mediatrix 44xx Gateway (Teiln.) - SIP -> Registrations

ISDN -> Basic Rate Interface

Konfigurieren Sie die ISDN-Parameter für jede zu verwendende Schnittstelle.

- Endpunkttyp: **NT**
- Connection Type: z.B.: **Point To Multipoint**

In einem reinen Teilnehmer-Szenario sehen die weiteren Schnittstellen in der Regel genauso wie die erste aus. Üblicherweise wird „Exclusive B-Channel Selection“ verwendet.

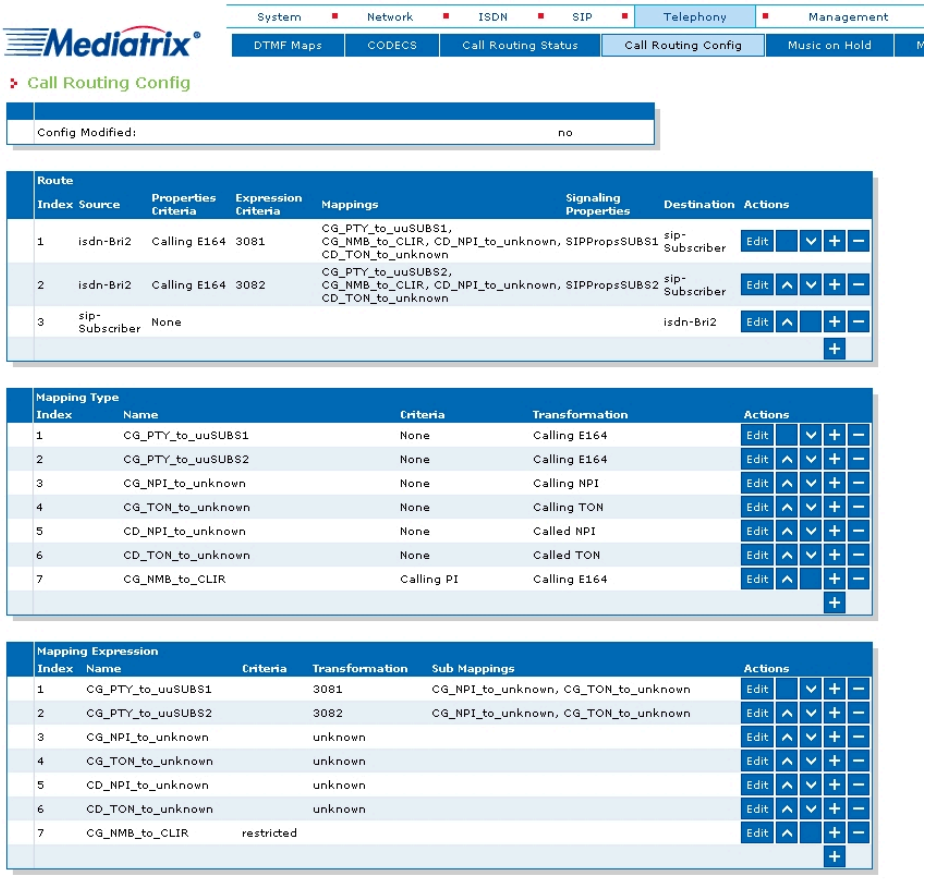


Mediatrix 44xx Gateway (Teiln.) - ISDN -> Basic Rate Interface

Telephony -> Call Routing Config

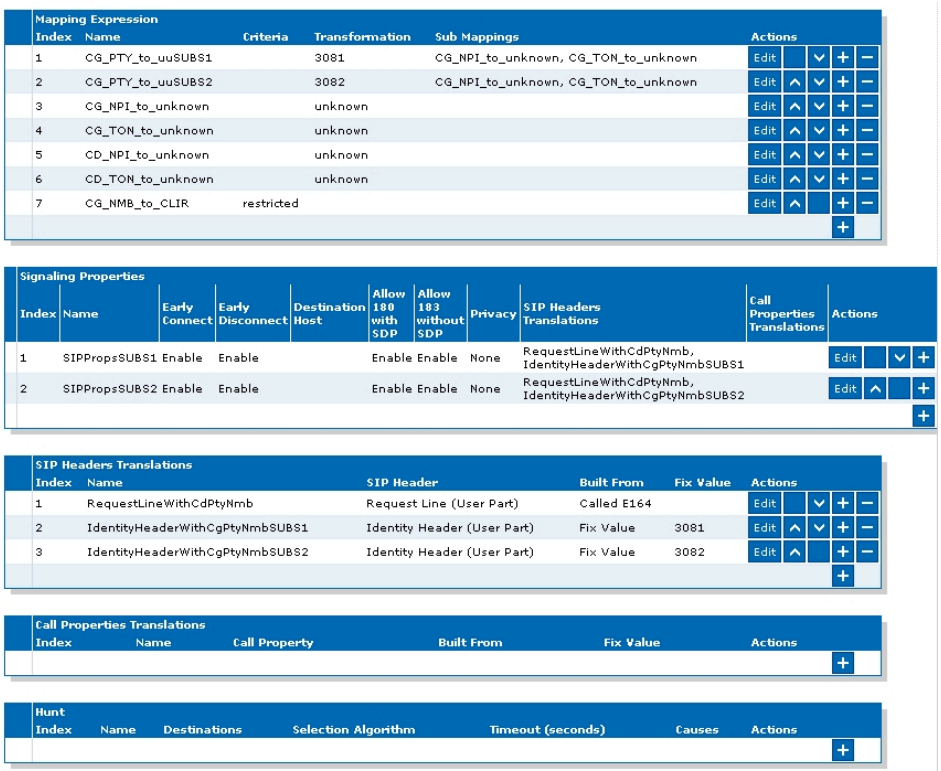
Legen Sie in diesem Fenster fest, wie die Anrufe vom/ins VoIP-Netzwerk zu den ISDN-Telefonen geroutet werden sollen.

Das Beispiel zeigt eine Konfiguration mit zwei Teilnehmern (3081 und 3082), die beide über einen ISDN-Bus am BRI2 des Gateways angeschlossen sind. In diesem Beispiel wird vorausgesetzt, dass beide Teilnehmer ihre Rufnummern mitliefern. Hinsichtlich CLIR zeigt dieses Beispiel einige sehr spezielle Konfigurationen, die üblicherweise nur sehr sparsam anzuwenden sind. Das Mediatrix-Gateway bietet auch eine Standard-Auswahl für die Handhabung von CLIR.



Mediatrix 44xx Gateway (Teiln.) - Telephony -> Call Routing Config 1

Für den SIP-Protokoll-Abgleich zwischen Mediatrix-Gateway und OpenScape 4000 SoftGate ist unter Umständen die Konfiguration „RequestLineWithCdPtyNmb“ notwendig.



Mediatrix 44xx Gateway (Teiln.) - Telephony -> Call Routing Config 2

3.3.3.2 S0-Trunking (Mediatrix 44xx)

Ein Mediatrix 4400 Gateway kann gleichzeitig eine ISDN-Teilnehmerleitung und eine Leitung zum öffentlichen Netz unterstützen.

3.3.3.2.1 Anforderungen

- ISDN-Verbindungen werden nur unterstützt, wenn Mediatrix-Gateways der Serie 44xx verwendet werden.
- ISDN-Sprach-Verbindungen werden nur für Teilnehmer oder Trunks unterstützt, die an dem selben OpenScape 4000 SoftGate eingerichtet sind.
- Es wird empfohlen, dass jedes Gateway mit einem gemeinsamen Takt synchronisiert wird. Beispielsweise erhalten die Gateways den Taktimpuls über eine direkte Verbindung zum öffentlichen Netz oder über eine interne ISDN-S0-Leitung (Layer-0 Verbindung) zu einem anderen synchronisierten Gateway, wie im Beispiel-Szenario dargestellt.

3.3.3.2.2 Beispiel-Szenario mit Mediatrix 4402 Gateway

In diesem Beispiel-Szenario wird ein Mediatrix-Gateway für Trunking zum öffentlichen Netz verwendet.

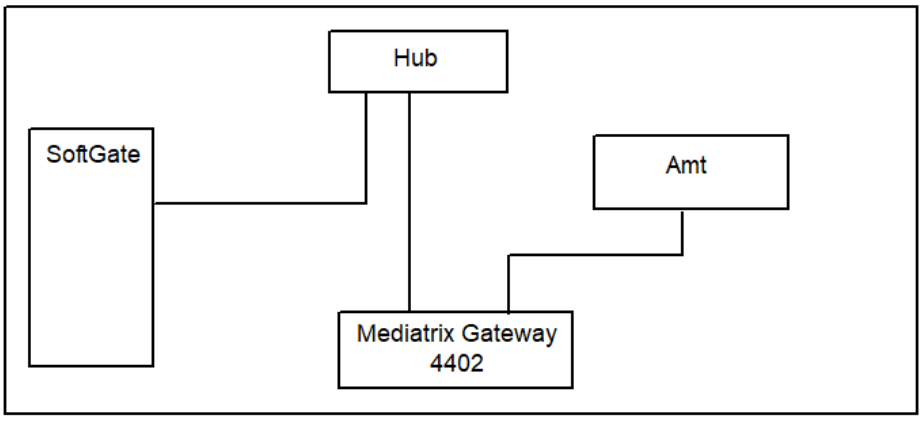


Abbildung 56: Szenario OpenScape 4000 SoftGate mit Mediatrix 4402 Gateway - Trunking

3.3.3.2.3 Konfiguration

Die Abbildungen in diesem Abschnitt beziehen sich auf die Konfiguration im Beispielszenario.

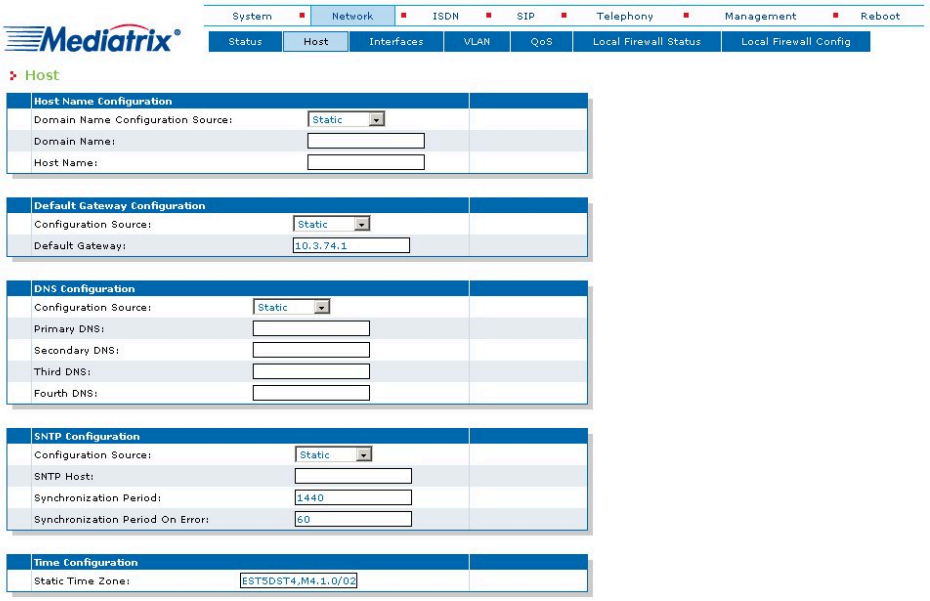
Überblick

- Netzwerk -> Host
- Network -> Interfaces
- SIP -> Gateways
- SIP -> Servers
- SIP -> Registrations
- ISDN -> Basic Rate Interface
- Telephony -> Call Routing Config

Netzwerk -> Host

Einrichten von **Static**

- im Abschnitt **Host Name Configuration** für die **Domain Name Configuration Source**,
- im Abschnitt **Default Gateway Configuration** für die **Configuration Source**,
- im Abschnitt **DNS Configuration** für die **Configuration Source** und
- im Abschnitt **SNTP Configuration** für die **Configuration Source** ein.



Mediatrix 44xx Gateway (Trunking) - Network -> Host

Network -> Interfaces

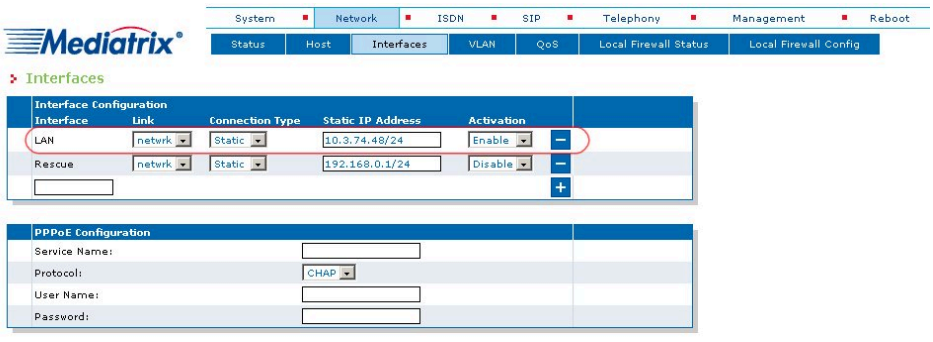
Die Netzwerk-Schnittstellen sollten mit eindeutigen LAN IP-Adressen eingerichtet werden. Theoretisch kann ein Mediatrix 4400 Gateway bis zu 48 Netzwerk-Schnittstellen unterstützen.

Wichtig: Die IP-Adressen müssen sorgfältig vergeben werden, damit sichergestellt ist, dass das OpenScape 4000 SoftGate sie auch erreichen kann!

Mit einem OpenScape 4000 SoftGate (bzw. vHG3500) kann nur eine Netzwerkschnittstelle des Mediatrix-Gateways bedient werden. Gegebenenfalls müssen Teilnehmer- und Trunking-Szenario über eine Netzwerkschnittstelle konfiguriert werden.

Richten Sie in diesem Fenster ein LAN-Interface ein.

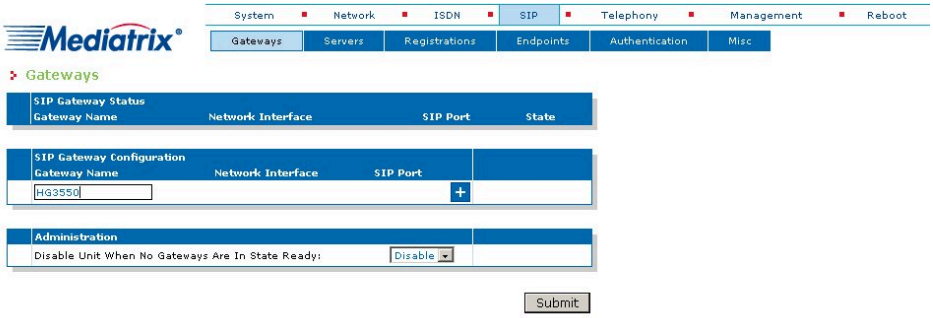
Wichtig: Der Name für das Interface ist frei wählbar und legt noch nicht die Nutzung fest. In diesem Fall nennen wir es „LAN“.



Mediatrix 44xx Gateway (Trunking) - Network -> Interfaces

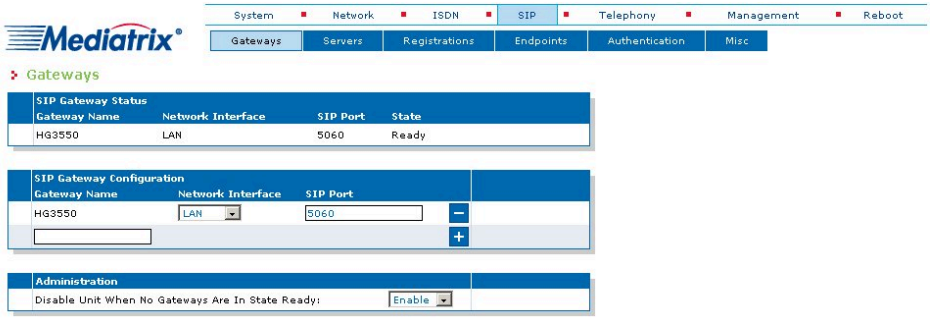
SIP -> Gateways

Richten Sie nun Ihr SIP-Gateway ein. Als Gatewaynamen (**Gateway Name**) können Sie beispielsweise „HG3550“ verwenden.



Mediatrix 44xx Gateway (Trunking) - SIP -> Gateways

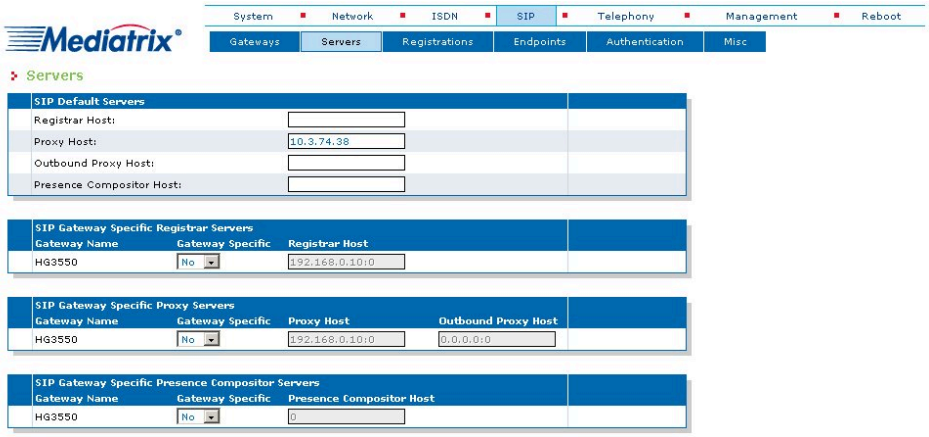
Wählen Sie im Feldbereich **SIP Gateway Configuration** im Feld **Network Interface** den Wert „LAN“ aus.



Mediatrix 44xx Gateway (Trunking) - SIP -> Gateways

SIP -> Servers

Geben Sie im Abschnitt **SIP Default Servers** im Feld **Proxy Host** die IP-Adresse der virtuellen HG 3550 ein (in diesem Fall 10.3.74.38).

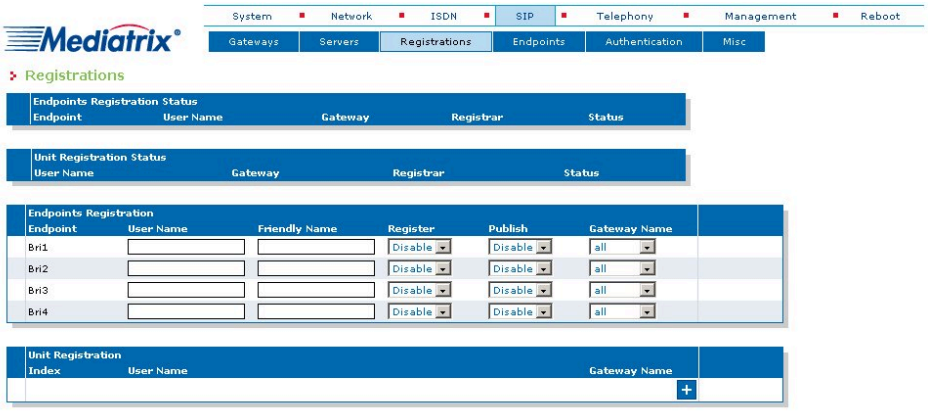


Mediatrix 44xx Gateway (Trunking) - SIP -> Servers

SIP -> Registrations

In der Trunking-Konfiguration gibt es keine Endpunkte, daher ist keine Registrierung notwendig.

Wichtig: Das Mediatrix-Gateway unterstützt lediglich SIP-Native (kein SIP-Q), daher ist im Fall von Trunking kein Registrierungsmechanismus vorgesehen.



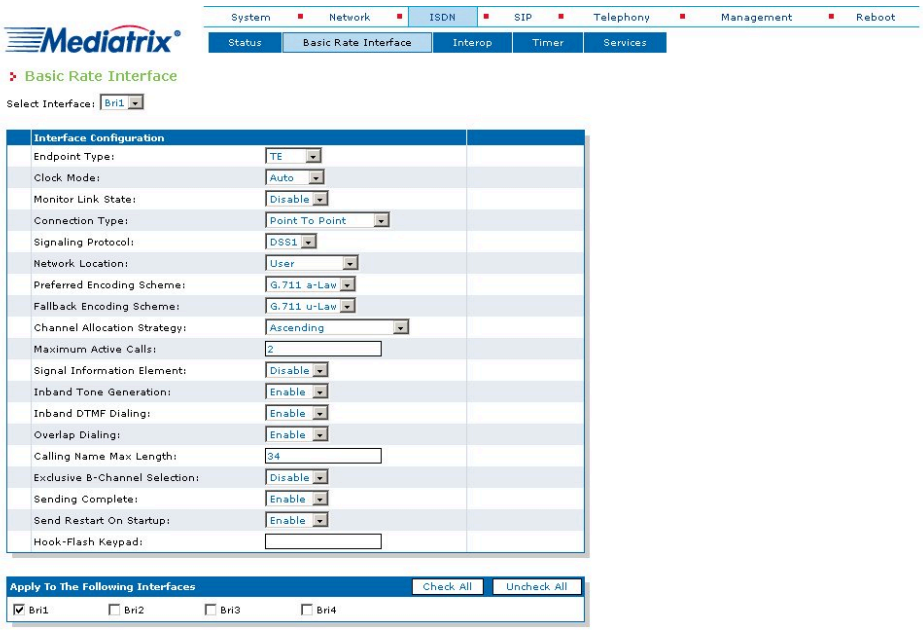
Mediatrix 44xx Gateway (Trunking) - SIP -> Registrations

ISDN -> Basic Rate Interface

Konfigurieren Sie die ISDN-Parameter für jede zu verwendende Schnittstelle.

- Endpunkttyp: **TE**
- Connection Type: z.B.: **Point To Point**

Entsprechend dem Protokoll des ISDN-Trunking-Partners/CO-Providers ist gegebenenfalls sicherzustellen, dass das Feld „Exclusive B-Channel Selection“ beider Schnittstellen aktiviert (enabled) ist.



Mediatrix 44xx Gateway (Trunking) - ISDN -> Basic Rate Interface

Telephony -> Call Routing Config

Im allgemeinen Szenario für CO-Trunks wird die „Telephony - Call Routing Config“ des Mediatrix-Gateways nicht (d.h. insbesondere nicht zur Unterscheidung aufgrund von E.164 Nummern) benutzt. Die

Rufnummernbehandlung wird üblicherweise im OpenScape-4000-System konfiguriert (siehe Konfigurationsbeispiel OpenScape 4000 für S0-Trunking).

Konfigurationsbeispiel OpenScape 4000 für S0-Trunking

```
EINR-
BFDAT:FCTBLK=34,FUNCTION=HG3550&SIP,BGBKAN=BKAN120,ATTR=SOCO;
AE-
BFDAT:CONFIG=WEITER,FCTBLK=34,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=1;
AE-
BFDAT:CONFIG=WEITER,FCTBLK=34,FUNCTION=SIP,ANZSATZ=20,ANZBKAN=2;
AE-BFDAT:CONFIG=OK,FCTBLK=34,ANTW=JA;
/*   */
EINR-BCSU:TYP=IPGW,LTG=1,LTU=19,EBT=8,SACHNR="Q2330-X
 ",FCTID=1,LWVAR=0,FCT►
BLK=34,BKANSIP=2,BKAN3550=10,ALARMNR=0;
/*   */
EINR-
CGWB:LTU=19,EBT=8,SMODE=NORMAL,IPADR=10.3.74.38,NETMASK=255.255.255.0;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=GLOBIF,MUSTER=213,VLAN=NEIN,VLANID=0,DE
0,BITRATE=AUTONEG,TRPRSIP=10,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TLSP=406
DR=0.0.0.0;
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=SERVIF,LOGINTRM="TRM";
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,UDPPRTLO=29100,TOSPL=48,TOSSIGNL=18
A,RFCFMOIP=JA,RFCDTMF=JA,REDRFCTN=JA,PRIO=PRIO1,CODEC=G711A,VAD=NEIN,R
```

REDRFCTN	Redundante Übertragung der RFC2833 Töne nach RFC2198
RFCDTMF	Übertragung von DTMF Tönen nach RFC2833
RFCFMOIP	Übertragung von Fax/Modem Tönen nach RFC2833

Wichtig: Die oben genannten Parameter müssen in allen IPDA-Gateways (STMI2/4 respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

```
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO2,CODEC=G729A,VAD=NEIN,RTP
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO3,CODEC=NONE,VAD=NEIN;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO4,CODEC=NONE,VAD=NEIN,RTP=
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO5,CODEC=NONE,VAD=NEIN,RTP=
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO6,CODEC=NONE,VAD=NEIN,RTP=
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=ASC,PRIO=PRIO7,CODEC=G729AB,VAD=JA,RTP=
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=DSP,JITBUFD=60;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=MGNTDATA,MGNTPN=8000,BUSPN=443;
```

```
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=DMCDATA,DMCCONN=0;
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=WBMDATA,LOGINWBM="HP4K-
DEVEL",ROLE=ENGR;
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=WBMDATA,LOGINWBM="HP4K-
SU",ROLE=SU;
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=WBMDATA,LOGINWBM="HP4K-
ADMIN",ROLE=ADMIN;
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=WBMDATA,LOGINWBM="HP4K-
READER",ROLE=READON►
LY;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=GWDATA,GWID1="PRIMARYRASMANAGERID"
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=H235DATA,SECSUBS=NEIN,SECTRNK=NEIN
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-1
218-74-169-221-78-102-174-170;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=LEGKDATA,GWNR=119,GWRNR=23,REGEXTG
AEND-CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=SIPTRERH,GWAUTREQ=NEIN;
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=SIPTRSSA,SIPREG=NEIN,REGIP1=0.0.0.
,PORTTLS1=5061,REGTIME=120,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=
AEND-
CGWB:MTYP=CGW,LTU=19,EBT=8,TYP=DLSDATA,DLSIPADR=10.3.0.200,DL►
SPORT=18443,DLSACPAS=JA;
/*  */
EINRICHTEN-GKREG:GWNR=19,GWATTR=EXTGW&HG3550V2&SIP,GWIPA►
DR=10.3.74.48,GWRNR=22,WAPLNUM=0,WABE=0,LBER=1,INFO="",SECLEVEL=T
/*  */
EINR-BUEND:BUNUM=119,NAME="CO AP19
 MEDIATRIX",ANZ=10,ANZFANG=0,ANZACD=*,PRIO►
NUM=1,TDDRFLAG=ON,GDTRRGL=0,ACDPMGRP=0,ZEICHUM=NEUTRAL;
/*  */
EINR-TDCSU:ART=NEU,LAGE=1-19-008-0,COTNR=21,CO►
PNR=21,WABE=4,VBZ=0,COS=1,LCOSS=1,LCOSD=1,SATZNR="
   ",ZLNR=0,PROT►
VAR=ECMAV2,SEGMENT=8,DEDSVC=KEINE,TRTBL=GDTR,SIDANI=N,TREFTYP=AMT
TCHARG=N,ANZUNT=0,TRACOUNT=31,SATCOUNT=VIELE,ALARMNR=2,FIDX=1,CAR
R,COTX=21,AULX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,
1&G729AOPT,TCCID="",BUNR=119,SUCHART=AB,INBETR=J,SECLEVEL=SECURE,
ANAL=1&&6,BKVER=N,BKGR=1,LWPAR=0,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=
/*  */
/* ------  LCR Bsp. für eine nationale Rufnummer------  */
/* ------  Rufnummer muß als Blockwahl rausgehen------  */
/* ------  In der Anlage muß entweder "vorbereitende Wahl"
 aktiviert sein  -----
-  */
/* ------  oder LDPLN mit -Z und Wahl mit # abschließen
 (SIP Funktionalität-----
-  */
/*  */
EINR-RICHT:ART=LRTGNEU,LRTG=119,LDIENST=ALLE,NAME="CO
 NATIONAL",BUNUM=119,ZKN►
NR=1-1-
119,MFVTEXT="",ROUTATT=JA,EMCYRTT=NEIN,INFO="",PZKNNR=0,CONFTON=N
IN,KPRCAUL=NEIN,KATG=NEIN,CLNAMEDL=NEIN,FWDSWTCH=NEIN,LINFNOT=NEI
```

```
RTE=NEIN;
/*  */
EINRICHTEN-LODR:LWR=19,LWREL=ZIFFSEND,ZIFFERN=49;
EINRICHTEN-LODR:LWR=19,LWREL=ECHOFELD,FELD=4;
EINRICHTEN-LODR:LWR=19,LWREL=NPI,NPI=ISDN,TON=INTERNAT;
EINRICHTEN-LODR:LWR=19,LWREL=ENDE;
/*  */
EINRICHTEN-
LDAT:LRTG=119,LDIENST=ALLE,LWERT=1,BUNUM=119,LWR=19,LBER=1,CARRI►
ER=1,ZONE=LEER,LATTR=KEINE,VCCYK=4,GW1=19-0;
/*  */
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=0-W-0-
Z,LRTG=119,LBER=1,PIN►
DP=NEIN;
```

Es wird davon ausgegangen, dass die OpenScape 4000 alle Wahlmuster (**subscr**, **national**, **internat**) im E164 ISDN / International Format sendet (es muss Blockwahl eingerichtet sein).

Bei dem hier angegebenem Beispiel handelt es sich um einen Standort mit der Rufnummer +49 (30) 430-xxx.

Wichtig: Die am längsten zu bearbeitende Rufnummer muss an erster Stelle bei den Kriterien stehen!

Gehende Rufe vom OpenScape 4000 SoftGate zum CO Carrier

Über das sip-HG3550 Interface kommen alle Wählmuster mit einem „+“ am Anfang am Mediatrix-Gateway an. Daran erkennt das Mediatrix, dass es sich um eine E164-Nummer im ISDN / INTERNATIONAL Format handelt. Je nach Anforderung des CO-Carriers kann dann in Richtung ISDN-BRI auf ein Nationales („CO_outg_national“) oder Subscriber („CO_outg_subscr“) Format modifiziert werden. Die Modifikation gilt für Calling und Called Number.

Kriterien/Umwandlung

Deshalb wird die folgende Criteria/Transformation angwendet:

- E164 -> E164 bzw. TON -> TON.

Kommende Rufe vom CO Carrier zum OpenScape 4000 SoftGate

Gleiches gilt für kommende Rufe in Richtung sip-HG3550.

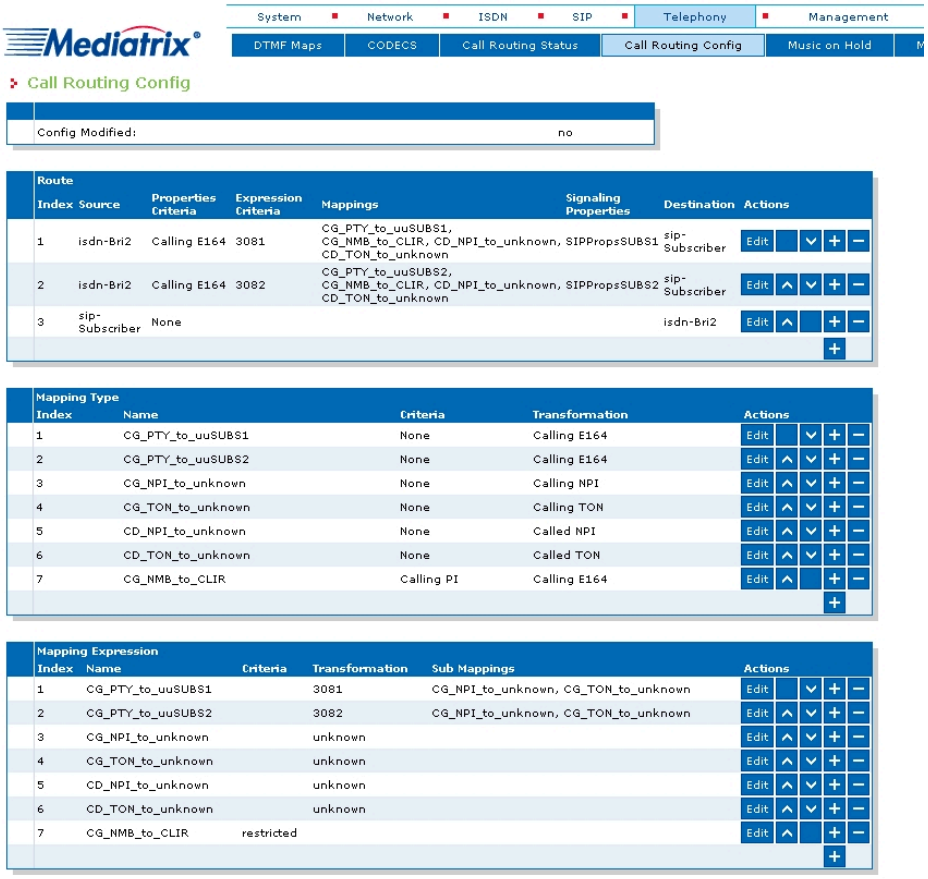
Die Called Number im Subscriber Format wird auf Internationales („CO_inc_called“) Format umgewandelt. Falls der Carrier die Called Number im nationalen Format sendet, muss das Routing von „CO_inc_called (.+) +4930\1“ auf „CO_inc_called (.+) +49\1“ geändert werden.

Die ankommende Rufnummer (Calling Number) wird je nach Format über die Routingeinträge „CO_inc_calling_subscr_to_4930â¦“ bzw. „CO_inc_calling_national_to_49â¦“ modifiziert. Für die Calling Number gelten andere Regelan als für die Called Number, da die Called Number immer gleich ist (je nach Carrier entweder Subscriber oder National) aber die Calling Number unterschiedlich sein kann (**Subscriber**, **National** oder **International**).

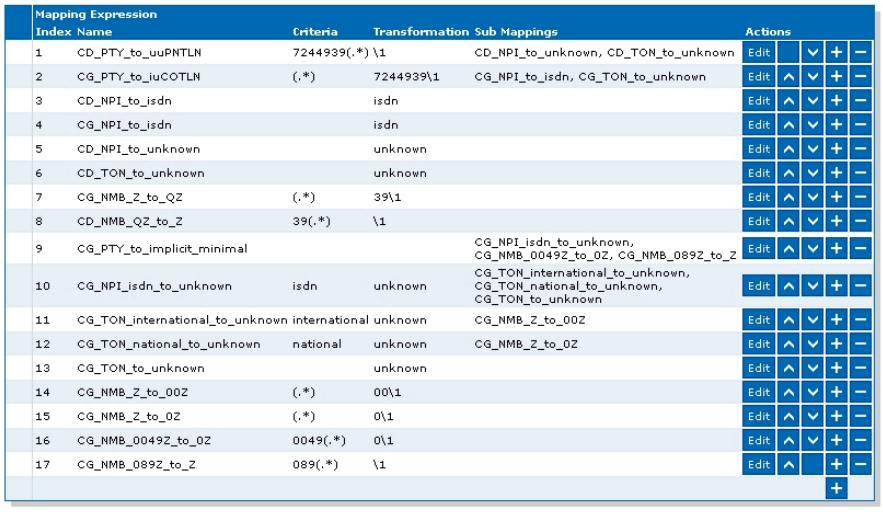
Criteria/Transformation

Deshalb werden die folgenden Criteria/Transformationen angewendet:

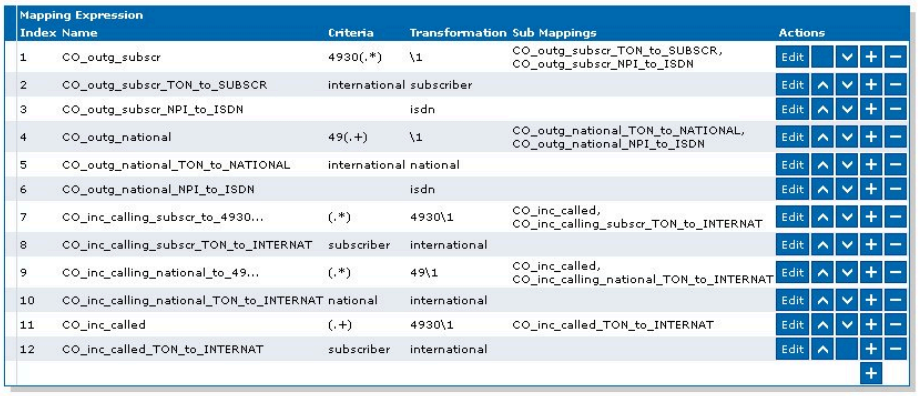
- Calling E164 -> Calling E164 bzw. Calling TON -> Calling TON und
- Called E164 -> Called E164 bzw. Called TON -> Called TON.



Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 1



Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 2



Mapping Expression Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	CO_outg_subscr	4930(.*)	\1	CO_outg_subscr_TON_to_SUBSCR, CO_outg_subscr_NPI_to_ISDN	Edit
2	CO_outg_subscr_TON_to_SUBSCR	international	subscriber		Edit
3	CO_outg_subscr_NPI_to_ISDN		isdn		Edit
4	CO_outg_national	49(.+)	\1	CO_outg_national_TON_to_NATIONAL, CO_outg_national_NPI_to_ISDN	Edit
5	CO_outg_national_TON_to_NATIONAL	international	national		Edit
6	CO_outg_national_NPI_to_ISDN		isdn		Edit
7	CO_inc_calling_subscr_to_4930...	(.*)	4930\1	CO_inc_called, CO_inc_calling_subscr_TON_to_INTERNAT	Edit
8	CO_inc_calling_subscr_TON_to_INTERNAT	subscriber	international		Edit
9	CO_inc_calling_national_to_49...	(.*)	49\1	CO_inc_called, CO_inc_calling_national_TON_to_INTERNAT	Edit
10	CO_inc_calling_national_TON_to_INTERNAT	national	international		Edit
11	CO_inc_called	(.+)	4930\1	CO_inc_called_TON_to_INTERNAT	Edit
12	CO_inc_called_TON_to_INTERNAT	subscriber	international		Edit

Mediatrix 44xx Gateway (Trunking) - Telephony -> Call Routing Config 3

3.3.3.3 ISDN (S0) Daten-Verbindungen (Mediatrix 44xx)

3.3.3.3.1 Anforderungen für ISDN (S0) Daten-Verbindungen

Wichtig: Grundlegende Informationen zur Installation von S0 Daten-Szenarien finden Sie in der Beschreibung über die Installation von S0 Teilnehmern und S0 Trunking Szenarien. Dieser Abschnitt beschreibt die besonderen Anforderungen für S0 Daten-Verbindungen, die zusätzlich berücksichtigt werden müssen.

- ISDN Daten-Verbindungen werden nur unterstützt, wenn Mediatrix-Gateways der Serie 44xx verwendet werden.
- ISDN Daten-Verbindungen werden nur für Teilnehmer oder Trunks unterstützt, die an dem selben OpenScape 4000 SoftGate eingerichtet sind.

Wichtig: Direct Media über LAN (DMC) ist für S0 Daten-Verbindungen nicht möglich.

- Alle ISDN S0-Gateways für Datenverbindungen sollten mit einer gemeinsamen Uhr synchronisiert werden. Beispielsweise erhalten die Gateways den Taktimpuls über eine direkte Verbindung zum öffentlichen Netz oder über eine interne ISDN-Leitung (Layer-2-Verbindung) zu einem anderen synchronisierten Gateway.

3.3.3.3.2 Beispiel-Szenario mit zwei Mediatrix 44xx Gateways

In diesem Beispiel-Szenario wird ein Mediatrix-Gateway für Teilnehmer, das andere für Trunking zum öffentlichen Netz verwendet.

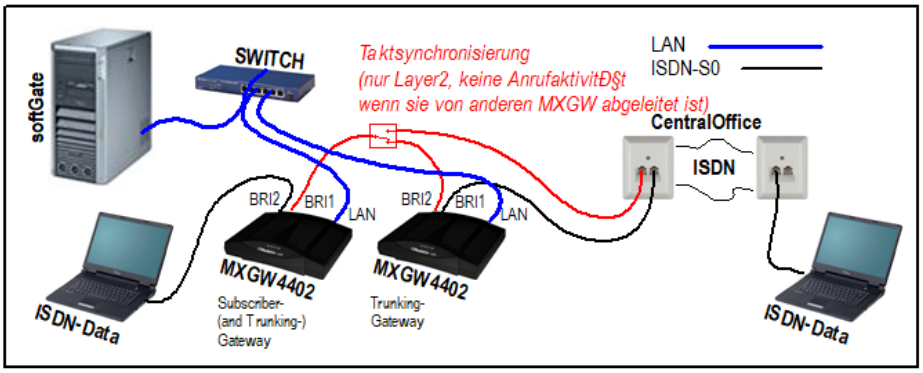


Abbildung 57: Szenario OpenScape 4000 SoftGate mit 2 Mediatrix-Gateways

Ein solches Szenario ist eine Alternative zum Einrichten von Teilnehmern und Trunking innerhalb eines Gateways. Diese Taktsynchronisations-Methode wird außerdem benötigt, wenn mehr als vier ISDN S0 Ports konfiguriert werden sollen (an einem einzelnen Mediatrix-Gateway sind maximal vier S0 Ports verfügbar).

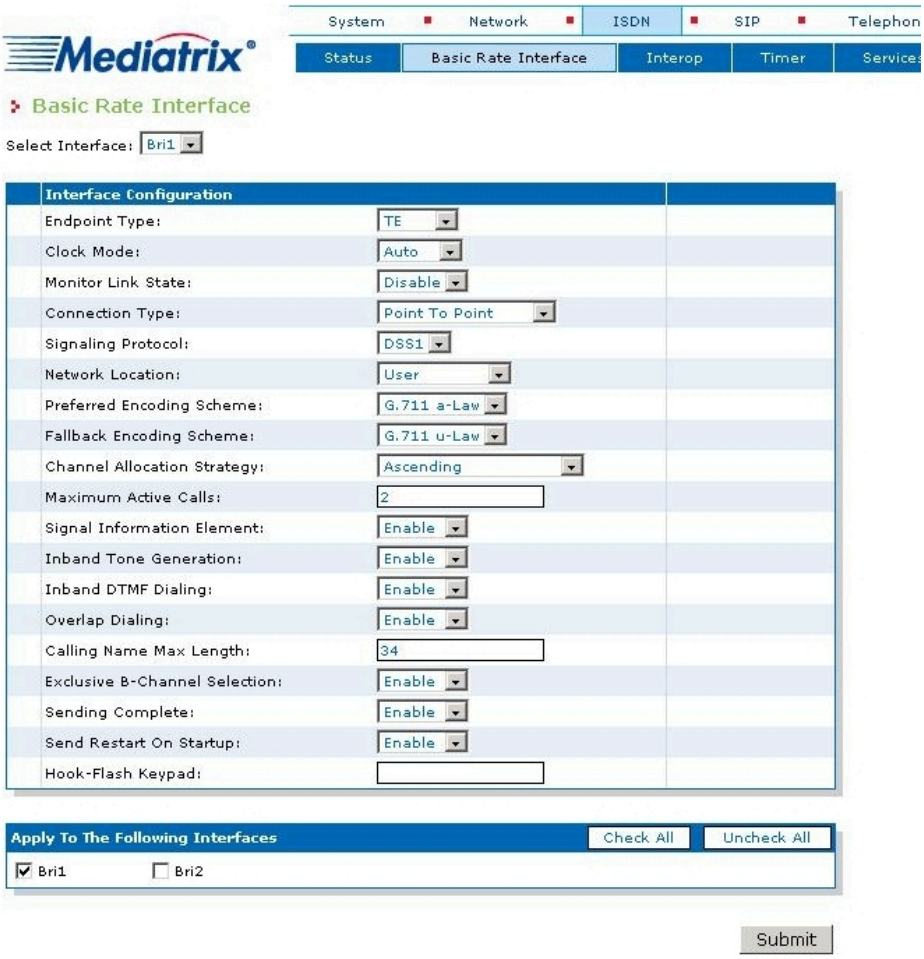
3.3.3.3.3 Trunking-Gateway

Überblick

- ISDN -> Basic Rate Interface (BRI 1)
- ISDN -> Basic Rate Interface (BRI 2)
- ISDN -> Status
- Codec-Parameter Trunking- und Teilnehmer-Gateway

ISDN -> Basic Rate Interface (BRI 1)

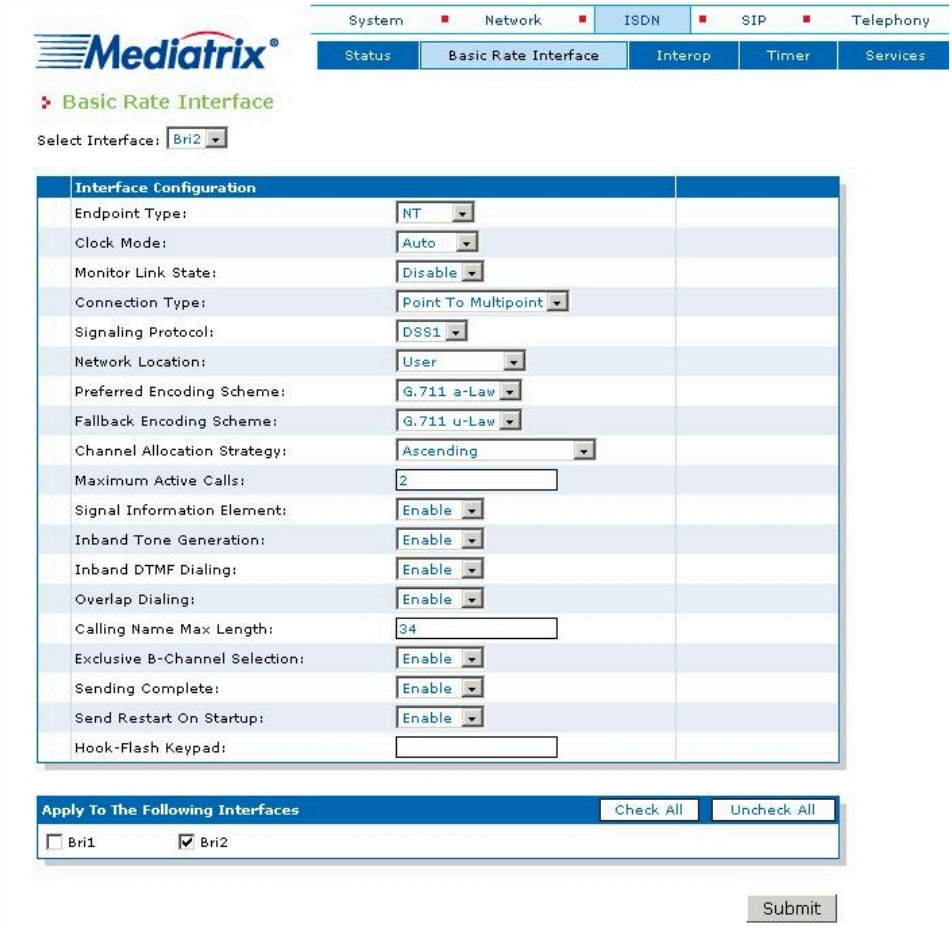
Das Trunking-Gateway ist mit dem öffentlichen Netz über den BRI 1 Port verbunden und synchronisiert sich mit dem empfangenen Taktimpuls.



Mediatrix Gateway Trunking - ISDN -> Basis Rate Interface 1

ISDN -> Basic Rate Interface (BRI 2)

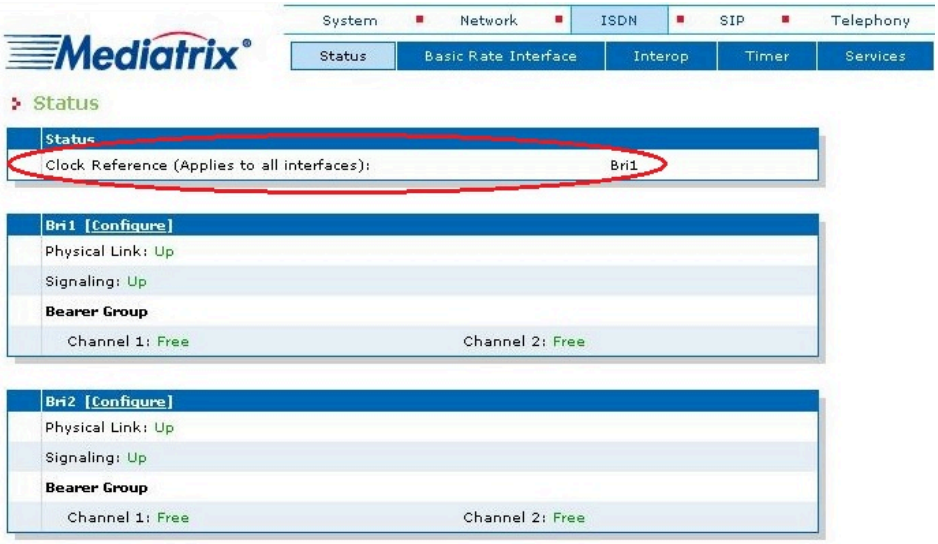
Der Port BRI 2 wird verwendet, um den Taktimpuls an das Teilnehmer-Gateway weiterzugeben.



Mediatrix 44xx Gateway Trunking - ISDN -> Basis Rate Interface 2

ISDN -> Status

Im Statusfenster wird angezeigt, dass die Takelung über den BRI1 Port erfolgt, der an das öffentliche Netz angeschlossen ist. Außerdem sieht man, dass der Link am Port BRI 2 zur Übergabe des Taktimpulses zum Teilnehmer-Gateway ebenfalls funktioniert (die Layer- 3-Signalisierung wird bei diesem Link nicht verwendet).



Mediatrix 44xx Gateway Trunking - ISDN -> Status

3.3.3.3.4 Teilnehmer-Gateway

Überblick

- ISDN -> Basic Rate Interface (BRI 1)
- ISDN -> Status
- Codec-Parameter Trunking- und Teilnehmer-Gateway

ISDN -> Basic Rate Interface (BRI 1)

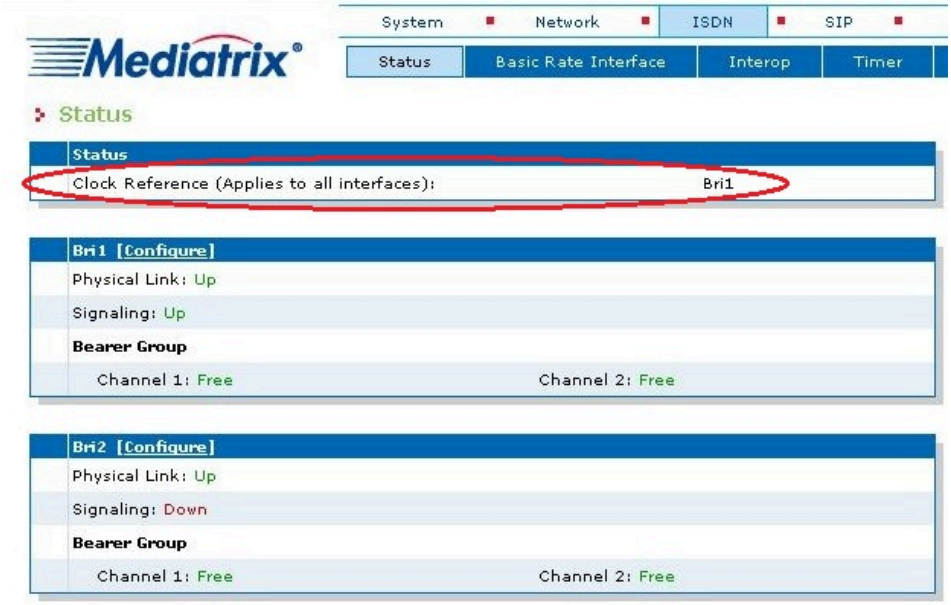
Das Teilnehmer-Gateway ist mit dem Trunking-Gateway (alternativ auch zum öffentlichen Netz) über den BRI 1 Port ohne Layer-3-Signalisierung verbunden und synchronisiert sich auch mit dem indirekt empfangenen Taktimpuls.



Mediatrix 44xx Gateway Teilnehmer - -> Basis Rate Interface 1

ISDN -> Status

Im Statusfenster wird angezeigt, dass die Taktung über den BRI1 Port erfolgt, der die Taktung direkt oder indirekt vom öffentlichen Netz bereitstellt.

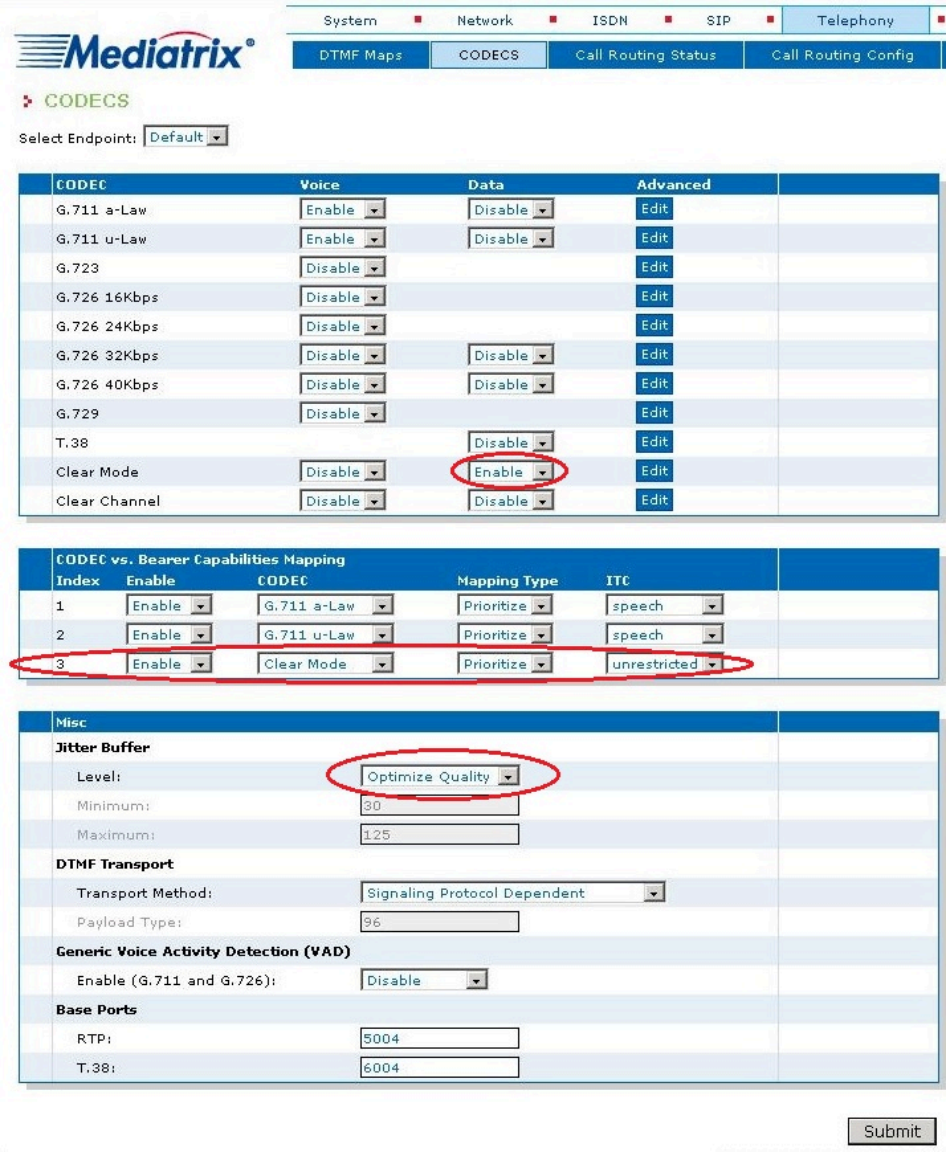


Mediatrix 44xx Gateway Teilnehmer - ISDN -> Status

3.3.3.3.5 Codec-Parameter Trunking- und Teilnehmer-Gateway

Die Einstellungen im Fenster Codec sind für beide Gateways identisch.

- Für den „Codec ClearMode“ muss ein Bearer-Type-Mapping auf „ITC unrestricted“ eingerichtet werden.
- Das Feld „ITC-Typ“ muss den Wert **unrestricted** enthalten.
- Die Einstellung im Feld „Jitter Buffer“ kann zum Verbessern der Qualität der Datenübertragung verwendet werden, wenn die Verzögerungszeit nicht optimiert werden muss.



Mediatrix 44xx Gateway Teilnehmer und Trunking - Telephony -> Codecs

3.3.3.4 S2-Schnittstelle (Mediatrix 36xx)

In diesem Beispiel wird ein Mediatrix Gateway für das Trunking in das öffentliche Netzwerk verwendet.

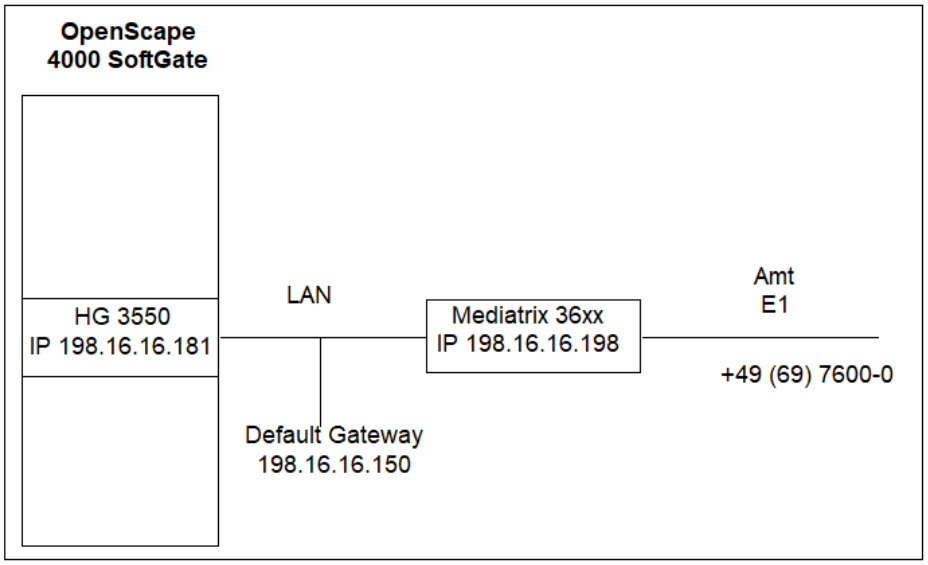


Abbildung 58: OpenScape 4000 SoftGate-Szenario mit Mediatrix 36xx-Gateway - S2-Schnittstelle

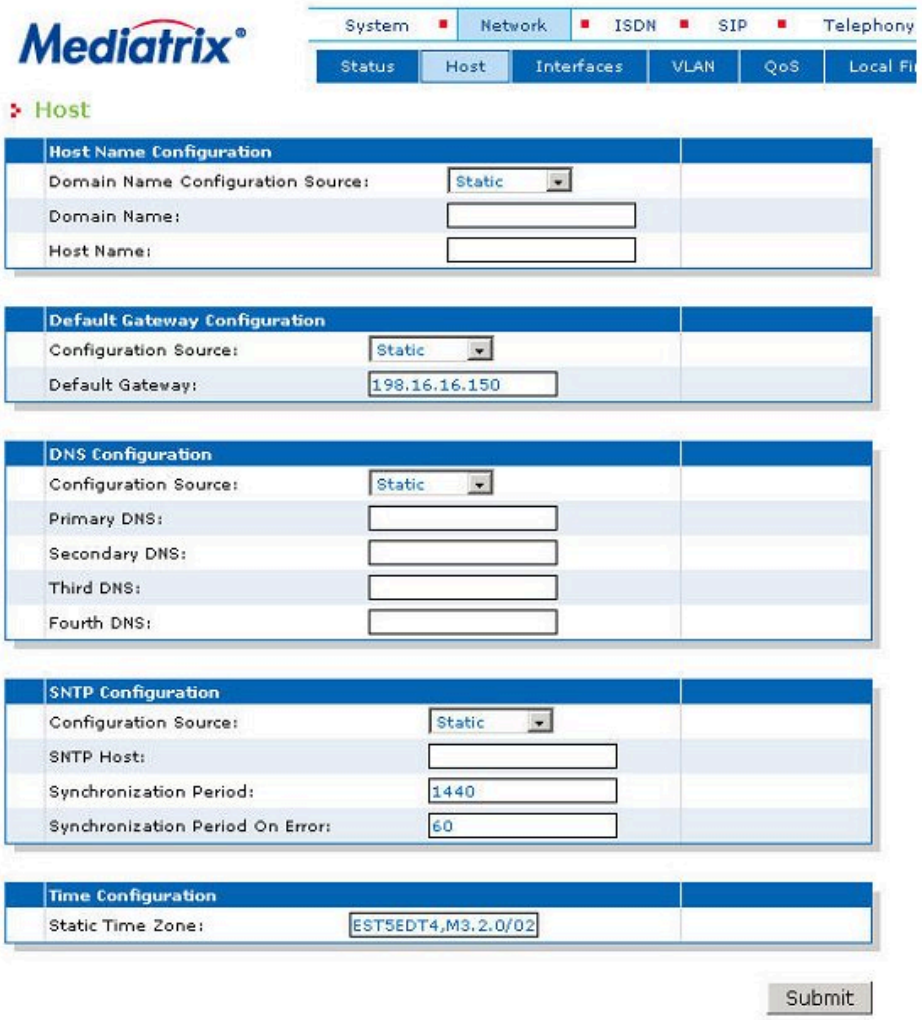
Überblick

- Netzwerk -> Host
- Netzwerk -> Schnittstellen
- SIP -> Gateways
- SIP -> Server
- SIP > Registrierungen
- System -> Hardware
- ISDN -> Primärmultiplexanschluss
- ISDN > Status
- Anruf-Router -> Routenkonfiguration

Netzwerk -> Host

Einrichten von **Static**

- unter **Host Name Configuration** für **Domain Name Configuration Source**,
- unter **DNS Configuration** für **Configuration Source**,
- unter **SNTP Configuration** für **Configuration Source**,
- unter **Standard-Gateway-Konfiguration** für **Konfigurationsquelle** ein.

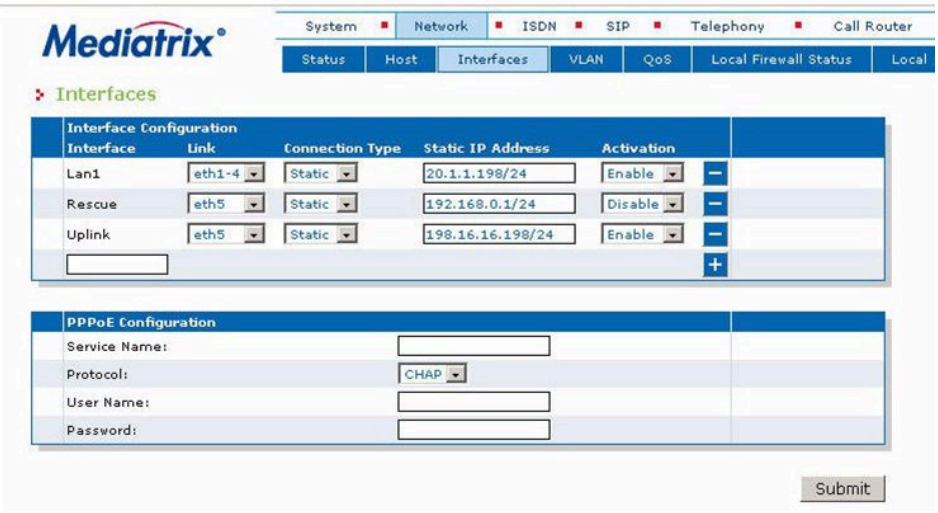


Mediatrix Gateway 36xx - Netzwerk > Host

Netzwerk -> Schnittstellen

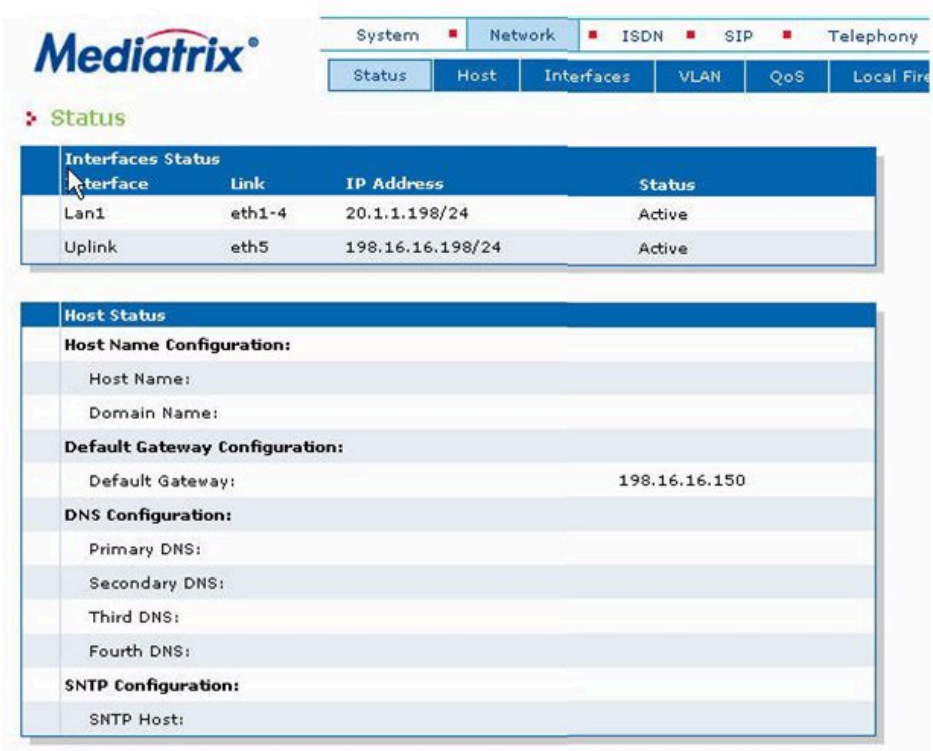
Die Netzwerkschnittstellen sollten mit eindeutigen LAN-IP-Adressen konfiguriert werden. Derzeit wird nur eth5 als uplink verwendet. Eth1-4 sind noch ungenutzt (sind zur Verwendung als Anlagenports vorgesehen).

Wichtig: Achten Sie darauf, dass alle IP-Adressen vom OpenScape 4000 SoftGate aus erreichbar sind.



Mediatrix Gateway 36xx - Netzwerk > Schnittstellen

Der Status kann mit „Netzwerk“ -> „Status“ abgefragt werden.



Mediatrix Gateway 36xx - Netzwerk > Status

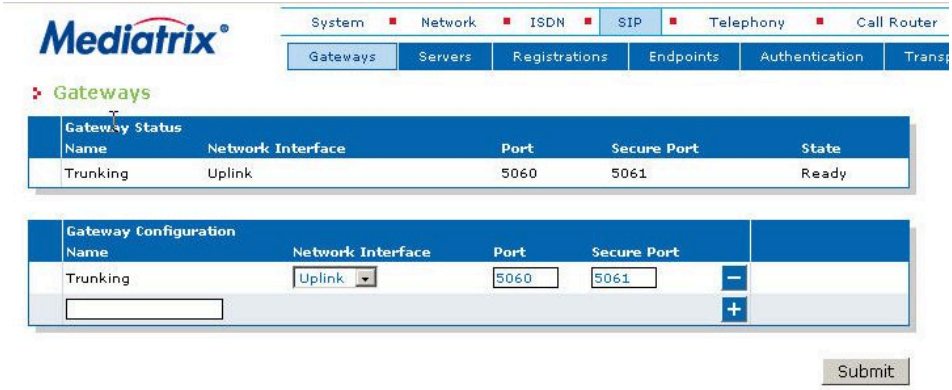
SIP -> Gateways

Konfigurieren Sie jetzt Ihr SIP-Gateway.

SIP-Gateway-Konfiguration:

In diesem Beispiel verwenden wir den **Gateway-Namen** „Trunking“.

Wählen Sie unter **Gateway-Konfiguration** im Feld **Netzwerkschnittstelle** die Einstellung **Uplink**.

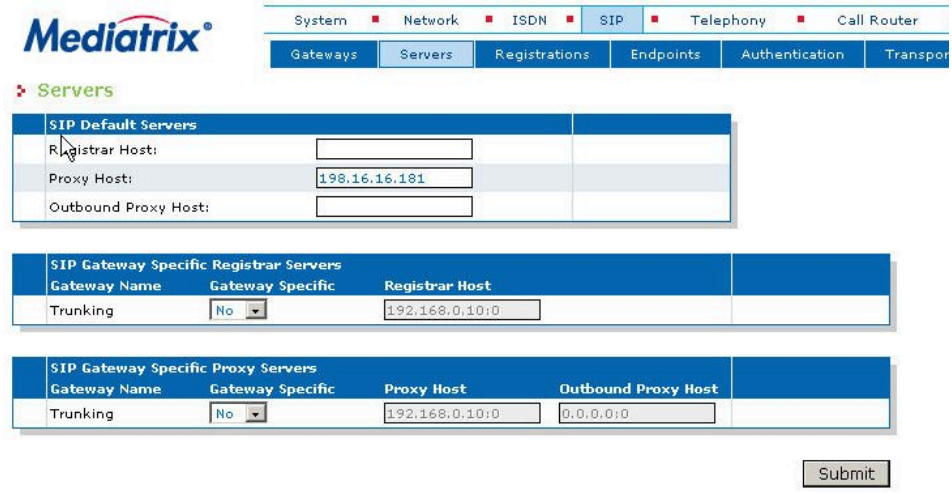


Mediatrix Gateway 36xx - SIP > Gateways

SIP -> Server

Konfigurieren der vHG 3550 Gateway-Adresse (198.16.16.181):

Tragen Sie die IP unter **SIP-Standardserver** in das Feld **Proxy-Host** ein.

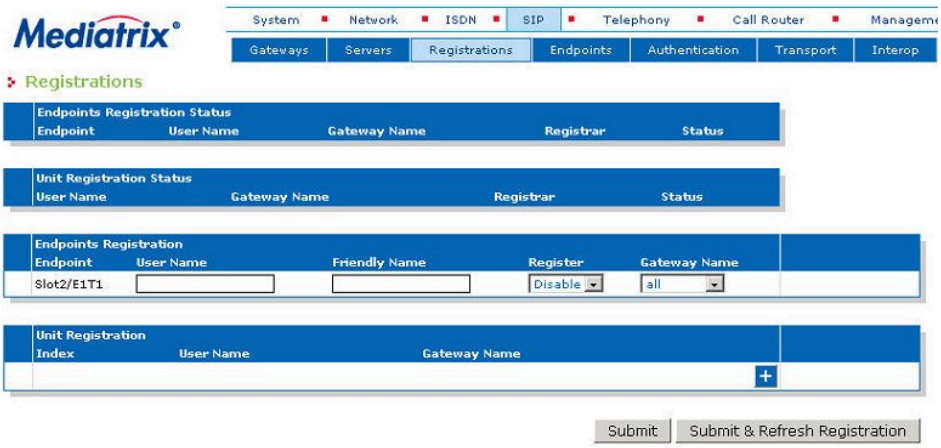


Mediatrix Gateway 36xx - SIP > Server

SIP > Registrierungen

Eine Registrierung ist nicht notwendig, weil die Trunking-Konfiguration keine Endpunkte aufweist.

Wichtig: Da das Mediatrix Gateway nur das native SIP (d.h. nicht SIP-Q) unterstützt, ist für das Trunking kein Registrierungsmechanismus vorgesehen.



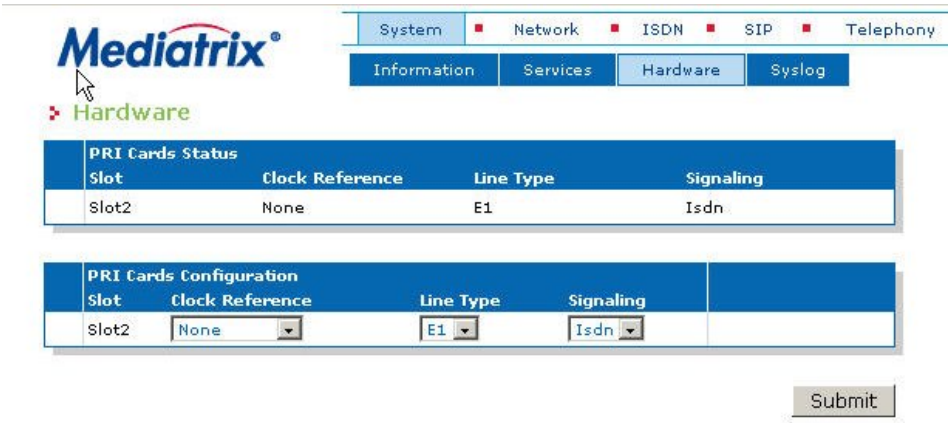
Mediatrix Gateway 36xx - SIP > Registrierungen

System -> Hardware

Hardwarekonfiguration der PRI-Karte.

Wählen Sie unter **PRI-Kartenkonfiguration**

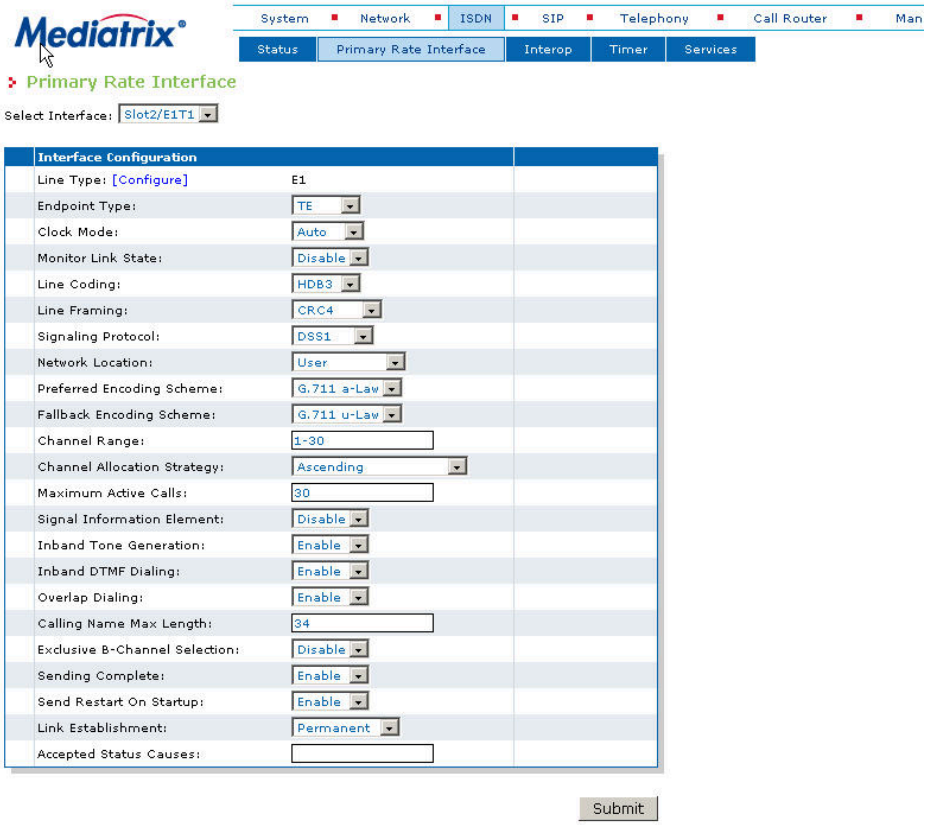
- den **Leitungstyp** (**E1** oder **T1**) aus.
- Wählen Sie unter **Signalisierung** die Einstellung **ISDN**



Mediatrix Gateway 36xx - System > Hardware

ISDN -> Primärmultiplexanschluss

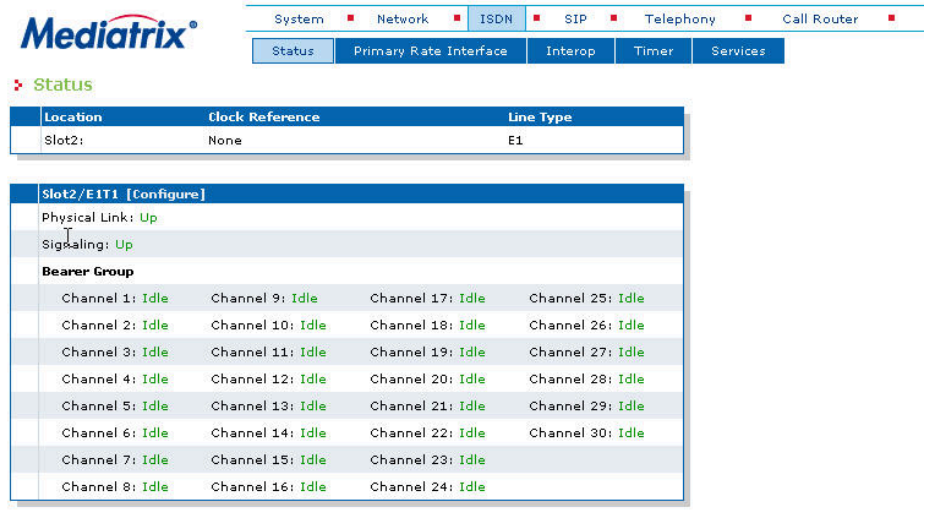
Konfigurieren Sie den Primärmultiplexanschluss.



Mediatrix Gateway 36xx - ISDN > Primärmultiplexanschluss

ISDN > Status

Der Status kann mit „ISDN“ > „Status“ abgefragt werden.



Mediatrix Gateway 36xx - ISDN > Status

Anruf-Router -> Routenkonfiguration

Die Einstellung „Anruf-Router - Routenkonfiguration“ des Mediatrix Gateways wird im allgemeinen Szenario für Amtsleitungen nicht verwendet (insbesondere nicht für die E.164-Nummernbasierte Differenzierung). Die Verarbeitung der Teilnehmerrufnummer wird in der Regel im OpenScape-4000-System konfiguriert (siehe OpenScape 4000-Beispielkonfiguration für S2-Schnittstelle).

OpenScape 4000-Beispielkonfiguration für S2-Schnittstelle

```
EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=18,LTSACHNR="Q2329-X    ",SRCGRP=18,FRAMETYP=SO►
COAP,VERBART=APDL,LSRTADR=198.16.16.186,APRTADR=198.16.16.150,STANDOID=001,STAN►
DORT="CPCI23 SOFTGATE18",PLCHECK=JA,ANZBKAN=120,KONVLAW=NEIN,TCLASS=0,ALARM►
NR=0,SOCOTYP=SOCO50;
EINRICHTEN-BFDAT:FCTBLK=34,FUNCTION=HG3550&SIP,BGBKAN=BCHL120,ATTR=SOCO;
AE-BFDAT:CONFIG=WEITER,FCTBLK=34,FUNCTION=HG3550,ANZSATZ=1,ANZEINH=3;
AE-BFDAT:CONFIG=WEITER,FCTBLK=34,FUNCTION=SIP,ANZSATZ=1,ANZBKAN=4;
AE-BFDAT:CONFIG=OK,FCTBLK=34,ANTW=JA;
EINRICHTEN-BCSU:MTYPE=IPGW,LTG=1,LTU=18,SLOT=1,PARTNO="Q2330-X ",FCTID=1,LW►
VAR=0,FCTBLK=34,BCHLSIP=4,BCHL3550=30,ALARMNO=0;
EINRICHTEN-CGWB:LTU=18,EBT=1,SMODE=NORMAL,IPADR=198.16.16.181,NET►
MASK=255.255.255.0;
AENDERN-CGWB:MTYP=CGW,LTU=18,EBT=1,TYP=GLOBIF,DEFRT=198.16.16.150,BI►
TRATE=100MBFD,TRPRSIP=30;
AENDERN-CGWB:MTYP=CGW,LTU=18,EBT=1,TYP=LEGKDATA,GWNR=199,GWRNR=199,REGEXT►
GK=NEIN;
EINRICHTEN-BUEND:BUNUM=18,NAME="AMT SOCO18 S2     ",ANZ=60,ANZFANG=0,AN►
ZACD=*,PRIONUM=1,TDDRFLAG=ON,GDTRRGL=0,ACDPMGRP=0,ZEICHUM=NEUTRAL;
EINRICHTEN-COT:COTNU=60,COTPAR=RCL&IBSY&ANS&CEBC&CBBN&BSHT&LWNC&NLCR&TSCS&DF►
NN&NLRD&NTON;
EINRICHTEN-COP:COPNU=60,COPPAR=L3AR&SPTR,BERAMT=FBKW,BERFERN=FBKW;
EINRICHTEN-TDCSU:ART=NEU,LAGE=1-18-001-0,COTNR=60,CO►
PNR=60,WABE=0,VBZ=0,COS=1,LCOSS=1,LCOSD=1,SATZNR="AMT SOCO18  ",ZLNR=0,PROT►
VAR=ECMAV2,SEGMENT=8,DEDSVC=KEINE,TRTBL=GDTR,SIDANI=N,TREFTYP=AMT,CBMATTR=KEINE,
TCHARG=N,ANZUNT=0,TRACOUNT=31,SATCOUNT=VIELE,ALARMNR=2,FIDX=1,CARRIER=1,ZONE=LEE
R,COTX=21,AULX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,CLASSMRK=EC&G71
1&G729AOPT,TCCID="",BUNR=18,SUCHART=AB,INBETR=J,SECLEVEL=TRADITIO,GER=HG3550CO,B
KANAL=1&&30,BKVER=N,BKGR=1,LWPAR=0,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCERL=N;
EINRICHTEN-GKREG:GWNR=199,GWATTR=INTGW&HG3550V2&SIP,WAPLNUM=0,WABE=0,LBER=1,IN►
FO="";
EINR-GKREG:GWNR=19,GWATTR=EXTGW&HG3550V2&SIP,GWIPADR=198.16.16.198,
GWRNR=119,WAPLNUM=0,WABE=0,LBER=1;INFO="",SECLEVEL=TRADITIO;
/* -- LCR-Beispiel einer nationalen Rufnummer -- */
/* -- Rufnummer muss per Blockwahl gesendet werden -- */
/* -- Im System muss entweder "prepared dial" aktiviert sein -- */
/* -- oder die LDPLN auf -Z und die Wählziffernfolge auf # enden (SIP-Funktion)
-- */
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=1011,LDIENST=ALLE,NAME="AMT-ORT SOCO18 ",BU►
NUM=18,ZKNNR=1-2-68,ROUTOPT=JA,MFVUMS=NAWA,MFVANZ=ZIFFERN,MFVTEXT="MFV-NACHWAHL

",MFVPULS=PP300,ZLNR=60,ROUTATT=JA,EMCYRTT=NEIN,INFO="",PZKNNR=0,ZEICHUM=NEU►
TRAL;
EINRICHTEN-LODR:LWR=1011,LWREL=ZIFFSEND,ZIFFERN=49;
EINRICHTEN-LODR:LWR=1011,LWREL=ECHOFELD,FELD=4;
EINRICHTEN-LODR:LWR=1011,LWREL=NPI,NPI=ISDN,TON=INTERNAT;
EINRICHTEN-LODR:LWR=1011,LWREL=ENDE;
EINR-LDAT:LRTG=1011,LDIENST=ALLE,LWERT=1,BUNUM=18,LWR=1011,LBER=1,CARRI►
ER=1,ZONE=LEER,LATTR=GEBAKT,VCCYK=4,GW1=19-0;
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=0-W-0-Z,LRTG=1011,LBER=1,PIN►
```

```
DP=NEIN;
```

Es wird davon ausgegangen, dass OpenScape 4000 alle Wählmuster (Teiln., national, international) im internationalen E164 ISDN-Format sendet (d.h. Blockwahl muss konfiguriert sein).

Dieses Beispiel bezieht sich auf einen Standort mit der ISDN-Rufnummer +49 (69) 7600-XXXXX.

Wichtig: Die längste zu modifizierende Rufnummer muss die ersten mit diesen Kriterien sein.

Abgehende Rufe vom OpenScape 4000 SoftGate an den Netzbetreiber

Zwischen dem Mediatrix Gateway und der HG 3550-Schnittstelle werden allen Rufnummern im internationalen E-164 ISDN-Format übertragen. Dieses Rufnummernformat ist durch ein „+“ am Anfang eines jeden Musters gekennzeichnet.

Je nach Anforderungen des Netzbetreibers kann das Format der an die ISDN-Schnittstelle gesendete Rufnummer in den Rufnummerntyp „National“ („CO_outg_national“) oder „Teilnehmer“ („CO_outg_subscr“) geändert werden.

Die Modifikation wird für rufende und gerufene Nummern vorgenommen.

Kriterien/Umwandlung:

Daher gelten die folgenden Kriterien/Umwandlung:

1) E164 -> E164 oder TONE -> TONE.

Ankommende Anrufe vom Netzbetreiber an OpenScape 4000

Dasselbe gilt für ankommende Anrufe bei der SIP HG 3550.

Die gewählte Rufnummer wird vom Teilnehmerformat in das internationale Format („CO_inc_called“) umgewandelt. Wenn der Netzbetreiber die gerufene Nummer im nationalen Format überträgt, muss das Routing von „CO_inc_called (.+) +4969\1“ in „CO_inc_called (.+) +49\1“ geändert werden.

Die ankommende Rufnummer (des rufenden Teilnehmers) wird je nach Format gemäß dem Eintrag „CO_inc_calling_subscr_to_4969â¦“ oder „CO_inc_calling_national_to_49â¦“ modifiziert. Für die Nummer des Anrufers und die gerufene Nummer gelten unterschiedliche Regeln, da die gerufene Nummer immer dieselbe ist (je nach Netzbetreiber entweder Teilnehmer oder national), während die Nummer des Anrufers wechseln kann (Teilnehmer, national oder international).

Kriterien/Umwandlung:

Daher gelten die folgenden Kriterien/Umwandlung:

1) Calling E164 -> Calling E164 bzw. Calling TON -> Calling TON und

- Gerufen E164 -> Gerufen E164 oder Called TONE -> Called TONE.



Mediatrix Gateway 36xx - Anruf-Router > Routenkonfiguration

3.3.3.5 Analoge Teilnehmer (Mediatrix 41xx)

An einem Mediatrix 41xx Gateway können analoge Teilnehmer für den Dienst „Sprache“ oder „Fax“ eingerichtet werden.

IMPORTANT: Für dieses Gerät ist nur DGW-Firmware freigegeben. Bei Verwendung von SIP-Firmware besteht ein hohes Risiko, dass einige Ihrer Szenarien nicht funktionieren.

Analoge Teilnehmer eines Mediatrix 41xx Gateways müssen in der OpenScape 4000 als SIP-Teilnehmer eingerichtet sein.

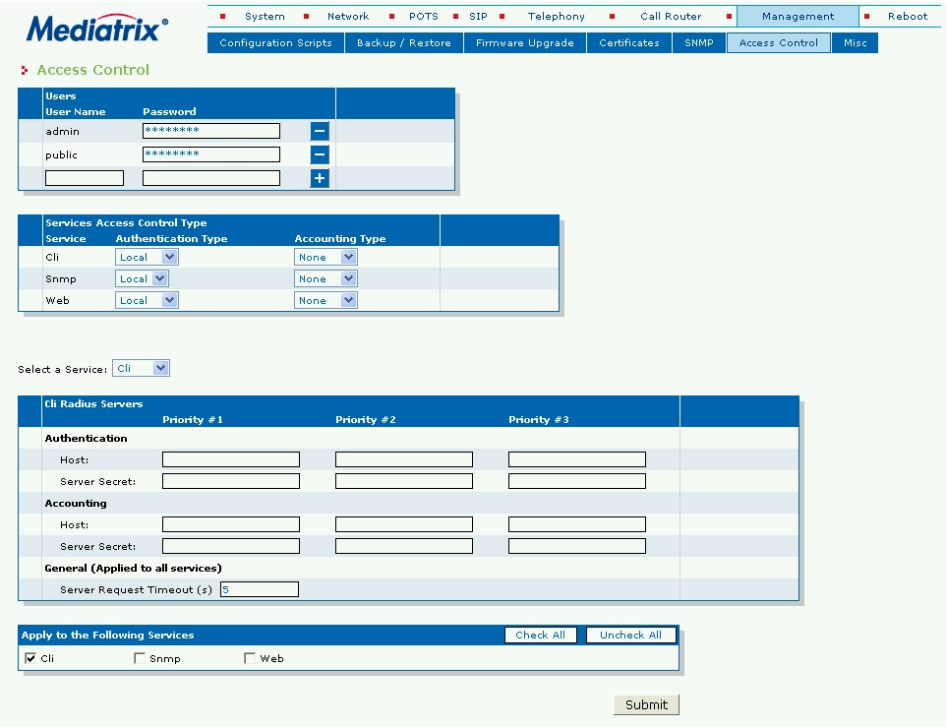
Beispiel:

```
ADD-SBCSU:STNO=25030,OPT=OPTI,CONN=IP2,PEN=1-50-3-0,
DVCFIG=UFIP,TSI=1,COS1=2,COS2=2,LCOSV1=1,LCOSV2=1,LCOSD1=1,
LCOSD2=1,DPLN=0,ITR=0;
```

IMPORTANT: Das DGW Mediatrix arbeitet in den Standardeinstellungen nicht ordnungsgemäß. Daher müssen einige der Parameter von Hand geändert werden. Bitte beachten Sie die Abschnitte SIP->Server, SIP->Registrations, SIP->Interop und SIP->Transport.

Management > Access Control

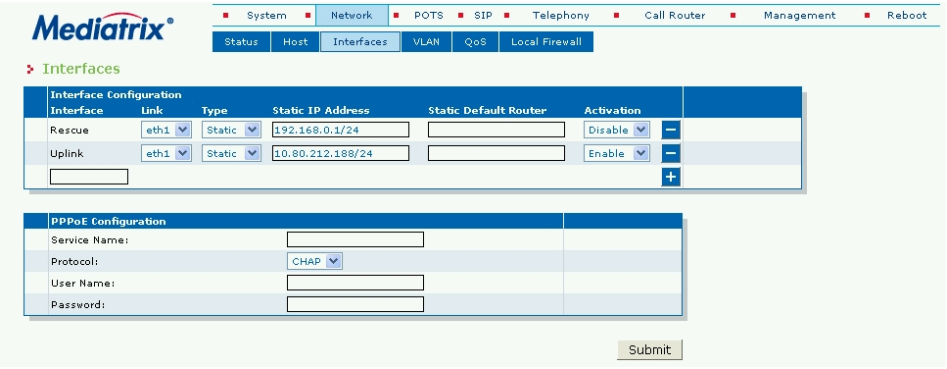
Richten Sie die Parameter für die Leitungsadministration und ##public ein.



Mediatrix 41xx – Management -> Access Control

Network -> Interfaces

In diesem Fenster richten Sie die Parameter der Netzwerkeinstellungen ein. Konfigurieren Sie die IP-Adresse, die Subnetzmaske, den Standard-Router und den SNMP-Port.



Mediatrix 41xx – Network -> Interfaces

Network -> Host

In diesem Fenster richten Sie die Parameter der Netzwerkeinstellungen ein. Konfigurieren Sie den Standard-Router, DNS, SNTP.

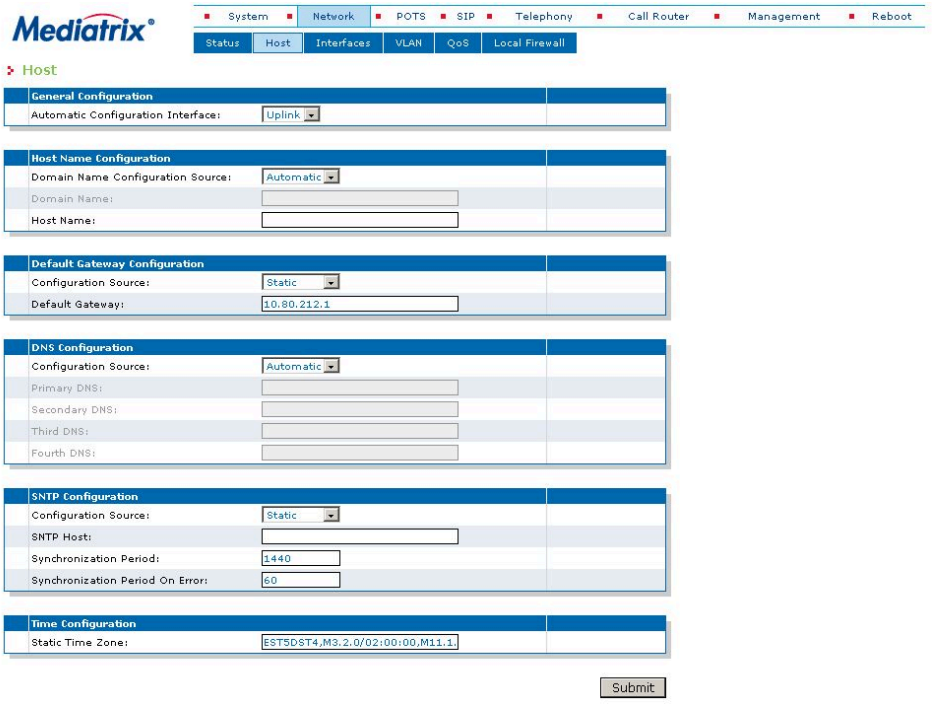
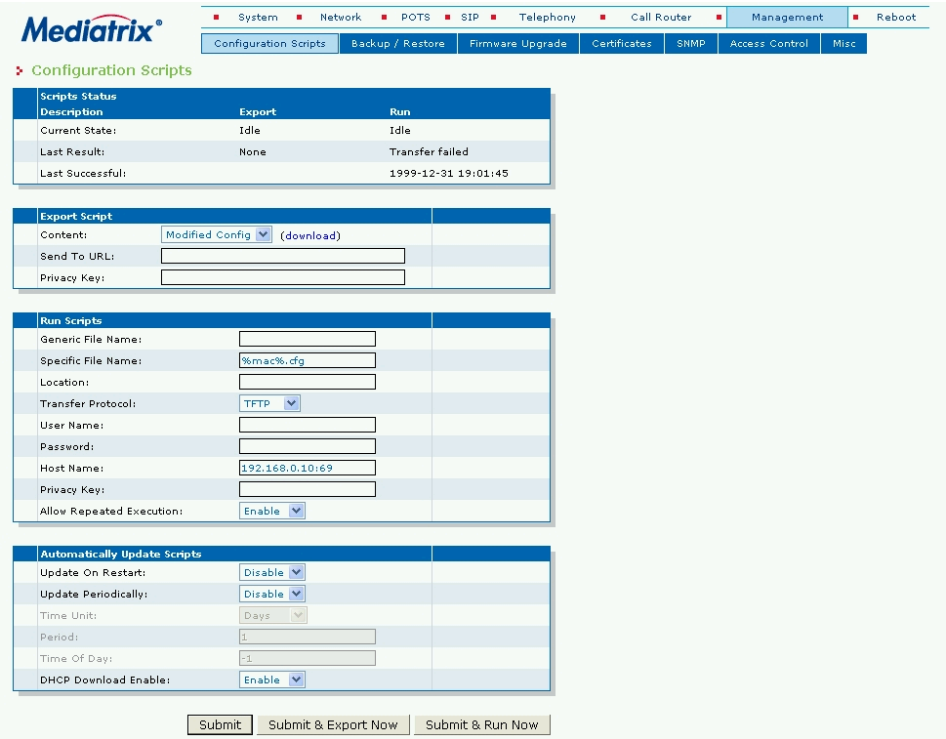


Figure 59: Mediatrix 41xx – Network -> Host

Management > Configuration Scripts

In diesem Fenster werden die Download-Parameter für die Konfigurationsskripts verwaltet.

Geben Sie die Werte für den Configuration File Server ein.



Mediatrix 41xx – Management -> Configuration Scripts

Management -> Firmware upgrade

In diesem Fenster werden die Download-Parameter für die Firmware verwaltet.

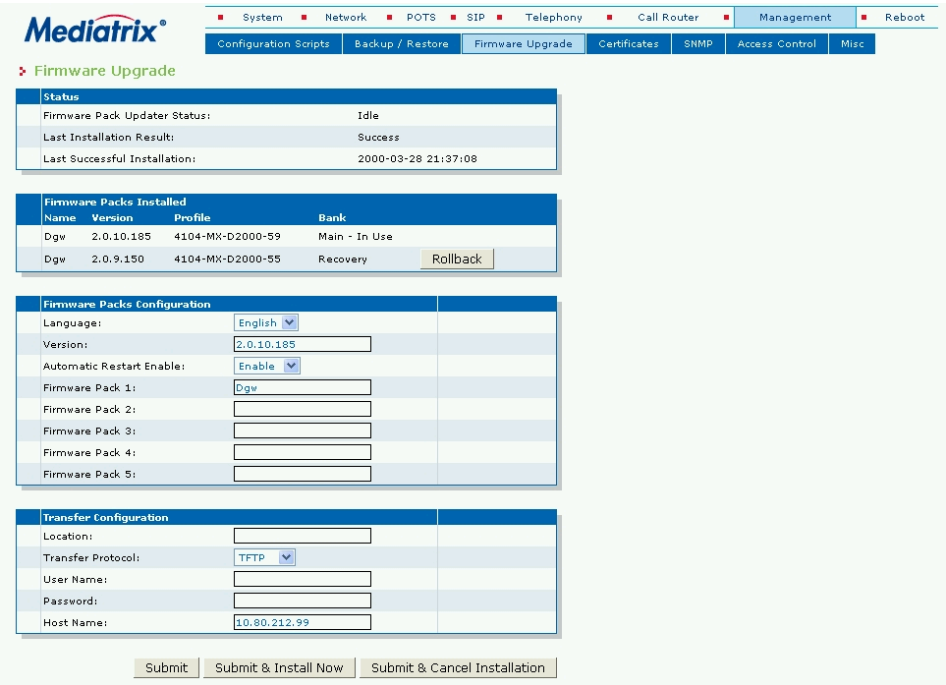


Figure 60: Mediatrix 41xx – Management -> Firmware Upgrade

SIP -> Servers

In diesem Fenster werden die Parameter für die SIP-Server verwaltet. Geben Sie die IP-Adresse des SIP-Servers an.

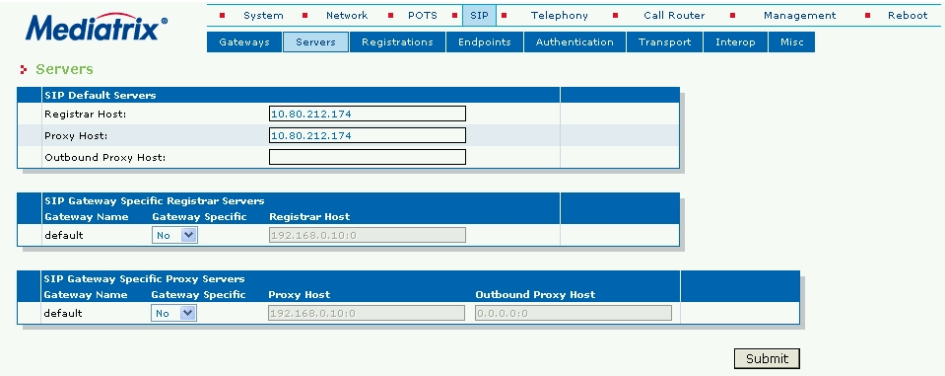
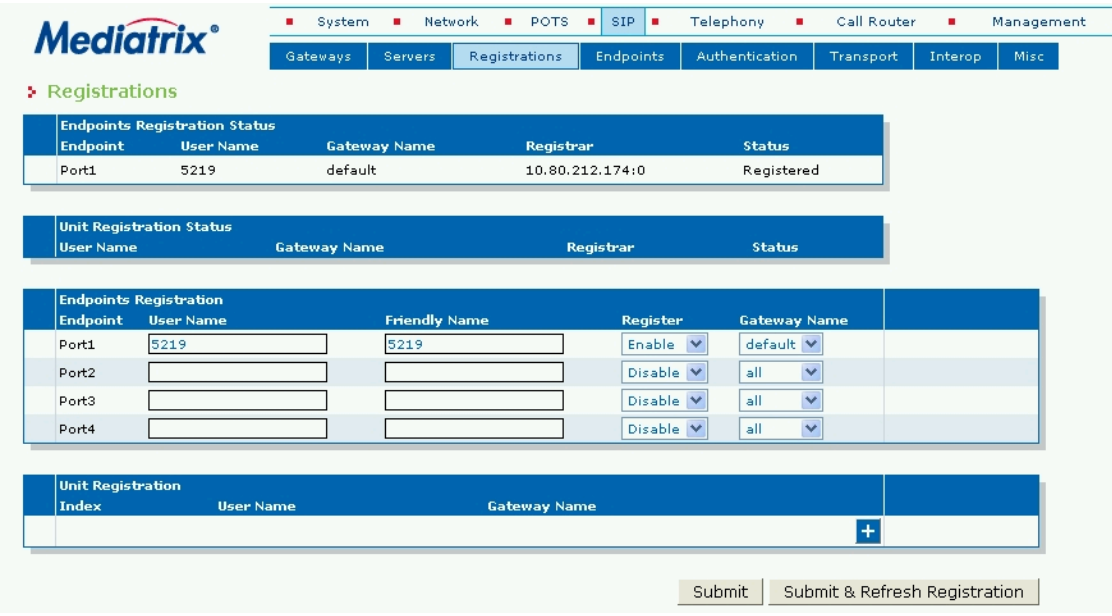


Figure 61: Mediatrix 41xx – SIP -> Servers

SIP -> Registrations

In diesem Fenster werden die Parameter für die SIP-Teilnehmer verwaltet. Geben Sie für jeden Teilnehmer die Rufnummer und den Namen ein. Diese Daten werden auch für die Anzeige der Rufnummernidentifikation (Caller-ID Information) verwendet.



Mediatrix 41xx – SIP -> Registrations

SIP -> Interop

Für die ordnungsgemäße Funktion des Mediatrix 41xx sollten Werte in den Feldern 406 und 488 eingestellt werden (Use Previous Media Negotiation).

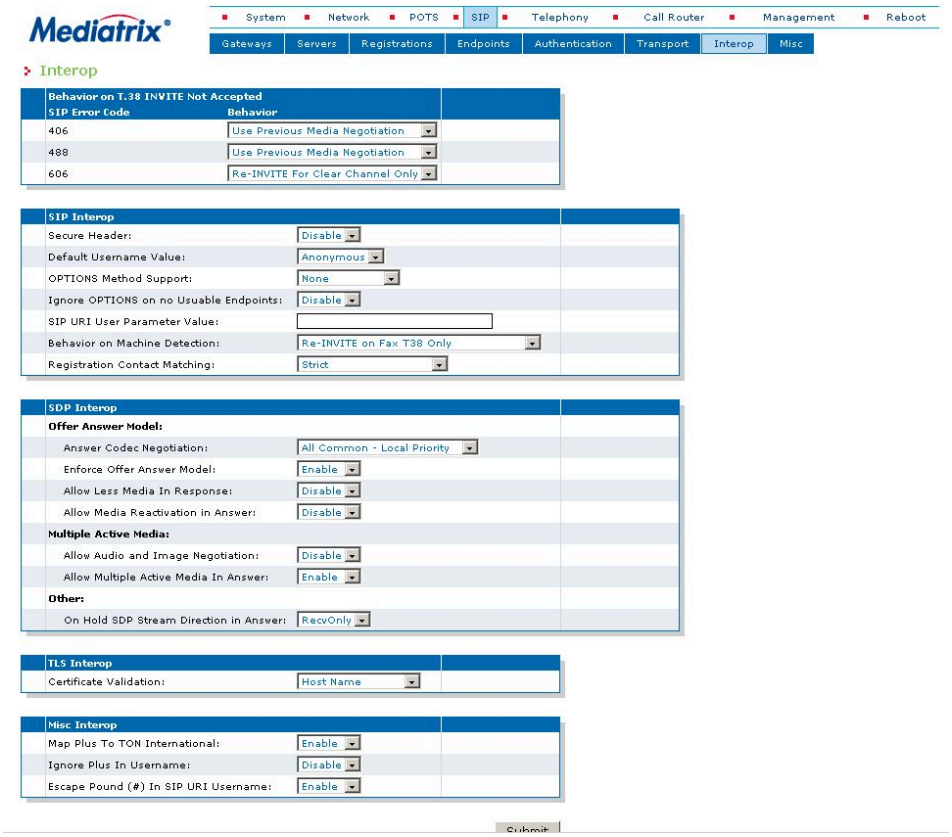


Figure 62: Mediatrix 41xx – SIP -> Interop

SIP -> Transport

Für die ordnungsgemäße Funktion des Mediatrix 41xx sollten die Werte für Transport auf „Enable“ eingestellt werden.



Figure 63: Mediatrix 41xx – SIP -> Transport

Telephony -> Codecs

In diesem Fenster (Screenshots der drei folgenden Bilder) werden Codec-Parameter eingestellt. Der bevorzugte Codec ist G.711 a-Law.

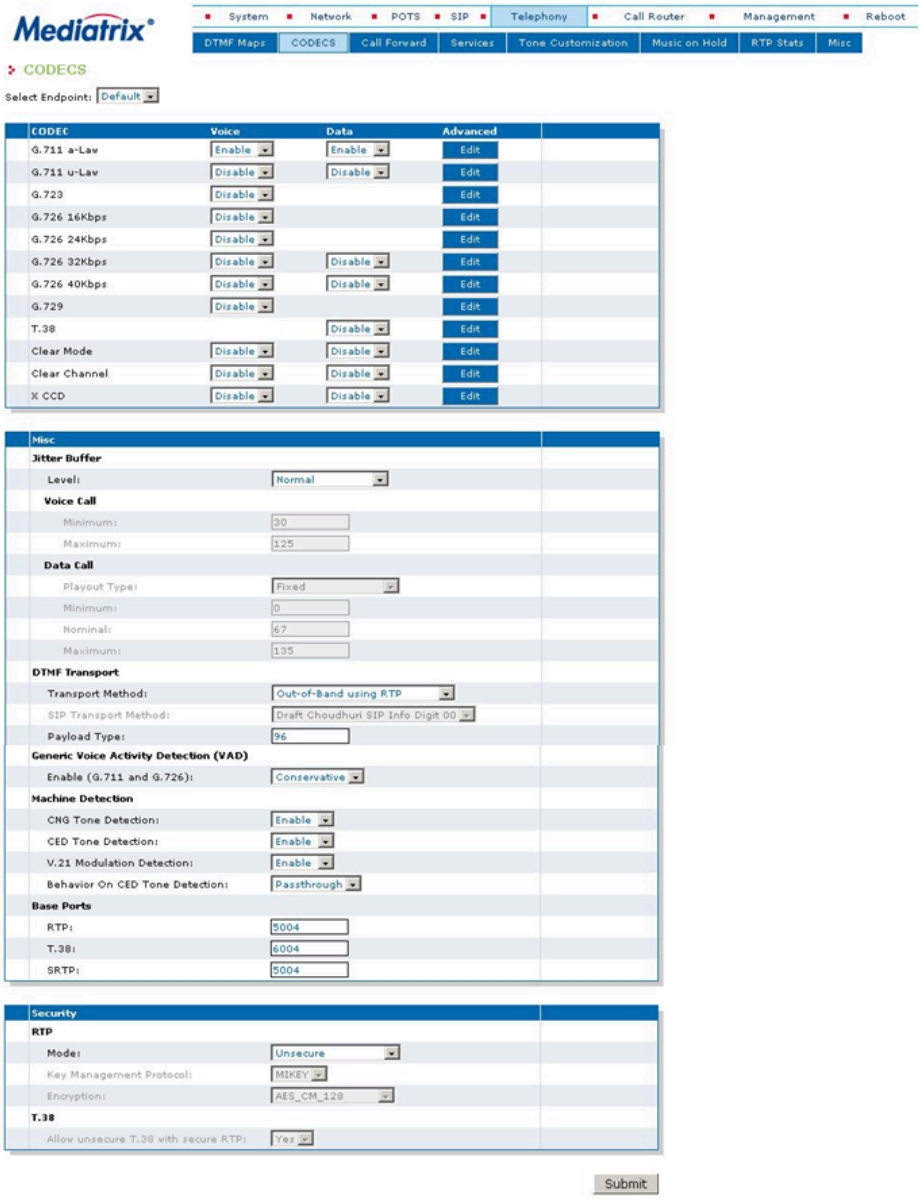


Figure 64: Mediatrix 41xx – Telephony -> Codecs

Wenn mehr als ein Codec erlaubt sein muss, kann die Priorität der einzelnen Codecs unter der Schaltfläche **Edit** eingestellt werden. Zulässig sind Werte im Bereich zwischen 0 (niedrigste Priorität) und 10 (höchste Priorität).



Mediatrix 41xx – Telephony -> Codecs

Telephony -> Misc

In diesem Fenster werden Ländereinstellungen und die Einstellungen der kundenspezifischen Wähltöne verwaltet.

- Ländereinstellung Germany 1 = andauernder Wählton
- Ländereinstellung Germany 2 = unterbrochener Wählton (3 kurze „Beeps“)



Figure 65: Mediatrix 41xx – Telephony -> Misc

3.3.3.6 Analog Trunking (Mediatrix 1204)

OpenScape 4000 SoftGate 50 > SIP-Amtsleitung > Mediatrix 1204 > Analoge Amtsleitung

3.3.3.6.1 Konfiguration auf OpenScape 4000

Überblick

- SoftGate 50 (SOCO) vIPDA Shelf 50, Direct Link-Konfiguration mit 120 B-Kanälen
- EBT 8, vSIP 04-Amtsleitung zu Mediatrix 1204 (SIP <==> Telco Analogleitung)
- NCUI-Konfiguration, LTU 50
- vSIP-Amtsleitung zu Mediatrix 1204 (SIP <==> Telco Analogleitung)
- Mediatrix 1204 AMO-Konfiguration
- Einstellen des Mediatrix-Proxy (ip 57) in OpenScape 4000 / SoftGate 50 / WBM SIP-Amtsleitung (ip 58)
- LCR-Einstellungen

SoftGate 50 (SOCO) vIPDA Shelf 50, Direct Link-Konfiguration mit 120 B-Kanälen

```
EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=50,LTSACHNR="Q2329-",SRCGRP=50,FRAMETYP=SO▶
COAP,VERBART=APDL,LSRTADR=155.75.27.50,APRTADR=155.75.27.1,STANDOID=050,STAN▶
DORT="DIRECT LINK, CPCI#2",TEL=9727145968,PLCHECK=JA,ANZBKAN=120,KON▶
VLAW=NEIN,TCLASS=0,ALARMNR=0,SOCOTYP=SOCO50;
```

EBT 8, vSIP 04-Amtsleitung zu Mediatrix 1204 (SIP <==> Telco Analogleitung)

```
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=50,EBT=8,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR=0,FCTBLK=59,BKAN3550=4,ALARMNR=0;
```

NCUI-Konfiguration, LTU 50

```
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=GLOBAL,MUSTER=255;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=IFDATA,VLAN=NEIN,TOSLAN=72,TOSMO▶
DEM=80,VLANID=0,BITRATE=100MBFD;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=DSP,JITBUFD=60;
AENDERN-STMIB: MTYP=NCUI2,LTU=50,TYP=SERVIF,LOGINTRM="TRM",LOGINPPP="PPP";
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=SIGQOS,BANDW=0,MAX▶
RTD=0,MINTHRPT=0,SIGPTHSW=STD,QOSSTAT=NEIN;
AENDERN-
```

```
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,TOSPL=48,T38FAX=JA,RFCFMOIP=JA,RF
CDTMF=JA,REDRFCTN=JA,PRIO=PRIO1,CODEC=G729,VAD=NEIN,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO2,CODEC=G729A,VAD=NEIN,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO3,CODEC=G711U,VAD=NEIN,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO4,CODEC=G711A,VAD=NEIN,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO5,CODEC=G729B,VAD=JA,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO6,CODEC=G729AB,VAD=JA,RTP=20;
AENDERN-
STMIB:MTYP=NCUI2,LTU=50,TYP=ASC,UDPPRTLO=29100,T38FAX=JA,RFCFMOIP=JA,RFCDTMF=JA,
REDRFCTN=JA,PRIO=PRIO7,CODEC=NEINNE,VAD=NEIN,RTP=20;
```

REDRFCTN	Redundante Übertragung der RFC2833 Töne nach RFC2198
RFCDTMF	Übertragung von DTMF Tönen nach RFC2833
RFCFMOIP	Übertragung von Fax/Modem Tönen nach RFC2833

Wichtig: Die oben genannten Parameter müssen in allen IPDA-Gateways (STMI2/4/X (vSTMI) respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

```
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=H323,Q931T1=50,Q931T2=500,GWNAME="HG3575-2";
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=DMCDATA,DMCALLWD=NEIN,DMCCONN=0;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=SNMP,CS1="public";
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=MGNTDATA,MGNTPN=8000,BUSPN=443;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLLE=ING;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=WBMDATA,LOGINWBM="HP4K-SU",ROLLE=SU;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLLE=ADMIN;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=WBMDATA,LOGINWBM="HP4K-READER",ROLLE=READON►
LY;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=GWSECTOR,GWSECTNO=0;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=DLSDATA,DLSIPADR=192.0.2.40,DL►
SPORT=18443,DLSACPAS=NEIN;
AENDERN-STMIB:MTYP=NCUI2,LTU=50,TYP=SOCODATA,CLAIPADR=155.75.27.50;
```

vSIP-Amtsleitung zu Mediatrix 1204 (SIP <==> Telco Analogleitung)

```
EINRICHTEN-CGWB:LTU=50,EBT=8,SMODE=NORMAL,IPADR=155.75.27.58,NET►
MASK=255.255.255.0;
AENDERN-
CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=GLOBIF,MUSTER=255,VLAN=NEIN,VLANID=0,DEFRT=155.75
.27.1,BITRATE=100MBFD,TRPRSIP=4,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TLSP=4060,DNSI►
PADR=0.0.0.0;
```

```
AENDERN-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=SERVIF,LOGINTRM="TRM";
AENDERN-
CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=ASC,UDPPRTLO=29100,TOSPL=48,TOSSIGNL=184,T38FAX=J
A,RFCFMOIP=JA,RFCDTMF=JA,REDRFCTN=JA,PRIO=PRIO1,CODEC=G729,VAD=NEIN,RTP=20;
```

REDRFCTN	Redundante Übertragung der RFC2833 Töne nach RFC2198
RFCDTMF	Übertragung von DTMF Tönen nach RFC2833
RFCFMOIP	Übertragung von Fax/Modem Tönen nach RFC2833

Wichtig: Die oben genannten Parameter müssen in allen IPDA-Gateways (STMI2/4 (vSTMI) respektive AMO CGWB & NCUI2+/4 respektive AMO STMIB) den gleichen Wert haben. Damit werden Probleme vermieden und es wird eine einheitliche Funktion anlagenweit erreicht!

```
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=ASC,PRIO=PRIO2,CO►
DEC=G729A,VAD=NEIN,RTP=20;
AENDERN-CGWB:MTYPE=CGW,LTU=50,EBT=8,TYP=ASC,PRIO=PRIO3,CO►
DEC=G711U,VAD=NO,RTP=20;
AENDERN-CGWB:MTYPE=CGW,LTU=50,EBT=8,TYP=ASC,PRIO=PRIO4,CO►
DEC=G711A,VAD=NEIN,RTP=20;
AENDERN-CGWB:MTYPE=CGW,LTU=50,EBT=8,TYP=ASC,PRIO=PRIO5,CO►
DEC=NONE,VAD=NEIN,RTP=20;
AENDERN-CGWB:MTYPE=CGW,LTU=50,EBT=8,TYP=ASC,PRIO=PRIO6,CO►
DEC=G729B,VAD=JA,RTP=20;
AENDERN-CGWB:MTYPE=CGW,LTU=50,EBT=8,TYP=ASC,PRIO=PRIO7,CO►
DEC=G729AB,VAD=JA,RTP=20;
AENDERN-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=DSP,JITBUFD=60;
AENDERN-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=MGNTDATA,MGNTPN=8000,BUSPN=443;
AENDERN-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=DMCDATA,DMCCONN=4;
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=WBMDATA,LOGINWBM="HP4K-DEVEL",ROLE=ENGR;
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=WBMDATA,LOGINWBM="HP4K-SU",ROLE=SU;
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=WBMDATA,LOGINWBM="HP4K-ADMIN",ROLE=AD►
MIN;
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=WBMDATA,LOGINWBM="HP4K-READ►
ER",ROLE=READONLY;
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=GWDATA,GWID1="PRIMARYRASMANAGERID";
AENDERN-CGWB:MTYP=CGW,LTU=50,SLOT=8,TYP=H235DATA,SECSUBS=NEIN,SECTRNK=NEIN,GLO►
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-161-43-0-70-36-
218-74-169-221-78-102-174-170;
AENDERN-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=SIPTRERH,GWAUTREQ=NEIN;
AENDERN-
CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=SIPTRSSA,SIPREG=NEIN,REGIP1=0.0.0.0,PORTTCP1=5060
,PORTTLS1=5061,REGTIME=120,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS2=5061;
AEND-CGWB:MTYP=CGW,LTU=50,EBT=8,TYP=DLSDATA,DLSIPADR=192.0.2.40,DL►
SPORT=18443,DLSACPAS=NEIN;
```

Mediatrix 1204 AMO-Konfiguration

```
EINRICHTEN-BUEND:BUNUM=58,NAME="MEDIATRIX_1204 ",ANZ=8,ANZFANG=0,ANZACD=*,PRIO►
NUM=1,TDDRFLAG=ON,GDTRRULE=0,ACDPMGRP=0,ZEICHUM=NEUTRAL;
EINRICHTEN-TDCSU:ART=NEU,LAGE=1-50-008-0,COTNR=59,CO►
PNR=59,WABE=0,VBZ=0,COS=59,LCOSS=1,LCOSD=1,SATZNR="",ZLNR=58,PROTVAR=ECMAV2,SEGM
```

```
ENT=8,DEDSVC=KEINE,TRTBL=GDTR,SIDANI=N,TREFTYP=AMT,CBMATTR=KEINE,TCHARG=N,ANZUNT
=0,TRACOUNT=31,SATCOUNT=VIELE,KNNR=58,ALARMNR=2,FIDX=1,CARRIER=1,ZONE=LEER,COTX=
59,AULX=1,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWMUXTIM=10,SRCGRP=50,CLASSMRK=EC&
G711&G729AOPT,BUNR=58,SUCHART=ZYK,INBETR=J,SECLEVEL=SECURE,GER=HG3550CO,BKANAL=1
&&4,BKVER=N,BKGR=1,LWPAR=2,LWPP=0,LWLT=0,LWPS=0,LWR1=0,LWR2=0,DMCERL=N;
EINRICHTEN-
COT:COTNU=59,COTPAR=PRI&RCL&ANS&KNOR&CEBC&CBBN&CBFN&FWDN&FNAN&COTN&BSHT&BLOC&PRO
V&ATRS&TSCS&ICZO&TRSC&CFOS&CFVA&PINR&AOCC&BCNE&NTON;
```

Einstellen des Mediatrix-Proxy (ip 57) in OpenScape 4000 / SoftGate 50 / WBM SIP-Amtsleitung (ip 58)

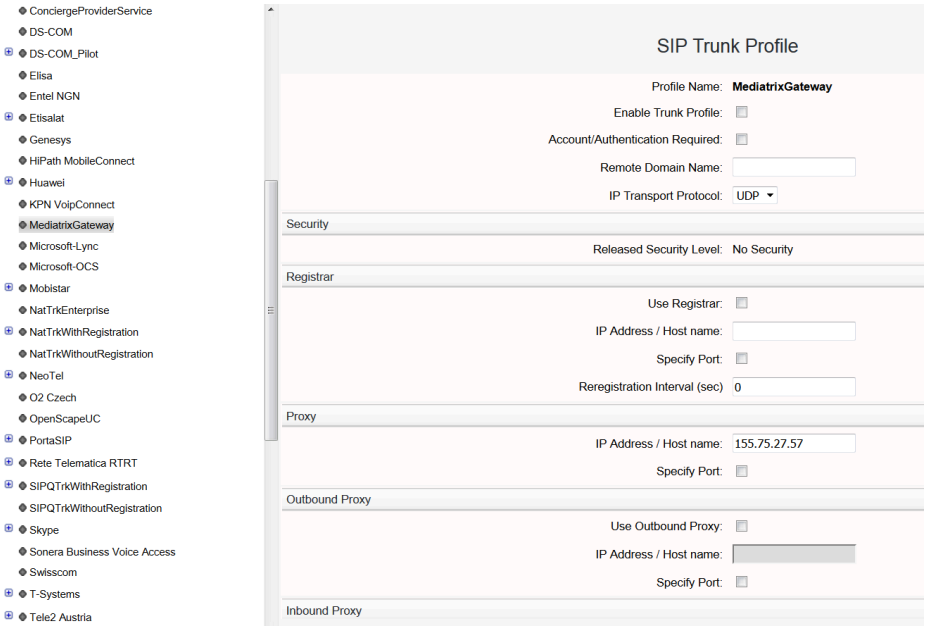


Abbildung 66: Mediatrix 1204 Gateway - WBM - SIP-Amtsleitungsprofil

Der MediatrixGateway-Ordner sollte aktiviert werden, rechter Mausklick > EINSCHALTEN ==> Ordner wird grün.

LCR-Einstellungen

AMO WABE - Kennziffer für abgehende Verbindungen durch Mediatrix 1204

```
EINRICHTEN-WABE:RNR=958,KZP=QUER,PRUEF=N;
```

AMO LDPLN

```
EINR-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=958-W-Z,PROFIDX=58,LBER=1,PINDP=N;
```

W	zweiter „externer“ Wählton
Z	beliebige Ziffernfolge, maximal 22 Ziffern, beendet mit Zeitüberschreitung oder Ersatzzeichen „#“ (Raute) am Anschluss
LWM	Wenn Telco auf 10 Ziffern eingestellt ist, LDP = 958-W-XXXXXXXXXX

AMO LPROF

```
EINRICHTEN-LPROF:PROFNAME="SIP TRK SG 50-8",SRCGRP=1&25&50,LRTG=958,PROFIDX=58;
```

AMO LDAT - CDR-Attribut und PUBNUM von Anschluss senden

```
EINRICHTEN-LDAT:LRTG=958,LDIENST=ALLE,LWERT=1,BUNUM=58,LWR=959,LBER=1,CARRI▶
ER=1,ZONE=LEER,LATTR=WCHREG&PUBNUM,VCCYK=4;
```

AMO LODR - Echofeld 3 = Z aus „958-W-Z“

```
EINRICHTEN-LODR:LWR=959,LWREL=ECHOFELD,FELD=3;
EINR-LODR:LWR=959,LWREL=NPI,NPI=UNKNOWN,TON=UNKNOWN;
EINRICHTEN-LODR:LWR=959,LWREL=ENDE;
EINRICHTEN-LODR:LWR=959,INFO="SIP TRK SG 50-9";
```

AMO RICHT

```
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=958,LDIENST=ALLE,NAME="MEDTRX1204 508",BU►
NUM=58,ZKNNR=58,ROUTATT=JA,EMCYRTT=NEIN,PZKNNR=0,ZEICHUM=NEUTRAL,CONFTON=NEIN,RE
RINGRP=NEIN,KPRCAUL=NEIN,KATG=NEIN,CLNAMEDL=NEIN,FWDSWTCH=NEIN,LINFNOT=NEIN,KIN►
TRRTE=NEIN;
```

3.3.3.6.2 Hinweise zur Konfiguration

Standardmäßig ist MDX1204 auf DHCP eingestellt. Ermitteln Sie die von DHCP an MDX zugewiesene IP anhand eines Wireshark oder Ethereal Sniffer-Trace am gespiegelten Port der Datenanlage des Kunden, oder fragen Sie bei seiner IT-Abteilung nach. Im Recovery-Modus verwendet das Mediatrix 1204 die Standard-IP-Adresse 192.168.0.1.

Überblick

- LAN-Einstellungen bei fester IP 155.75.27.57
- Allgemeine Konfiguration von Mediatrix 1204
- Konfiguration mit Mediatrix Software Unit Manager Express (UME)
- Mediatrix 1204 Firmware-Upgrade

LAN-Einstellungen bei fester IP 155.75.27.57

Management > Netzwerkeinstellungen

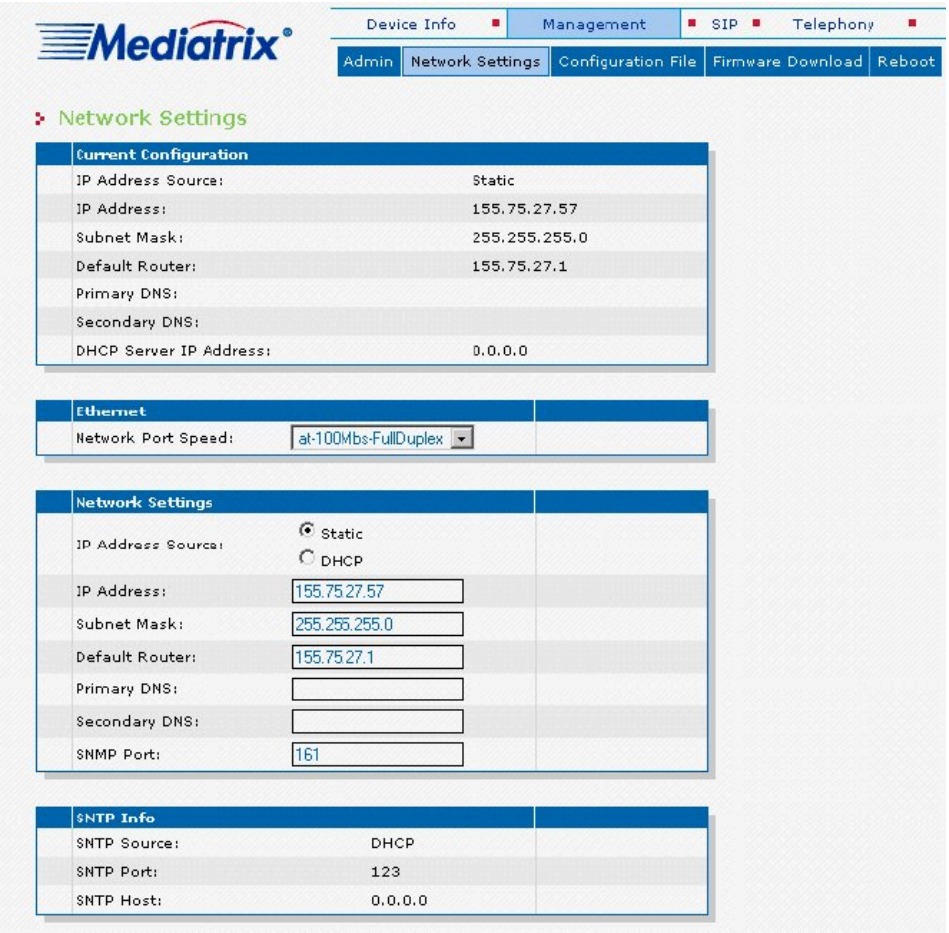


Abbildung 67: Mediatrix 1204 Gateway - LAN-Einstellungen

Allgemeine Konfiguration von Mediatrix 1204

Mediatrix 1204 zeigt auf OpenScape 4000 SoftGate 50 SIP-Amtsleitung (AMO BCSU, PEN 1-50-8-0 = IP 155.75.27.58)

Port-Benutzername = Telco Analog Trunk

Nach dem Anschluss an den MDX-Port wird bei ankommenden Telco-Anrufen auf Leitung 1 im Display der Teilnehmer 1234567890 angezeigt.

Bei ankommenden Anrufen auf Leitung 4 wird im Display der OpenScape 4000-Teilnehmer 333004 angezeigt; der Anruf wird auf Leitung 4 angenommen.

Außerdem verwendet auf SIP: Invite 333004@ip_addr.

Management > Konfigurationsdatei

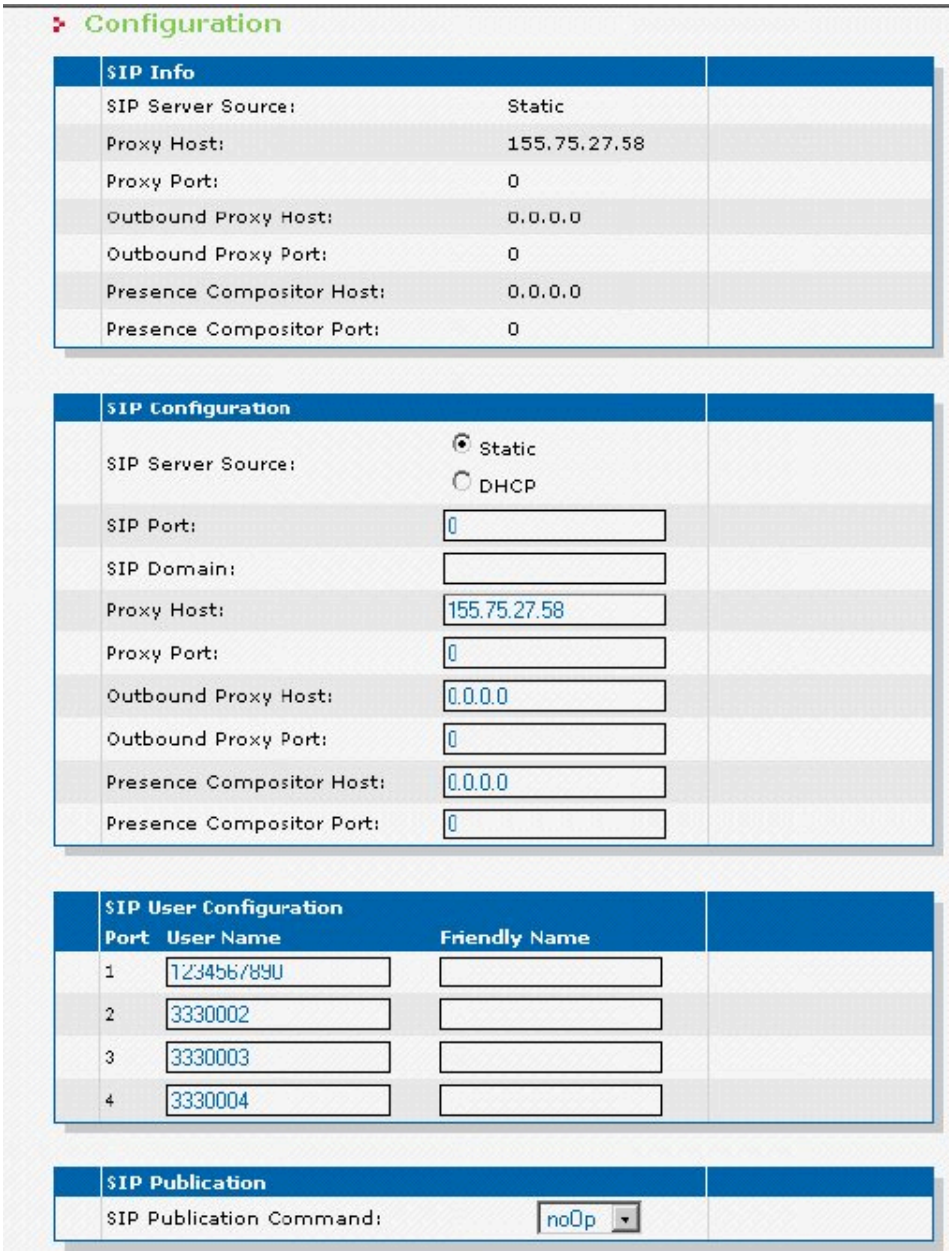


Abbildung 68: Mediatrix 1204 Gateway - Konfiguration

Konfiguration mit Mediatrix Software Unit Manager Express (UME)

Die folgenden Änderungen an MDX1204 erfordern die Installation der Mediatrix-Software **UMN** (**U**nit **M**anager **N**etwork) auf Ihre, PC. Sie finden diese Software unter **SWS > Partner Products > Mediatrix 1204** oder im Internet (http://www.media5corp.com/support/mediatrix--media5boss/downloads). Die Dokumentation kann im DMS oder auf der MDX-Website abgerufen werden.

Der **UME** (**U**nit **M**anager **E**xpress) ist ein Unterprogramm von UMN.

Bei einem rechten Mausklick auf das Feld **fxoIfAnalogLineType** wird Folgendes angezeigt:

1) Get = Parameter abrufen und anzeigen.

- Set = Geänderten Parameter an MDX senden.
- mx1204_MIB_line_type_change_set = Analoge Telco-Amtsleitung LS oder GS auf Leitung 1 bis 4.

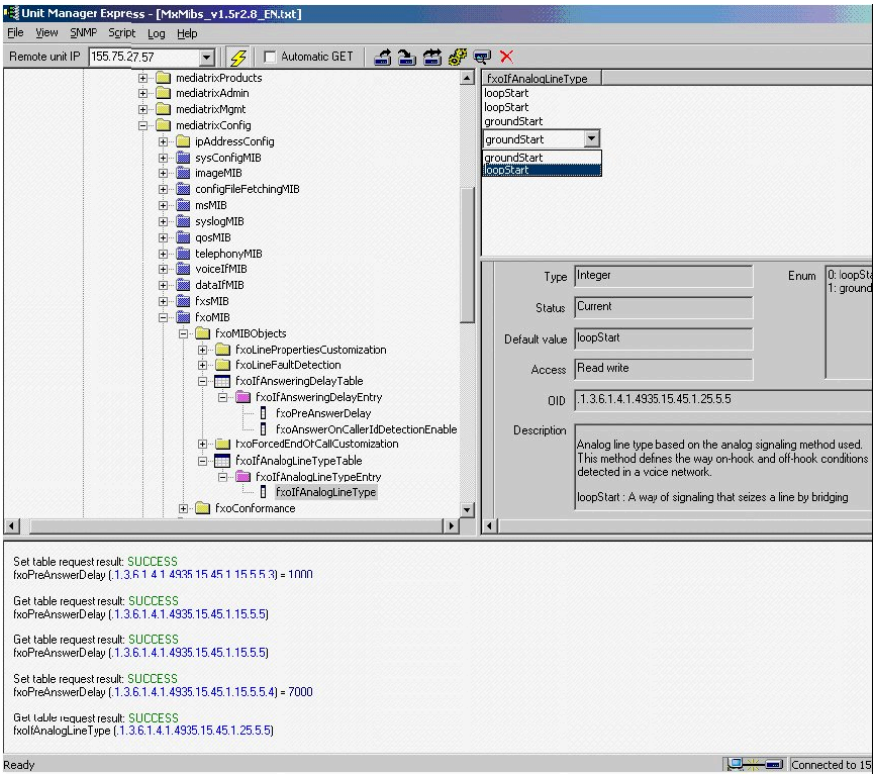


Abbildung 69: Mediatrix 1204 Gateway - Analoge Telco-Amtsleitung LS oder GS auf Leitung 1 bis 4

- mx1204_MIB_enable_incoming_ringing_direct_to_stn
- Auf den Leitungen 1 und 4 ankommende Anrufe werden direkt am OpenScape 4000-Anschluss gemeldet. Bei auf den Leitungen 2 und 3 ankommenden Telco-Anrufen legt MDX den zweiten Wählton an,

und der externe Anrufer wird nach Eingabe der OpenScape 4000-Teilnehmerrufnummer verbunden.

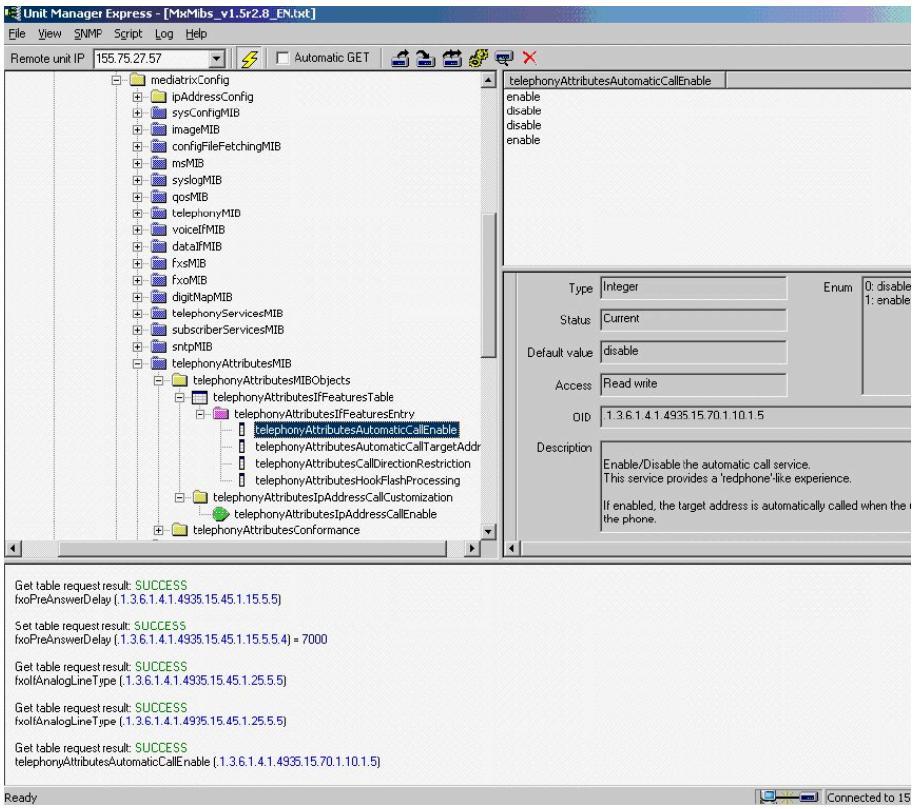


Abbildung 70: Mediatrix 1204 Gateway - Auf Leitung 1 und 4 ankommende Anrufe

Ein auf Leitung 1 ankommende Telco-Anruf wird am Anschluss 25015 gemeldet.

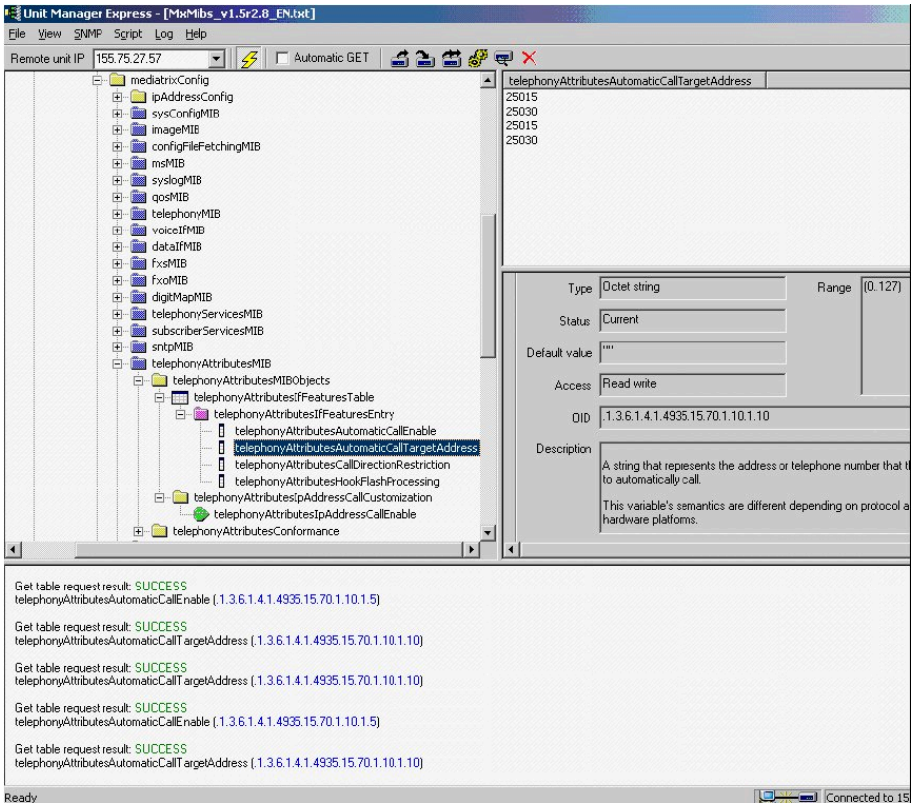


Abbildung 71: Mediatrix 1204 Gateway - Auf Leitung 1 ankommende Telco-Anrufe werden direkt zugestellt über Leitung 25015

- mx1204_MIB_delay_incoming_ringing

  Auf den Leitungen 1 und 4 ankommende Telco-Anrufe werden nach 1 Sekunde am OpenScape 4000-Anschluss gemeldet.

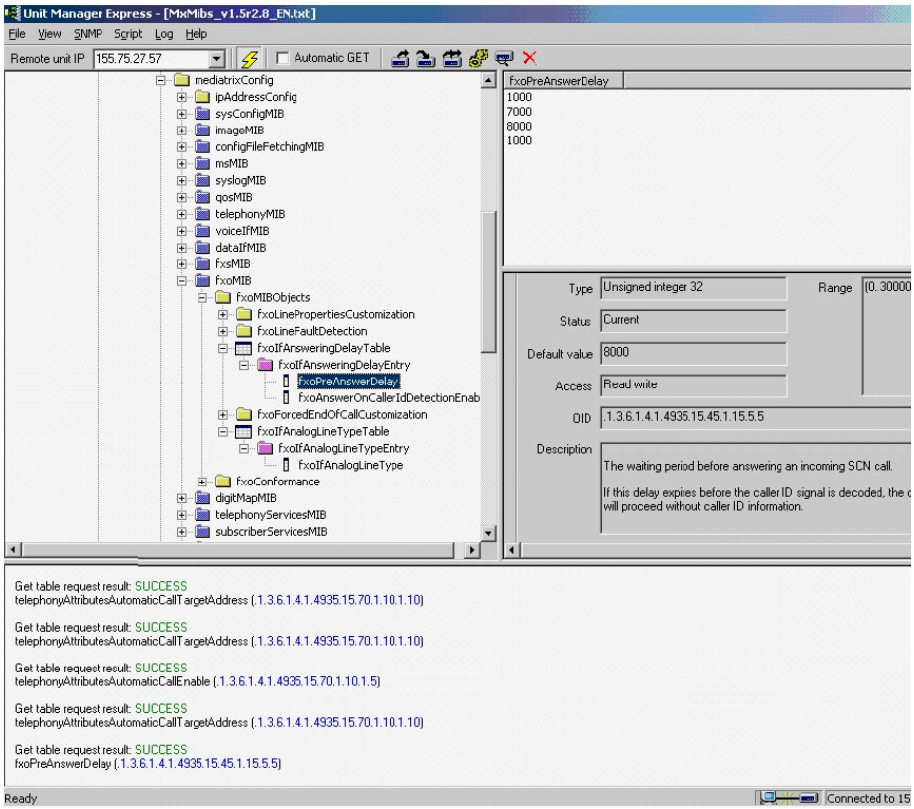


Abbildung 72: Mediatrix 1204 Gateway - Meldung ankommender Anrufe verzögern

Mediatrix 1204 Firmware-Upgrade

SW-Versionsupgrade auf:

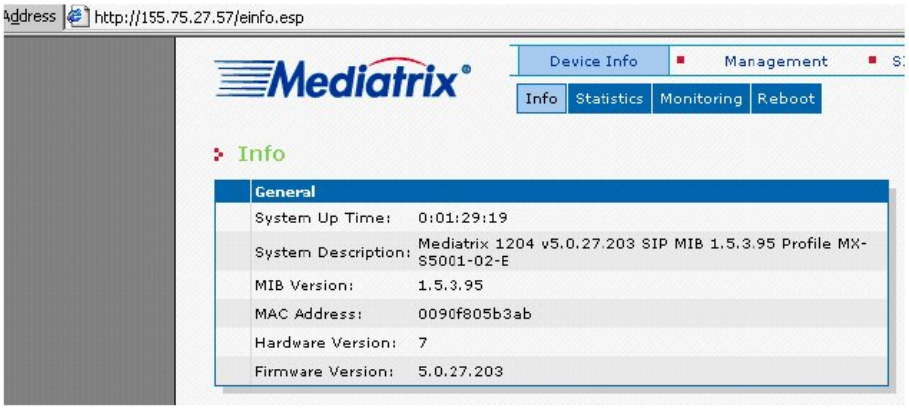


Abbildung 73: Mediatrix 1204 - Firmware

Vorgehensweise:

- Laden Sie die neue Version von der MDX-Website (http://www.media5corp.com/support/mediatrix--media5boss/downloads) herunter.

- Verwenden Sie eine TFTP-Software (z.B. 3CDaemon, kostenlos im Internet erhältlich)
- Extrahieren Sie die heruntergeladene Firmware-Datei in ein in TFTP eingestelltes Verzeichnis (in unserem Beispiel C:\Dokumente und Einstellungen\om837441\Eigene Dateien\0_Lixo\)

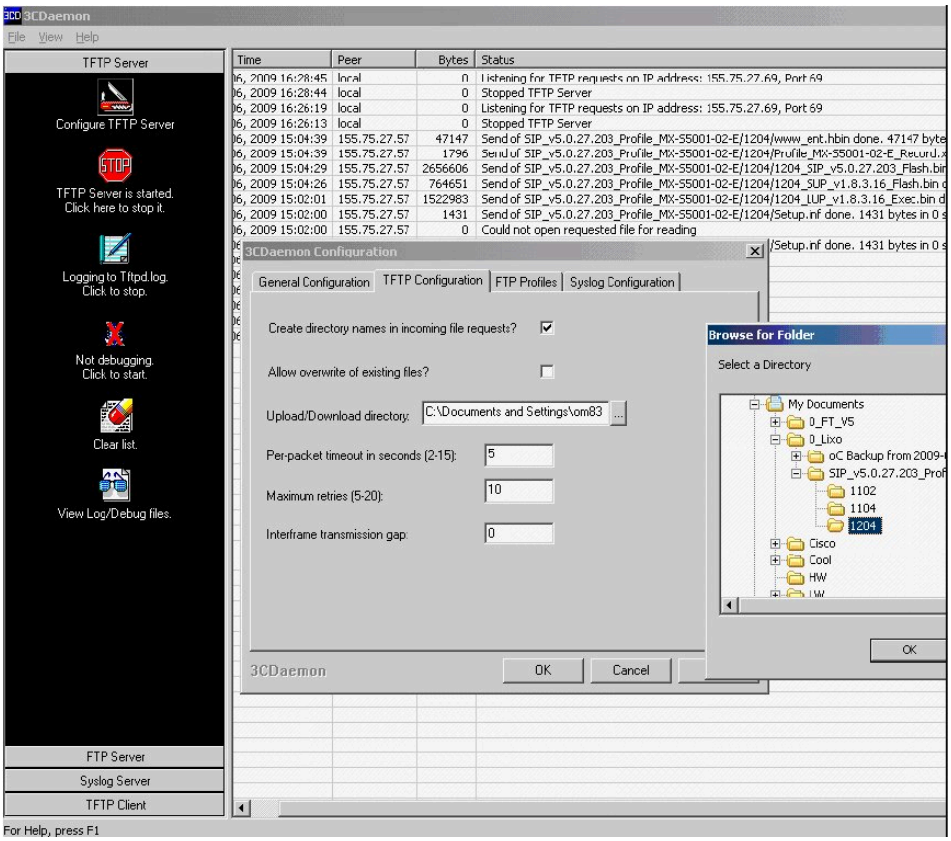


Abbildung 74: Mediatrix 1204 - Firmware-Download

In MDX ist als Server-Host Ihr PC mit der IP-Adresse 155.75.l27.69 angegeben, auf dem der 3CDaemon ausgeführt wird. Geben Sie den Speicherort der Firmware an. Der Status wird im Fenster „FW Download“ angezeigt.

Speicherort:

Hier ist nur der Name SIP_v5.0.27.203_Profile_MX-S5001-02-E\1204 in dem Verzeichnis erforderlich, in dem sich die Datei „Setup.inf“ nach dem Extrahieren befindet.

C:\Documents and Settings\om837441\MyDocuments\0_Lixo \SIP_v5.0.27.203_Profile_MX-S5001-02-E\1204

FW Download on Restart = REBOOT Im Mediatrix1204 und 3CDaemons-Protokoll wird die von Ihrem PC (IP.69) an MDX1204 (IP.57) übertragene Firmware (Send of Sip....) angezeigt - siehe 3CDaemon-Screenshot 15:02:00....

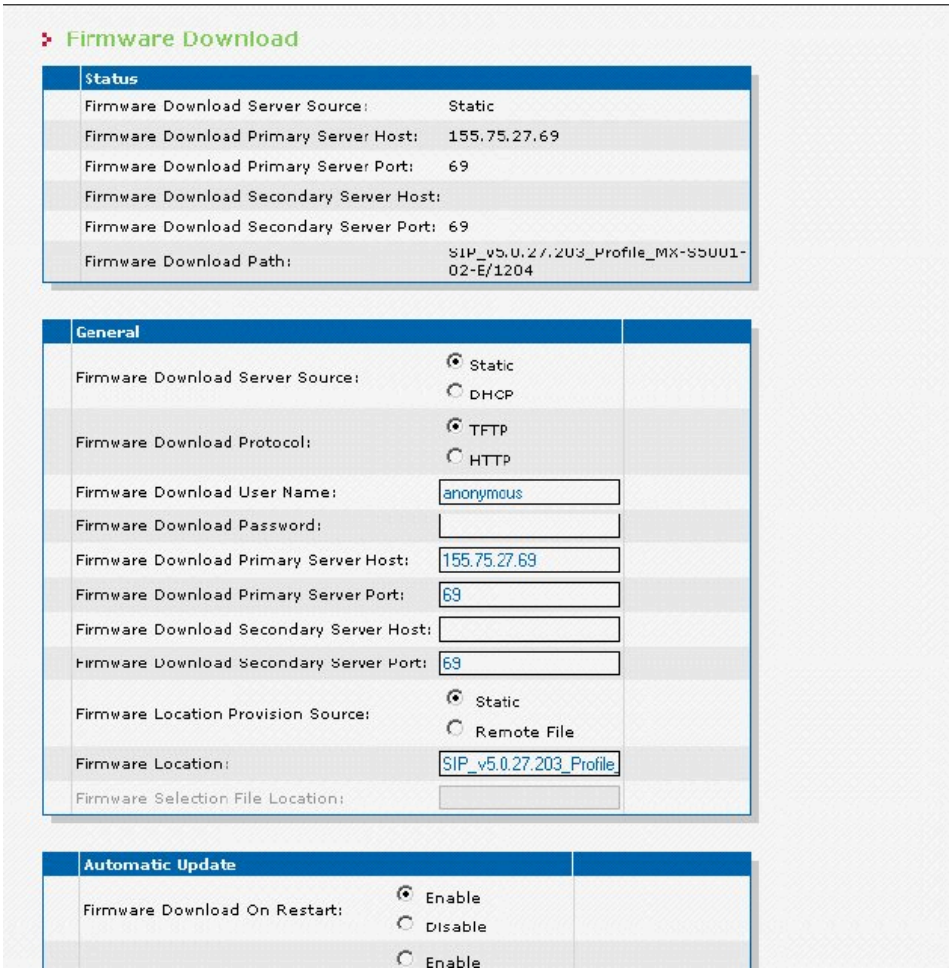
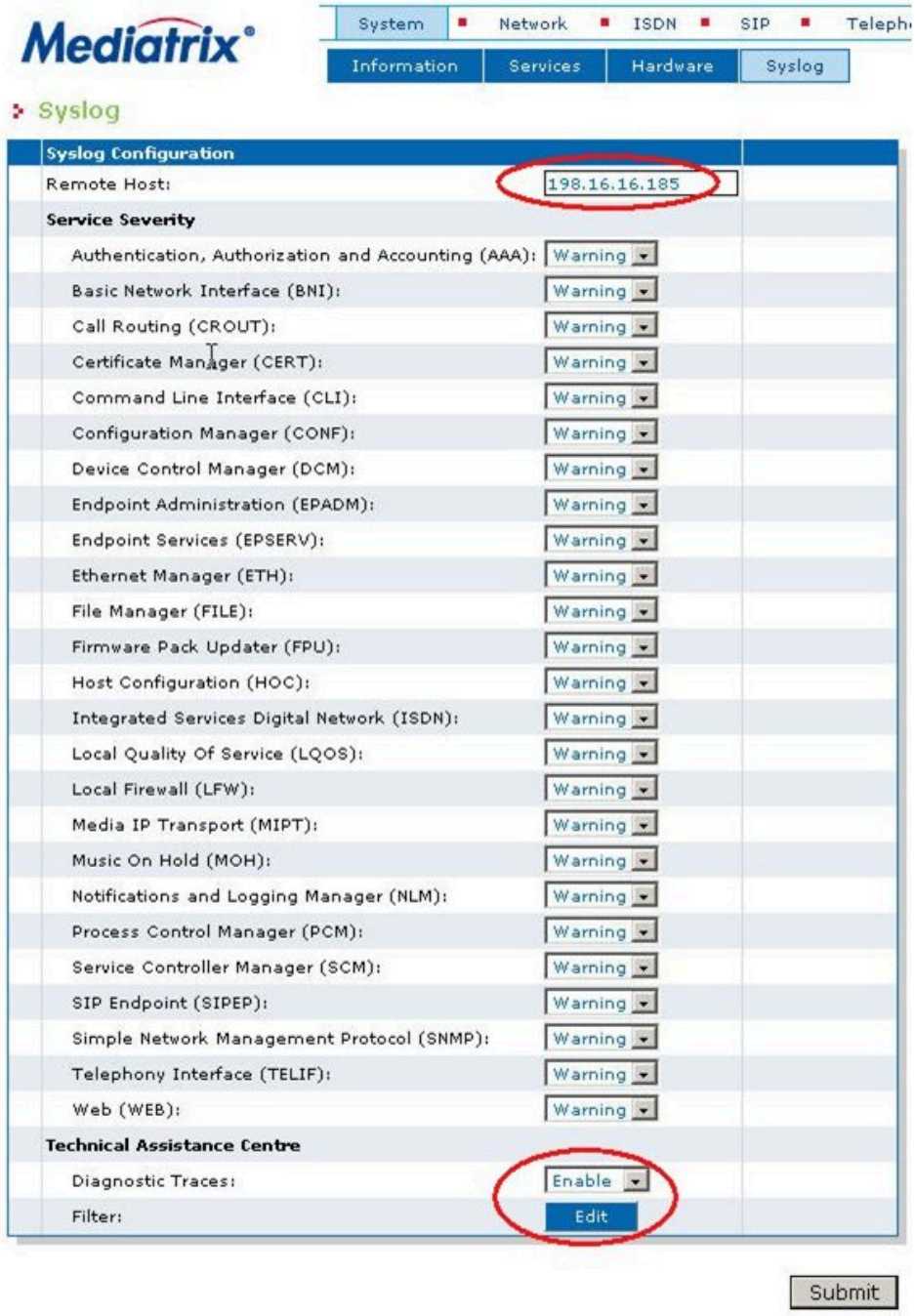


Abbildung 75: Mediatrix 1204 - Management > Firmware-Download

3.3.4 Fehlersuche mit syslog für Mediatrix 44xx und 36xx

Logging/Trace-Informationen oder Debugging-Meldungen werden an einen externen Syslog-Server gesendet. Hierfür muss ein Syslog-Server (z. B. 3CDaemon) erreichbar sein. Sie müssen den Syslog-Daemon-Server für die Erfassung dieser Meldungen konfigurieren. Geben Sie im Feld „Remote Host“ die Statische IP-Adresse oder den Domainnamen und die Portnummer des Geräts an, auf dem der Syslog-Server ausgeführt wird.

Wenn keine Syslog-Daemon-Adresse von einem DHCP-Server bereitgestellt oder vom Administrator festgelegt wird, werden keine Meldungen gesendet.



Syslog - System > Syslog > Diagnostic Traces

Legen Sie mithilfe der Dropdown-Menüs unter „Service Severity“ (Dienstschweregrad) fest, ab welchem Schweregrad eine Benachrichtigung an die verschiedenen Dienste gesendet wird.

Wenn Sie den Schweregrad auf „Debug“ einstellen, werden alle Benachrichtigungen ausgegeben.

Wenn Sie ausführliche Protokollinformationen benötigen, aktivieren Sie die Diagnose-Traces, indem Sie im Dropdown-Menü **Diagnostic Traces** die Einstellung **Enable** (Aktivieren) wählen.

Definieren Sie bei Bedarf den Filter für die Diagnose-Traces, indem Sie im Feld **Filter** auf **Edit** (Bearbeiten) klicken.



Syslog - System > Syslog > Diagnostic Traces > Edit

Probleme mit der ISDN-Schnittstelle:

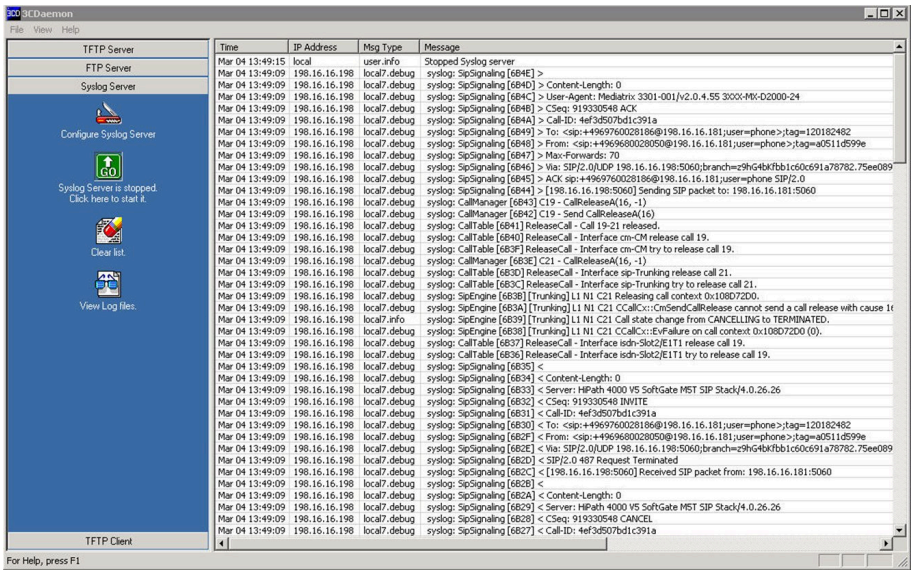
- Falls Probleme mit der ISDN-Schnittstelle (E1/T1/S0) auftreten, wird empfohlen, „ISDN“ auf „All“ (Alle) einzustellen.
- In der Regel benötigen Sie von den ISDN-Stack-Meldungen lediglich die Layer 3-Informationen, also die „ISDN Stack Q.931 Interpreted frames“.
- Für die Untersuchung von Problemen mit DTMF-Map, Zuordnungsproblemen, Sammelanschlüssen ... setzen Sie Call Router (Anruf-Router) auf Debug
- SIP-Meldungen können Sie verfolgen, indem Sie „SIP“ auf „Debug“ einstellen.

Für die Untersuchung allgemeiner Probleme müssen mindestens folgende Einstellungen vorgenommen werden:

- Ein Ethereal-Trace, das die SIP-Meldungen enthält.
- Ein Syslog-Trace, für das folgende Werte auf „Debug“ eingestellt sind:
  - Integrated Services Digital Network (Isdn)
  - Media IP Transport (Mipt)
  - SIP-Endpunkt (SipEp)
  - Telefonieschnittstelle (TelIf)
  - Diagnose-Traces

  Klicken Sie unter den Filtern auf „Edit“ (Bearbeiten) und setzen Sie folgende Traces auf „Debug“ oder „ALL“:
- Anruf-Router
- ISDN

- Line (Leitung)
- SIP
- Stream



3.4 Videoverbindungen

OpenScape 4000 SoftGate (und STMIX) bietet Videounterstützung für native SIP-Teilnehmer und -Trunks unter Verwendung der Funktion SIP Media Proxy (SMP).

Die SMP-Funktion ermöglicht es einem SDP, OS4K transparent zu durchlaufen, was zu einer E2E-Codec-Aushandlung führt.

Die Konfiguration der DMC-Funktion ist zwingend erforderlich, um die SMP-Aushandlung zu ermöglichen.

Die für SMP erforderlichen Informationen, die zur Aushandlung der E2E-Videocodecs und der Payload führen, werden ebenfalls netzweit über das Cornet NQ-Protokoll transportiert.

3.4.1 Einschränkungen

- Video-Endpunkte werden nur an OpenScape 4000 SoftGate und STMIX unterstützt.
- Kein Interworking zu HFA Video Endpunkten und TDM Video Endpunkten.
- Video ist nur für DMC-Slave-Verbindungen erlaubt.
- Eine Video-Verbindung kann nicht zu einer bestehenden Sprachverbindung hinzugefügt werden und SDP-Wiederverhandlung kann nicht durchgeführt werden (z.B. Video-/Sprach-Codecs) wenn die DMC-Verbindung bereitsbesteht.
- Die DMC-Verbindung (Video) wird unterbrochen, wenn Funktionen wie Halten, Übertragen, Weiterleiten verwendet werden. Während dieser Zeit ist keine Videoverbindung möglich.

- Die DMC-Verbindung wird nur wiederhergestellt und Videoverbindungen können nur im Falle eines Abrufs nach dem Halten wieder aufgebaut werden.
- Nachdem eine bereits bestehende DMC-Verbindung SDP Wiederverhandlung nicht unterstützt, werden auch keine Applikationen in Verbindung mit Video-Verbindungen unterstützt (z.B. Fernsteuerung der Kamera).
- Um eine sichere direkte Nutzlast in Transitszenarien zu unterstützen, müssen alle beteiligten Trunks auf den gleichen RTP-Sicherheitsmodus konfiguriert sein.

3.4.2 Szenarien

- High Definition Video- und Audio-Übertragung für Konferenzen
- Peer-to-Peer Video-Kommunikation mit SIP-basierten Video-Verbindungen

3.4.3 Merkmale

Die Verwendung von Video mit SMP hat keine direkten Auswirkungen auf die Systemmerkmale. Da SDP E2E ausgehandelt wird, sind alle Verhaltensweisen/ Einschränkungen der Merkmale kundenspezifisch.

3.4.4 Konfiguration

Nachdem die Video-Endpunkte wie normale SIP-Teilnehmer behandelt werden, werden sie auch als solche im System eingerichtet.

Informationen wie SIP-Teilnehmer einrichten finden Sie in Kapitel 2, “SIP-Teilnehmer” im Dokument „SIP-Konnektivität“.

Zusätzlich zur DMC-Konfiguration für den Endpunkt muss AMO CGWB SMP=YES (TYPE=DMCDATA) aktiviert werden.

Handelt es sich bei dem Endpunkt um einen Nicht-OS4K-SIPQ-Partner, muss zusätzlich zu SMP=YES der Parameter AMO CGWB SMP4OSV=YES (TYPE=DMCDATA) aktiviert werden, der eine SMP-Operation für den SIPQ-Trunk erzeugt.

Um Video auch auf den UC-, WebRTC- und Fusion-Clients zu aktivieren, muss die folgende Konfiguration durchgeführt werden:

```
CHANGE-ZANDE:TYPE=OPTFEA,OPTFEA=A,FEANUM=721;
```

NOTICE:

Einschränkung: Video ist nicht mehr möglich, sobald eine Funktion (z. B. Rückfrage) während eines aktiven Gesprächs verwendet wurde.

3.5 Music on Hold - OpenScape 4000 SoftGate zur Bereitstellung von Wartemusik oder Ansagen

3.5.1 Leistungsmerkmalbeschreibung

Das OpenScape 4000 SoftGate kann als Quelle für die Bereitstellung von Wartemusik (MOH, Music On Hold) oder Ansagen verwendet werden. Es funktioniert in ähnlicher Weise wie ein mit einer analogen Leitung verbundenes externes Gerät. Das OpenScape 4000 SoftGate stellt eine virtuelle SLMA-/TMOM-Baugruppe mit gespeicherten Sprachdateien dar, die eine echte SLMA-/TMOM-Baugruppe mit angeschlossenem externem Musikgerät emuliert.
Als Musikquelle werden Audiodateien verwendet (Informationen zu den Anforderungen finden Sie in Abschnitt 7.2, „Serviceinformationen“).

Die Musik bzw. die Ansage kann auf ein beliebiges Ziel innerhalb des OpenScape 4000 SoftGate (HFA-Telefon, SIP-Telefon, SIP-Amtsleitung) sowie auf ein beliebiges Gerät unter einem anderen Zugangspunkt oder in einem Hostbaugruppenrahmen (TDM-Telefon, analoges Telefon â¦) geschaltet werden.

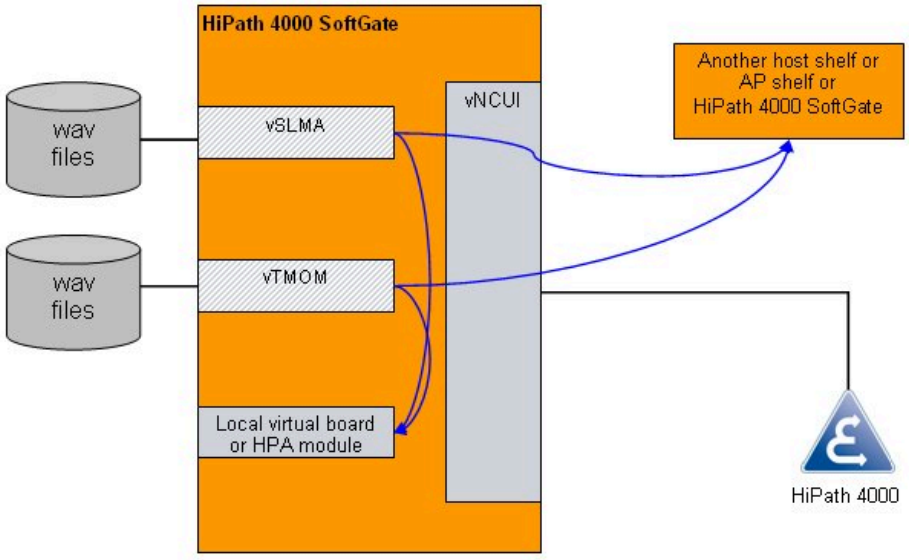


Abbildung 76: OpenScape 4000 SoftGate: Wartemusik, Ansagen

3.5.2 Serviceinformationen

Wichtige Information für Upgrade

Wenn bereits vSLMA Sätze konfiguriert sind und der Update nicht mittels AMO REGEN durchgeführt wurde, müssen alle vSLMA Sätze gelöscht und mit AMO SSC und AMO RCSU erneut konfiguriert werden.

Unterstützte Leistungsmerkmale

Folgende Leistungsmerkmale werden unterstützt:

- Musikanschaltung extern
  - Eine ausführliche Beschreibung des Leistungsmerkmals „Musikanschaltung extern“ finden Sie in dem entsprechenden Kapitel der Anwendungsfälle für Leistungsmerkmale (http://apps.g-dms.com:8081/techdoc/de/P31003H3170S103010020/musikex_de.html).
  - Anschluss an die SLMA-Baugruppe

  - Satz konfiguriert mit AMO SSC, **TYP=EXTANS**
- Mehrfach-Musikanschaltung
  - Anschluss an die SLMA-Baugruppe
  - Satz konfiguriert mit AMO RCSU, **ANWENDNG=WMUSIK**
  - Teilnehmer werden dem Wartemusik-Gerät mit AMO SCSU/AMO SBCSU/AMO SSCSU zugeordnet
- MOH und Ansagen für Flexrouting
  - Weitere Informationen zum Leistungsmerkmal „Flexrouting“ finden Sie in dem entsprechenden Kapitel der Anwendungsfälle für Leistungsmerkmale (http://apps.g-dms.com:8081/techdoc/de/P31003H3170S103010020/wwhelp/wwhimpl/js/html/wwhelp.htm?href=flexr_de.html).
  - Anschluss an die SLMA-Baugruppe
  - Satz konfiguriert mit AMO RCSU, **ANWENDNG= ANSAGE/ MUSIK**
- Synchrone Ansagen (Synchronized Announcements)
  - Weitere Informationen zum Leistungsmerkmal „Synchrone Ansagen“ finden Sie in dem entsprechenden Kapitel der Anwendungsfälle für Leistungsmerkmale (http://apps.g-dms.com:8081/techdoc/de/P31003H3170S103010020/wwhelp/wwhimpl/js/html/wwhelp.htm?href=anse1_de.html).
  - Anschluss an die TMOM-Baugruppe
  - Satz konfiguriert mit AMO TSCSU, **GER= ANSES**
- Ansageeinrichtung
  - Weitere Informationen zum Leistungsmerkmal „Ansageeinheit“ finden Sie in dem entsprechenden Kapitel der Anwendungsfälle für Leistungsmerkmale (http://apps.g-dms.com:8081/techdoc/de/P31003H3170S103010020/wwhelp/wwhimpl/js/html/wwhelp.htm?href=anse.html).
  - Anschluss an die TMOM-Baugruppe
  - Satz konfiguriert mit AMO TSCSU, **GER=ANSEA/ANSEM**

Details

Ab Openscape 4000 V7 haben die Baugruppen vSLMA und vTMOM eigene Sachnummern und haben auch die Möglichkeit alle 4 Highways im Shelf anzusprechen. Wenn die vSLMA oder vTMOM mit einer alten Sachnummer eingerichtet wird, dann ersetzt der AMO automatisch die alten Sachnummern durch die neuen Sachnummern.

Tabelle 17: Overview classical and virtual boards

Classical Boards		Virtual Boards	
Q2246-X	SLMA24	Q2339-X	vSLMA
Q2146-X	SLMA2	Q2339-X	vSLMA
Q2214-X	TMOM2	Q2340-X	vTMOM
Q2214-X100	TMOM2	Q2340-X	vTMOM
Q2187-X	SIUX2	Q2341-X	vSIUX

Die vSLMA-Baugruppe (Q2339-X) oder die vTMOM-Baugruppe (Q2340-X) kann mit dem AMO BCSU-Standardbefehl in einem oder mehreren OpenScape 4000 SoftGate-Steckplätzen konfiguriert werden.

Die unterstützten Leistungsmerkmale funktionieren wie bei einer „echten“ SLMA-/TMOM-Baugruppe.

Voraussetzungen für Audiodateien

Die Audiodateien müssen folgende Voraussetzungen erfüllen:

- .wav-Format
- PCM16-Codierung
- mono
- 8 kHz Samplingrate

3.5.3 Generierung (Beispiel)

Konfiguration der vSMLA-Baugruppe

Die vSLMA-Baugruppe (Q2339-X) kann mit dem AMO BCSU-Standardbefehl in einem oder mehreren OpenScape 4000 SoftGate-Steckplätzen konfiguriert werden.

```
LTG  1  LTU 23  SRCGRP 2   ALARMNO-LTU 0     SOFTGATE50
   10 PORTS USED
-----+----------+--------+---+-+-+---+-+------------
+------------+------------
     |          |        |   |S|H|AL-| |            |
       |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |
 HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE
 INFO  | STATUS
-----+----------+--------+---+-+-+---+-+------------
+------------+------------
   1 | Q2339-X    vSLMA          A   0| | Q2339-X    |  1
 -10 -  | READY
   2 | AVAILABLE                     0| | AVAILABLE  |
       |
   3 | Q2330-X    vHG3500    1   A   0| | Q2330-X    |  1
 -07 -  | READY
     +--------------------------------+-+------------
+------------+------------
     | IP ADDRESS : 172. 20. 12.133         B-CHANNELS :
 120    BCHLCNT : 120
     | IP MODE    :     IPV4                DHCP V4   :
 NO    DHCP V6 :   NO
     | BLOCK NO   :  40                     PRERESERVED
 LINES ASSIGNED :   NO
     |  1. FUNCT  : HG3530      240 LINES   B-CHANNELS :
 120    BCHLCNT : 120
     +--------------------------------+-+------------
+------------+------------
   4 | Q2333-X    SLMO24     1   A   0| | Q2333-X    |  1
 -11 -  | READY
```

```
     +--------------------------------+-+------------
+------------+------------
     | MAC ADRESS : 00-01-E3-8B-C1-EA
     +--------------------------------+-+------------
+------------+------------
   5 | Q2331-X    SLMAE          A    0| | Q2331-X    |  1
 -07 -  | READY
     +--------------------------------+-+------------
+------------+------------
     | MAC ADRESS : 00-01-E3-96-E2-C7
     +--------------------------------+-+------------
+------------+------------
   6 | Q2329-X    SoftGate   1        0| | Q2329-X    |  1
 -09 -  | READY
     +--------------------------------+-+------------
+------------+------------
     | IP ADDRESS : 172. 20. 12.136         B-CHANNELS :
 250    BCHLCNT : 250
     | IP MODE    :     IPV4                DHCP V4    :
 NO    DHCP V6 :   NO
     +--------------------------------+-+------------
+------------+------------
   7 | Q2339-X    vSLMA          A    0| | Q2339-X    |  1
 -10 -  | READY
   8 | Q2340-X    vTMOM          A    0| | Q2340-X    |  1
 -10 -  | READY
   9 | Q2340-X    vTMOM          A    0| | Q2340-X    |  1
 -10 -  | READY
  10 | Q2341-X    vSIUX      3        0| | Q2341-X    |  1
 -02 -  | READY
```

Konfiguration von Satz und Leistungsmerkmal

Die Sätze sowie sämtliche Leistungsmerkmale lassen sich mit AMO SSC oder AMO RCSU oder AMO TSCSU in derselben Weise konfigurieren wie bei einer echten SLMA-/TMOM-Baugruppe (siehe Verweise auf die Leistungsmerkmalbeschreibungen in Abschnitt 7.1, „Leistungsmerkmalbeschreibung“).

Konfiguration der Audiodatei

Die Audiodateien lassen sich in OpenScape 4000 SoftGate WBM mit **Konfiguration > Ansagen** (Configuration > Announcements) satzweise konfigurieren:

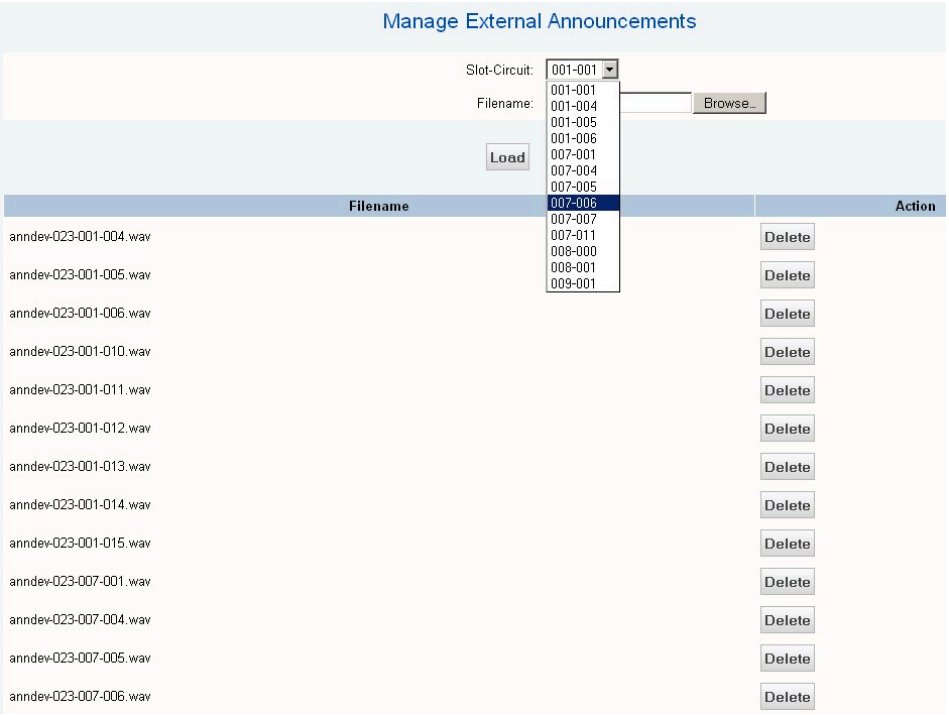


Abbildung 77: Konfiguration der Audiodatei mit OpenScape 4000 SoftGate WBM

Nach dem Laden oder Ändern der .wav-Datei für eine bereits aktive SLMA-Baugruppe muss diese mit RES-DSSU neu gestartet werden, um die neue .wav-Datei zu aktivieren. (Alternativ kann auch die virtuelle Baugruppe oder das gesamte OpenScape 4000 SoftGate neu gestartet werden.)

3.5.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU		d	vSLMA-Baugruppe einrichten
		e	Configure vSLMA board
RCSU	ANWENDNG=WMUSIK	d	Anwendung Wartemusik
	RECAPL=HMUSIC	e	Music on hold recorder
SSC	TYP=EXTANS	d	Externes Ansagegerät
	TYPE=EXTANN	e	External announcement

3.6 Gatekeeper-Redundanz für HFA/SIP-Teilnehmer

3.6.1 Leistungsmerkmalbeschreibung

Die Funktion Gatekeeper-Redundanz für HFA-Teilnehmer stellt eine weitere Möglichkeit zur Steigerung der Verfügbarkeit von VoIP-Endgeräten bei

- Ausfall der Verbindung zwischen SoftGate und Hostsystem
- Ausfall der OpenScape 4000 SoftGate Serverhardware oder
- bei Fehler in der Applikationssoftware vom SoftGate zu erhöhen.

Ab V8R2 unterstützt die Gatekeeper-Redundanzfunktion auch eine Vielzahl von SIP-Geräten. Folgende SIP-Geräte werden unterstützt:

- OpenStage WL3/WL4-Telefone
- Mediatrix 4102-Gateways
- Mediatrix 4104-Gateways
- Mediatrix 4108-Gateways
- CP-Telefone (DNSSRV erforderlich)
- Xpert

3.6.1.1 Lösungskonzept

Dazu werden zwei OpenScape 4000 SoftGates als Pool (redundand) miteinander verbunden. Die Funktion „aktiv“ oder „standby“ wird durch die Konfiguration der zusammengehörenden vHG3530 (HFA) / vHG 3500 (SIP)-Paare festgelegt. Es ist möglich innerhalb eines OpenScape 4000 SoftGates sowohl aktive Gateways (AMO CGWB, SMODE=**NORMAL**) als auch standby Gateways (AMO CGWB, SMODE=**STBYRDY**) zu konfigurieren. Zwei vHG3530 (HFA) / vHG 3500 (SIP) bilden immer ein Paar. Wobei jeweils ein Gateway im OpenScape 4000 SoftGate A und das andere im OpenScape 4000 SoftGate B konfiguriert sein muss.

Beide IP-Adressen (primäres Gateway und sekundäres Gateway) müssen am HFA/SIP-Telefon konfiguriert sein. Dies kann am Endgerät selber oder über DLS administriert werden.

Nicht alle SIP-Telefone unterstützen die Verwaltung von zwei IP-Adressen (Primär- und Sekundärserver). In diesem Fall muss DNSSRV verwendet werden.

3.6.1.2 Umschaltung

Ein Verlust der Verbindung zwischen CCA/CCB und vNCUI (also zwischen Host System und OpenScape 4000 SoftGate) führt zu der Fehlermeldung „LTUC OUT OF ATTENDANCE LIST“ und zur Umschaltung des OpenScape 4000 SoftGates („SOFTGATE RECONFIGURATION START“) (siehe AMO HISTA).

Das erfolgreiche Umschalten der einzelnen Baugruppen wird mit „BOARD RECONFIGURATION OK“ bestätigt. Das Ende der kompletten Umschaltung wird mit „SOFTGATE RECONFIGURATION END“ quittiert.

Mit Beginn der Rekonfiguration wird ein Timer (5 Minuten) gestartet. Dieser wird mit der „RECONFIGURATION END“ Meldung gestoppt. Wenn nach Ablauf des Timers noch keine END-Meldung erfolgt ist, wird die Meldung „SOFTGATE RECONFIGURATION TIME“ ausgegeben (AMO HISTA). Dies kann der Fall sein wenn mehrere OpenScape 4000 SoftGates bzw. eine große

Anzahl Teilnehmer umgeschaltet werden müssen und dient nur als zusätzlicher Hinweis, dass der Umzug noch andauert.

Vom FA-Standpunkt lässt sich nicht feststellen, ob ein Fehler auf der Anwendungs- oder PC-Ebene (Fehler oder geplantes Herunterfahren) oder aber ein IP-Netzwerkfehler (keine Verbindung OpenScape 4000 SoftGate - CCA/CCB) vorliegt.

Wichtig: Die automatische Umschaltung für Fehlerfälle wie z. B. Kabeltrennung/-ausfall oder OpenScape 4000 SoftGate Ausfall erfolgt nur einmal: von NORMAL auf STBYRDY. Unabhängig vom Zustand des ehemaligen NORMAL SoftGate gibt es keine weitere automatische Rückschaltung. Mit anderen Worten, der Fehlerfall ist eingetreten und die automatische Umschaltung wurde durchgeführt und der Fehler des ursprünglichen SoftGate wurde auf STBYRDY repariert, dann muss eine manuelle Umschaltung durchgeführt werden, um die automatische Umschaltung wieder verfügbar zu machen!

3.6.1.3 Voraussetzungen für eine Umschaltung

Die Umschaltung wird nur ausgeführt, wenn die folgenden Voraussetzungen erfüllt sind:

- Bei dem betreffenden Access Point muss es sich um ein OpenScape 4000 SoftGate handeln.
- Für das ausgefallene OpenScape 4000 SoftGate muss ein redundantes OpenScape 4000 SoftGate verfügbar sein.
- Das OpenScape 4000 SoftGate-Zielgateway muss den Status LTU READY aufweisen.

Anmerkung: Während das System oder das OpenScape 4000 SoftGate hochgefahren wird, wird keine Umschaltung eingeleitet.

3.6.1.4 Umschalt-Vorgang

Szenario 1: Alle vHG 3530 Baugruppen im ausgefallenen OpenScape 4000 SoftGate sind als aktive Gateways konfiguriert

Normal-Zustand:

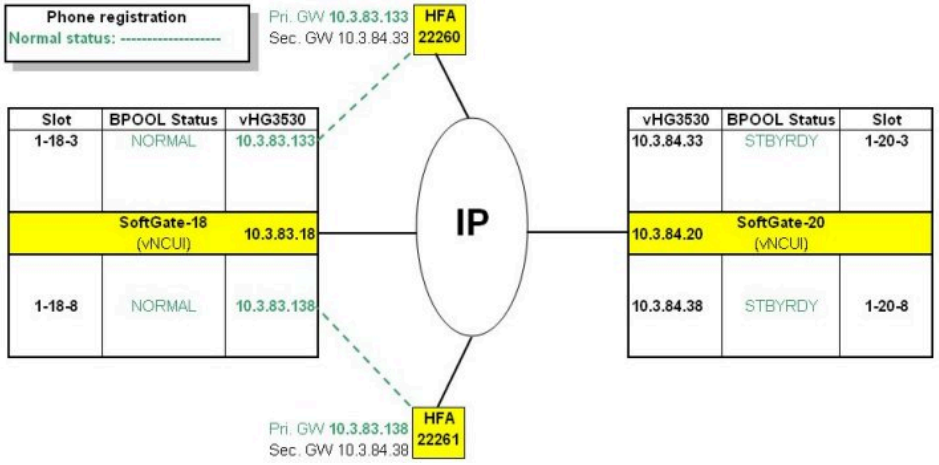


Abbildung 78: HFA-Gatekeeperredundanz „einfach“ Betrieb - Normalzustand

Bei Ausfall von OpenScape 4000 SoftGate 18:

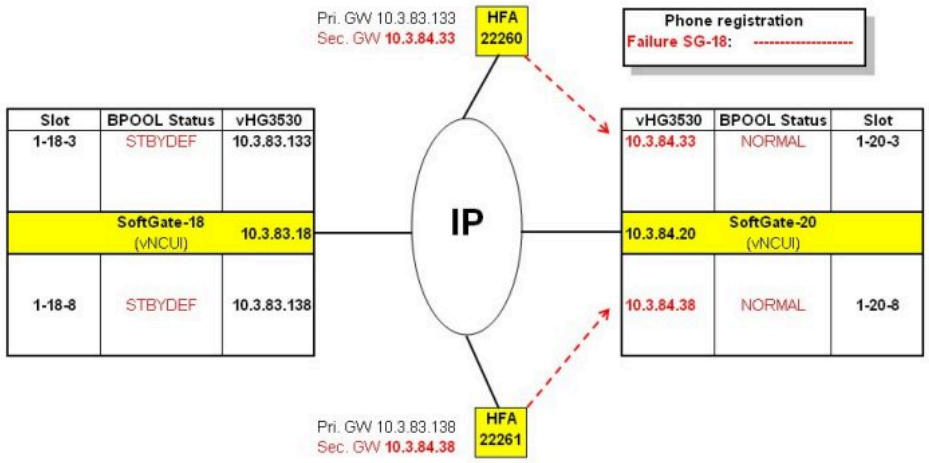


Abbildung 79: HFA-Gatekeeperredundanz „einfach“ Betrieb - Ausfall OpenScape 4000 SoftGate 18

Szenario 2: Im ausgefallenen OpenScape 4000 SoftGate befinden sich aktive vHG 3530 Gateways und Stanby vHG 3530 Gateways

Normal-Zustand:

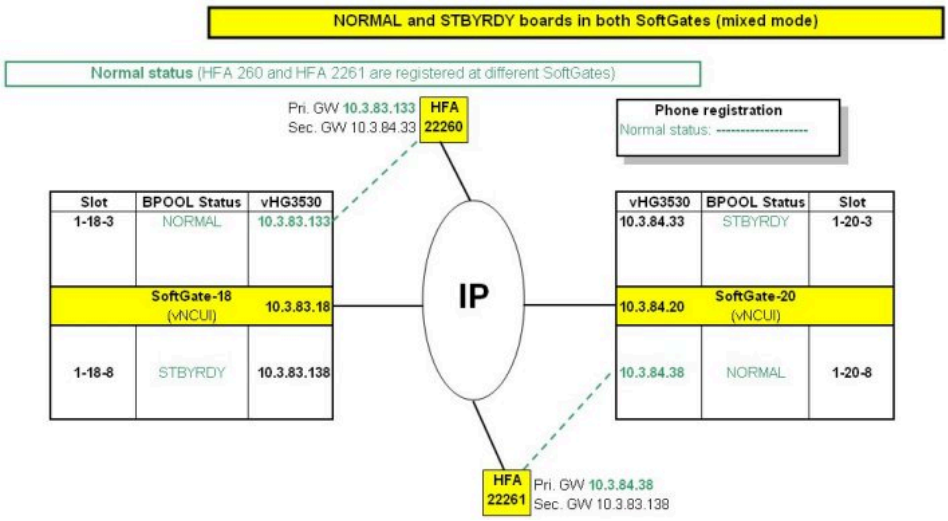


Abbildung 80: HFA-Gatekeeperredundanz Misch- Betrieb - Normalzustand

Bei Ausfall von OpenScape 4000 SoftGate 18:

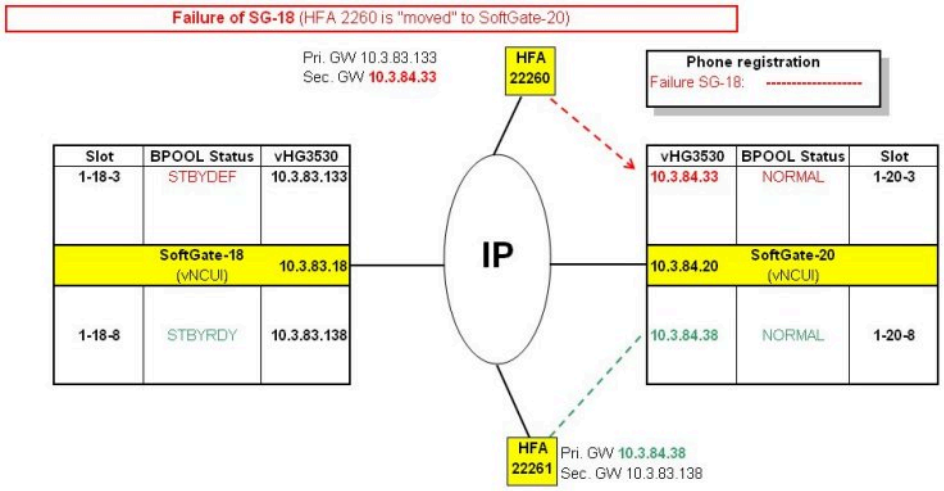


Abbildung 81: HFA-Gatekeeperredundanz Misch-Betrieb - Ausfall OpenScape 4000 SoftGate 18

Bei Ausfall von OpenScape 4000 SoftGate 20:

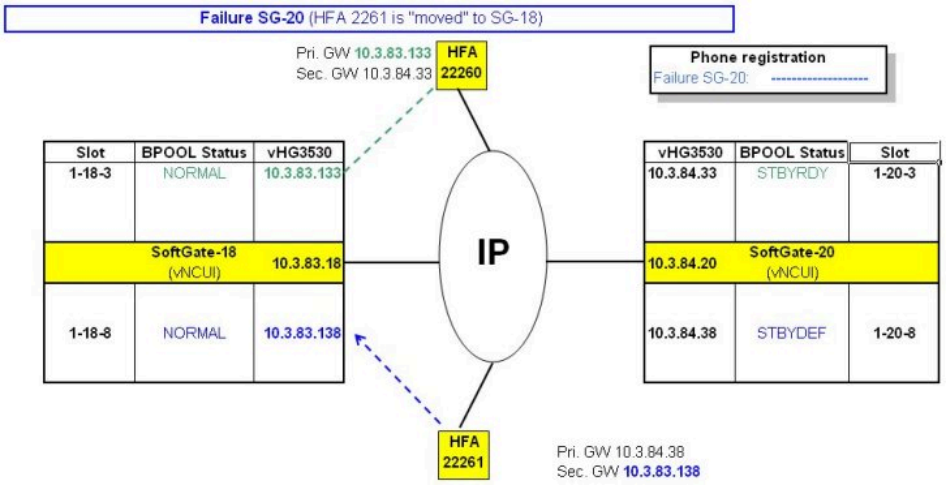


Abbildung 82: HFA-Gatekeeperredundanz Misch-Betrieb - Ausfall OpenScape 4000 SoftGate 2

Szenario 3: Alle vHG 3500 Baugruppen im ausgefallenen OpenScape 4000 SoftGate sind als aktive Gateways konfiguriert

Normal-Zustand:

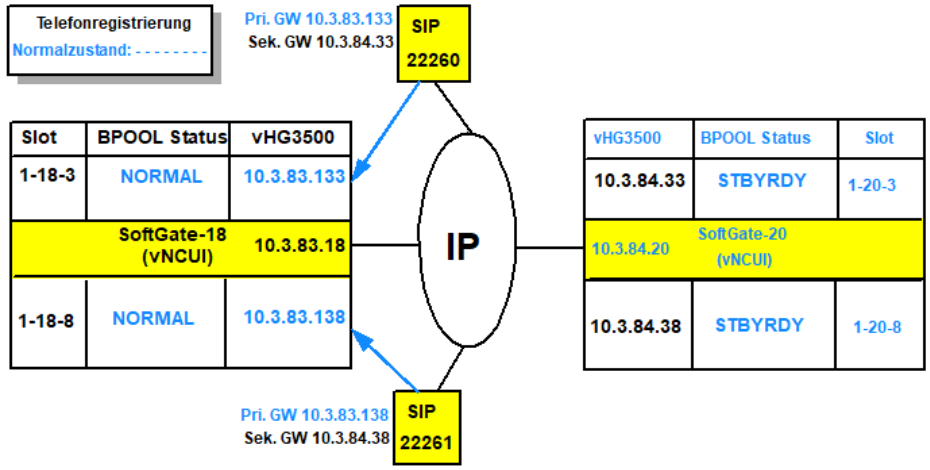


Abbildung 83: SIP-Gatekeeper-Redundanz „einfach“ Betrieb - Normalzustand

Bei Ausfall von OpenScape 4000 SoftGate 18:

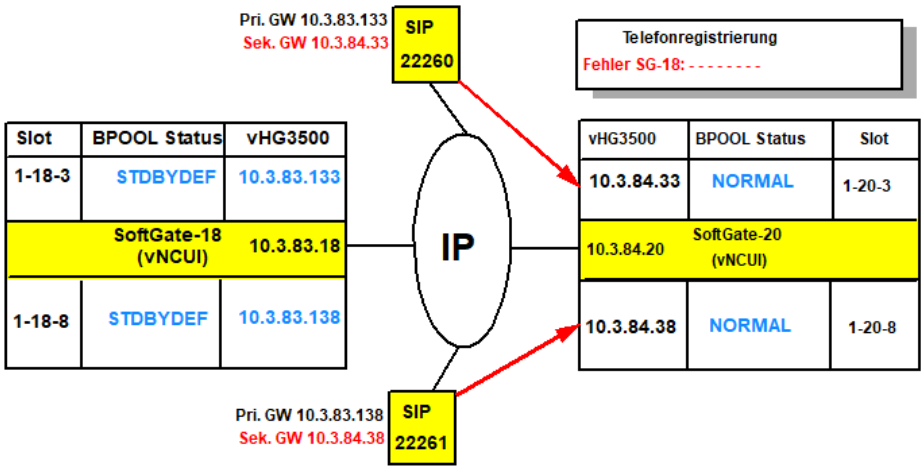


Abbildung 84: SIP-Gatekeeper-Redundanz „einfach“ Betrieb - Ausfall OpenScape 4000 SoftGate 18

Szenario 4: Im ausgefallenen OpenScape 4000 SoftGate befinden sich aktive vHG 3500 Gateways und Stanby vHG 3500 Gateways

Normal-Zustand:

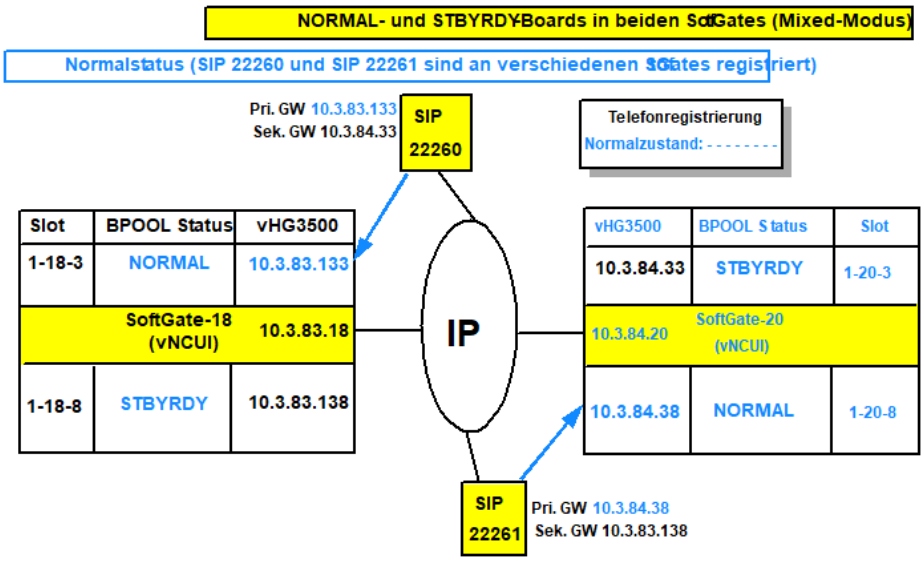


Abbildung 85: SIP-Gatekeeper-Redundanz „gemischt“ Betrieb – Normalzustand

Bei Ausfall von OpenScape 4000 SoftGate 18:

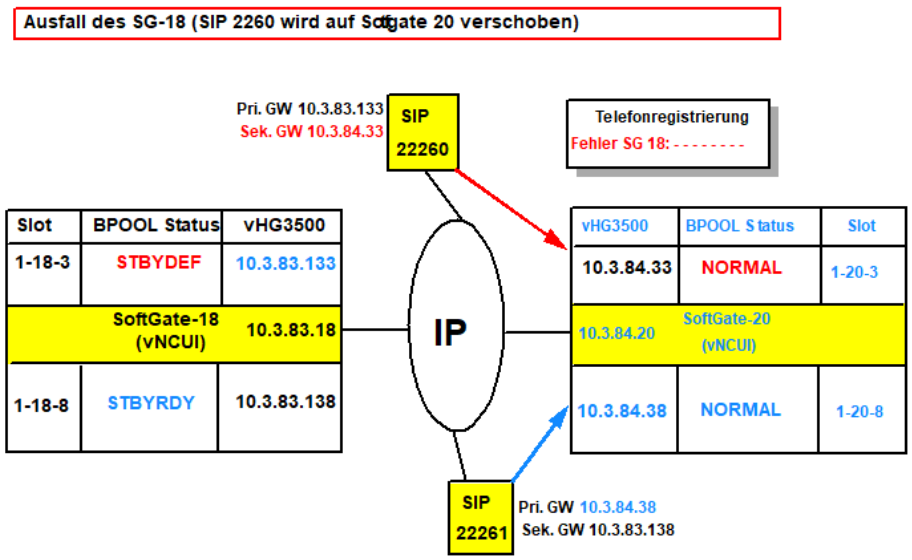


Abbildung 86: SIP-Gatekeeper-Redundanz „gemischt“ Betrieb - Ausfall OpenScape 4000 SoftGate 18

Bei Ausfall von OpenScape 4000 SoftGate 20:

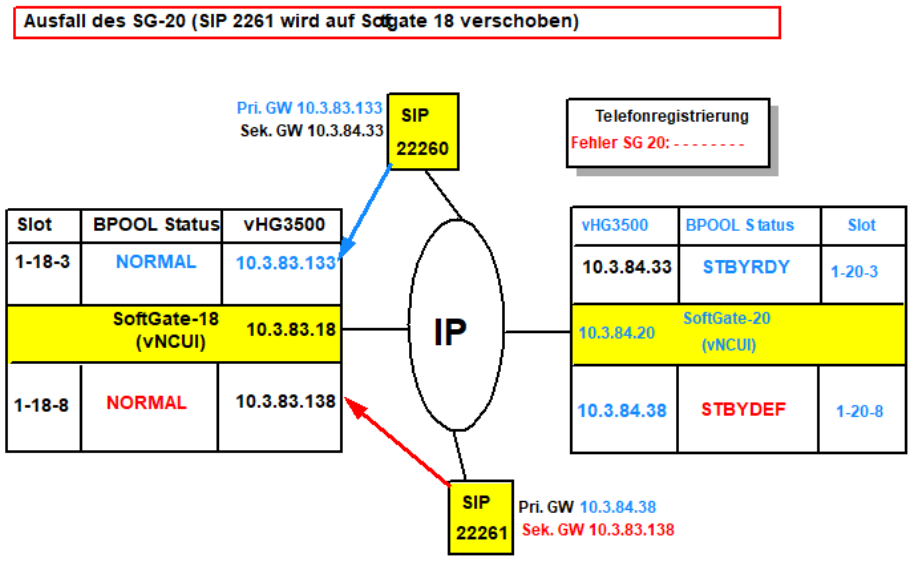


Abbildung 87: SIP-Gatekeeper-Redundanz „gemischt“ Betrieb - Ausfall OpenScape 4000 SoftGate 20

Der folgende Umstellungsprozess gilt für alle Szenarien:

Das OpenScape 4000 SoftGate 18 ist auf Grund eines Hardware-, Software- oder IT-Netzwerkfehlers (Verbindung zum CCA/CCB verloren) nicht mehr erreichbar. Daher wird die Umschaltung ausgeführt:

- Das OpenScape 4000 SoftGate 18 wird deaktiviert. Die Gateways vHG 3530 / vHG 3500 haben den Status **STBYDEF** (`AB-BP00L:MTYP=AP;`)
- Im OpenScape 4000 SoftGate 20 werden die zugehörigen Gateways neu gestartet (Warm Standby) und gehen in den Status **NORMAL**.

- Die HFA / SIP-Stationen werden in die Datenbank (AMO SBCSU) von Position 1-18-3 oder 1-18-8 auf Position 1-20-3 oder 1-20-8 umgeschrieben und die HFA / SIP-Terminals registrieren sich automatisch am entsprechenden vHG 3530 / vHG 3500 Gateway (Sekundär-Gateway).
- Die IP-Adressen der Baugruppen werden nicht (wie beim bisherigen, traditionellen BPOOL-Konzept) umgeschriben. Diese sind mit AMO CGWB fest konfiguriert.
- Manuelles Umschalten / Manuelles Rückschalten

  Mit dem AMO-Kommando `EXEC-USSU` kann ein manuelles umschalten durchgeführt werden, z. B. im Fall von bei Wartungsarbeiten oder nach einem automatischen Umschalten (im Fehlerfall) , wenn wieder auf die Original-Konfiguration zurückgeschaltet werden soll.

  Wichtig: Wird auf Grund von Wartungsarbeiten oder ähnlichem eine Umschaltung von OpenScape 4000 SoftGate 18 nach OpenScape 4000 SoftGate 20 **manuell** per AMO ausgeführt (`EX-USSU:ART=SGRED,LTU=18,SWTYPE=...`), gehen die vHG3530 vHG3500-Gateways im OpenScape 4000 SoftGate 18 in den Status **STBYRDY** (`AB-BPOOL:MTYP=AP,...;`). Dabei werden nur die Baugruppen umgeschaltet, die im entsprechenden BPOOL konfiguriert sind. Alle anderen im OpenScape 4000 SoftGate 18 befindlichen Baugruppen sind von der Umschaltung nicht betroffen.

3.6.1.5 Gatekeeperredundanz mit APE

Voraussetzungen:

- Die SoftGates, denen das Leistungsmerkmal Gatekeeperredundanz (AMO BPOOL) zugeordnet wird, müssen Mitglieder derselben APE Emergency Gruppe sein.
- Die SoftGates der APE Emergency Gruppe können nur als Gruppe (und nicht einzeln) zur CC-AP umgeschaltet werden, d. h. wenn beide SGs ihre Verbindung zum Host verloren haben. Dies bedeutet, dass die Gatekeeper-Umschaltung nur dann ausgelöst wird, wenn nur eines der beiden SG die Verbindung zum aktuellen Steuer-CC verloren hat. Wenn beide Verbindungen zu den SGs gleichzeitig unterbrochen werden, erfolgt keine Gatekeeper-Umschaltung.
- Die Rückschaltung kann automatisch und manuell erfolgen.

3.6.2 Service-Informationen

- Dieses Merkmal wird nur für OpenScape 4000 SoftGates implementiert.
- Es werden virtuelle Baugruppen (vHG 3530) mit nur HFA-Telefonen umgeschaltet.
- Es werden virtuelle Baugruppen (vHG 3500) mit nur SIP-Telefonen umgeschaltet.
- Baugruppen mit Trunking-Funktion werden nicht umgeschaltet.

- Das bestehende Leistungsmerkmal „Standby Board HG3500“ (hardwarebasierte Lösung für Hostsystem, Baugruppenrahmen und Hard-AP-Rahmen) bleibt unverändert.
- Mit MobileHFA oder Desksharing wird ein "erzwungener Abmeldung" im Falle eines Ausfalls/einer Umschaltung von OpenScape 4000 SoftGate durchgeführt. Der "Besucher" muss sich nach dem Umschalten erneut bei der Station anmelden.
- Für Verwaltungsaktivitäten oder Wartungsaktivitäten muss der OpenScape 4000 SoftGate von AMO AUSS-USSU blockiert werden (status MAN_AMO). Dies ist notwendig, um eine Umschaltung beim Herunterfahren des PC’s zu vermeiden.
- Nach Auftreten eines Fehlerfalls ist eine weitere automatische Rückschaltung nicht möglich, unabhängig davon, ob die Umschaltung zuvor automatisch (Kabeltrennung/-ausfall oder Ausfall des OpenScape 4000 SoftGate) oder durch AMO durchgeführt wurde. Die Rückschaltung muss danach immer manuell durchgeführt werden, um auf die ursprüngliche Konfiguration zurückzusetzen und damit eine Fehlerfallumschaltung wieder zu unterstützen.
- Eine Umschaltung ist nur möglich, wenn aktives und Standby OpenScape 4000 SoftGate die selbe OpenScape 4000 SoftGate Variante sind (z.B. OpenScape 4000 SoftGate 50).
- **Nur gilt bis zu und einschließlich V6 R1**: Nach einer Umschaltung von OpenScape 4000 SoftGate A auf OpenScape 4000 SoftGate B (d. h. OpenScape 4000 SoftGate A ist ausgefallen oder Verlust der LAN-Verbindung) zeigt AMO BPOOL korrekt alle Ports im Status **STBYDEF** auf OpenScape 4000 SoftGate A an.

  Nachdem OpenScape 4000 SoftGate A wieder aktiv wird, sollten alle Ports im Status **STBYRDY**sein, die Ports bleiben aber im **STBYDEF**.

  Dies ist auch der Fall, wenn die Platinen manuell zurück in OpenScape 4000 SoftGate A über EXECUTE-USSU:SGRED,<SG B>,HOME;.

  AMO BPOOL zeigt dann eigene Ports in Status **NORMAL**an, aber die Standby-Ports bleiben im Status **STBYDEF**.

  Dies ist ein Indikationsfehler von AMO BPOOL und kann von ADD-CGWB:<LTU>,<SLOT>,STBYRDY;gelöst werden.

  Fazit: Es handelt sich hier nur um ein Anzeigeproblem im AMO BPOOL, aber nicht um eine funktionale Einschränkung/Problem.
  4000 SoftGate A an.
- Wenn OpenScape 4000 SoftGate A wieder aktiv wird, sollten alle Ports den Status **STBYRDY** haben. Sie werden aber weiterhin mit **STBYDEF** angezeigt.

  Das ist auch der Fall, wenn die Baugruppen manuell mit EXECUTE-USSU:SGRED,<SG B>,HOME; auf OpenScape 4000 SoftGate A zurückgeschaltet werden.

  AMO BPOOL zeigt dann die eigenen Ports im Status **NORMAL**, aber die Standby-Ports bleiben im Status **STBYDEF**.

  Das ist ein Anzeigefehler des AMO BPOOL und kann durch EINRICHTEN-CGWB:<LTU>,<EBT>,STBYRDY; korrigiert werden.

  Fazit: Es handelt sich hier nur um ein Anzeigeproblem im AMO BPOOL, aber nicht um eine funktionale Einschränkung/Problem.

3.6.3 Generierung (Beispiel)

Das folgende Generierungsbeispiel entspricht dem im Abschnitt 10.1.4, „Umschalt-Vorgang“ dargestellten Szenario 2. Beide OpenScape 4000 SoftGates haben jeweils NORMAL und STBYRDY Baugruppen (Mischbetrieb).

Wichtig: Die in AMO BPOOL konfigurierten Paare müssen den selben Typ im AMO UCSU, Parameter **SOCOTYP** haben (z.B.: beide **SOCO50** oder beide **SOCO1000**).

Wichtig: Die in AMO BPOOL konfigurierten Paare können nicht geändert werden. Im Falle einer Fehlkonfiguration muss das Paar gelöscht und anschließend neu konfiguriert werden.

```
                    /* BFDAT NORMAL boards */
EINRICHTEN-BFDAT:FCTBLK=35,FUNCTION=HG3530,BGBKAN=BKAN120,ATTR="SOCO";
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=35,FUNCTION=HG3530,ANZSATZ=240,ANZBKAN=60;
AENDERN-BFDAT:CONFIG=OK,FCTBLK=35,ANTW=JA;
ADD-BFDAT:FCTBLK=30,FUNCTION=SIP,BGBKAN=BKAN120,ATTR="SOCO";
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=30,FUNCTION=SIP,ANZSATZ=120,ANZBKAN=120;
AENDERN-BFDAT:CONFIG=OK,FCTBLK=30,ANSW=JA;

                    /* BFDAT STBYRDY boards */
EINRICHTEN-BFDAT:FCTBLK=45,FUNCTION=STANDBY,BGBKAN=BKAN120,ATTR="SOCO";

                    /* OpenScape 4000 SoftGate 18 boards */
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=18,EBT=3,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=35,BKAN3530=30;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=18,EBT=11,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=45,BKANSIP=120,ALARMNR=0,IPMODE=IPV4,DHCPV4=NEIN,DHCPV6=NEIN;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=18,EBT=8,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=45;

                    /* OpenScape 4000 SoftGate 18 gateways */
EINRICHTEN-CGWB:LTU=18,EBT=3,SMODE=NORMAL,IPADR=10.3.83.133,NET▶
MASK=255.255.255.0, DEFRT=10.3.83.1;
EINRICHTEN-CGWB:LTU=18,EBT=11,SMODE=STBYRDY,IPADR=10.3.83.140,NET▶
MASK=255.255.255.0,VLAN=NEIN,VLANID=0,DEFRT=10.3.83.1;
EINRICHTEN-CGWB:LTU=18,EBT=8,SMODE=STBYRDY,IPADR=10.3.83.138,NET▶
MASK=255.255.255.0, DEFRT=10.3.83.1;

                    /* OpenScape 4000 SoftGate 20 boards */
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=20,EBT=3,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=45;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=20,EBT=11,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=30,BKANSIP=120,ALARMNR=0,IPMODE=IPV4,DHCPV4=NEIN,DHCPV6=NEIN;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=20,EBT=8,SACHNR="Q2330-X ",FCTID=1,LW▶
VAR="0",FCTBLK=35,BKAN3530=30;

                    /* OpenScape 4000 SoftGate 20 gateways */
EINRICHTEN-CGWB:LTU=20,EBT=3,SMODE=STBYRDY,IPADR=10.3.84.33,NET▶
MASK=255.255.255.0, DEFRT=10.3.84.1;
EINRICHTEN-CGWB:LTU=20,EBT=11,SMODE=NORMAL,IPADR=10.3.84.40,NET▶
MASK=255.255.255.0,VLAN=NEIN,VLANID=0,DEFRT=10.3.84.1;
EINRICHTEN-CGWB:LTU=20,EBT=8,SMODE=NORMAL,IPADR=10.3.84.38,NET▶
MASK=255.255.255.0, DEFRT=10.3.84.1;
```

```
                    /* BPOOL OpenScape 4000 SoftGate 18/20 */
EINRICHTEN-BPOOL:MTYP=AP,POOLNR=1,LTUA=18,EBTA=3,LTUB=20,EBTB=3,INFO="SG 18-20
POOL";
EINRICHTEN-BPOOL:MTYP=AP,POOLNO=1,LTUA=20,EBTA=11,LTUB=18,SLOTB=11;
EINRICHTEN-BPOOL:MTYP=AP,POOLNR=1,LTUA=20,EBTA=8,LTUB=18,EBTB=8;
```

Falls SIP-Karten in BPOOL konfiguriert sind, um das Softgate über die neuen SIP-Funktionskarten zu informieren, ist es notwendig, das Standby-Softgate neu zu starten.

Endgerätekonfiguration (HFA):

Beide IP-Adressen (Heimat-Gateway und Standby-Gateway) müssen dem Endgerät bekannt sein.

Einstellungen mit Hilfe des DLS:

- Aktives Gateway

  Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway/Server > Register **Gateway (HFA) / SIP Server > Reg-Adresse (HFA) / SIP Server Adresse**
- Standby Gateway

  Hauptmenü > IP Devices > IP Phone Konfiguration > Gateway/Server > Register **Gateway (Standby) > Reg-Adresse**
- Konfiguration der Teilnehmerredundanz am Endgerät:

  Hauptmenü > IP Devices > IP Phone Konfiguration > Small Remote Site Redundancy > Register **SRSR Einstellungen** > Checkbox **SRSR freigeschaltet aktivieren**

  Einstellungen über WBM:

- OpenStage

Administrator > System > Gateway

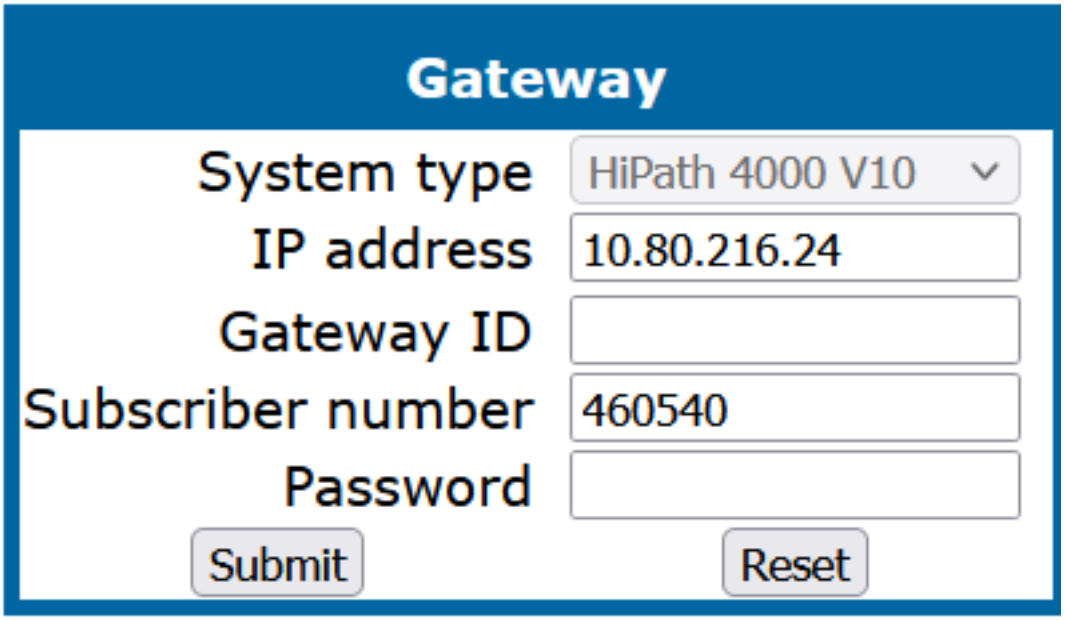


Abbildung 88: OpenStage - Teilnehmerredundanz - Gateway

Administrator > System > Standby Gateway

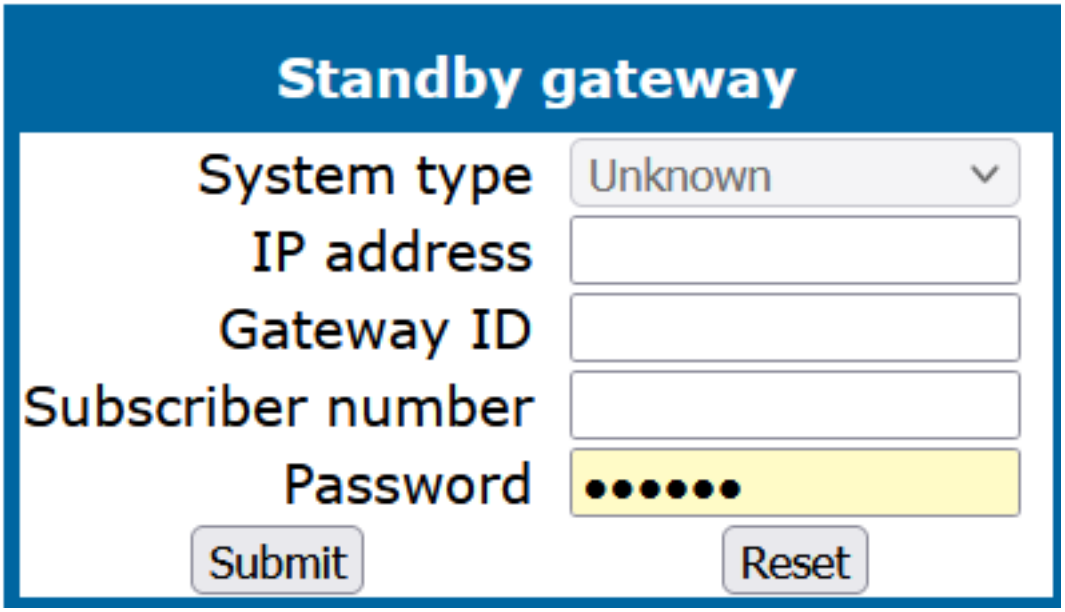


Abbildung 89: OpenStage - Teilnehmerredundanz - Standby Gateway

Administrator > System > Redundancy

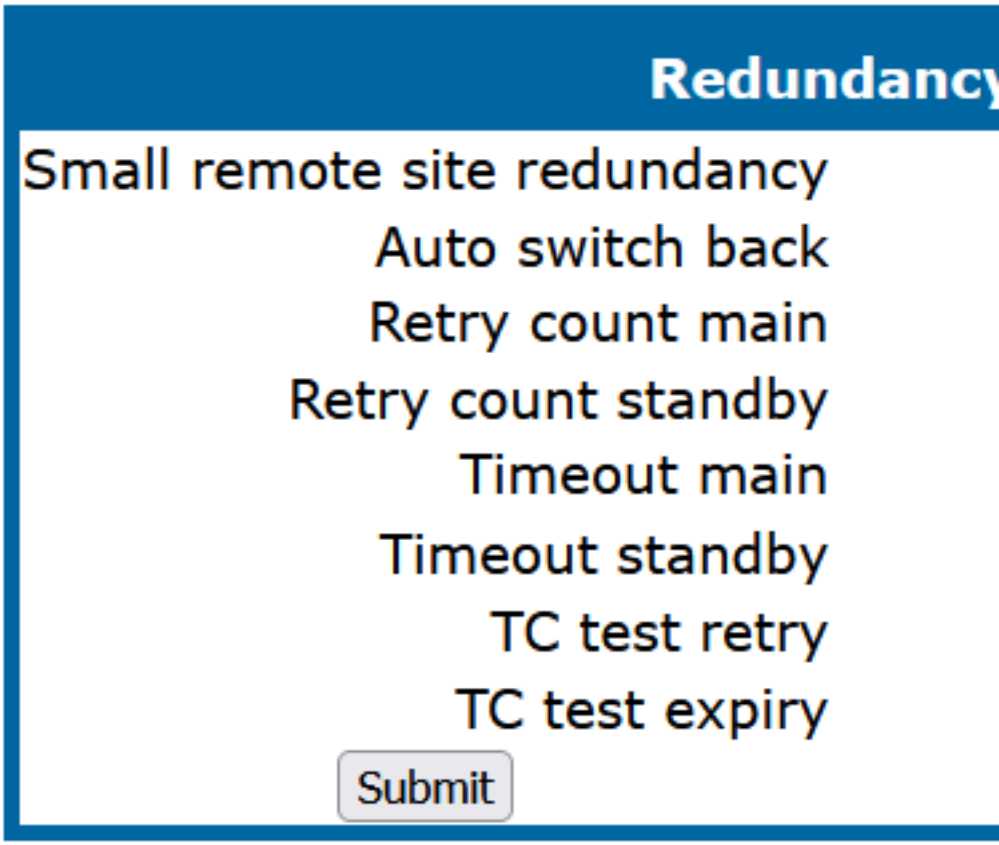


Abbildung 90: OpenStage - Teilnehmerredundanz aktivieren

- optiPoint

Administrator > System > Gateway Settings

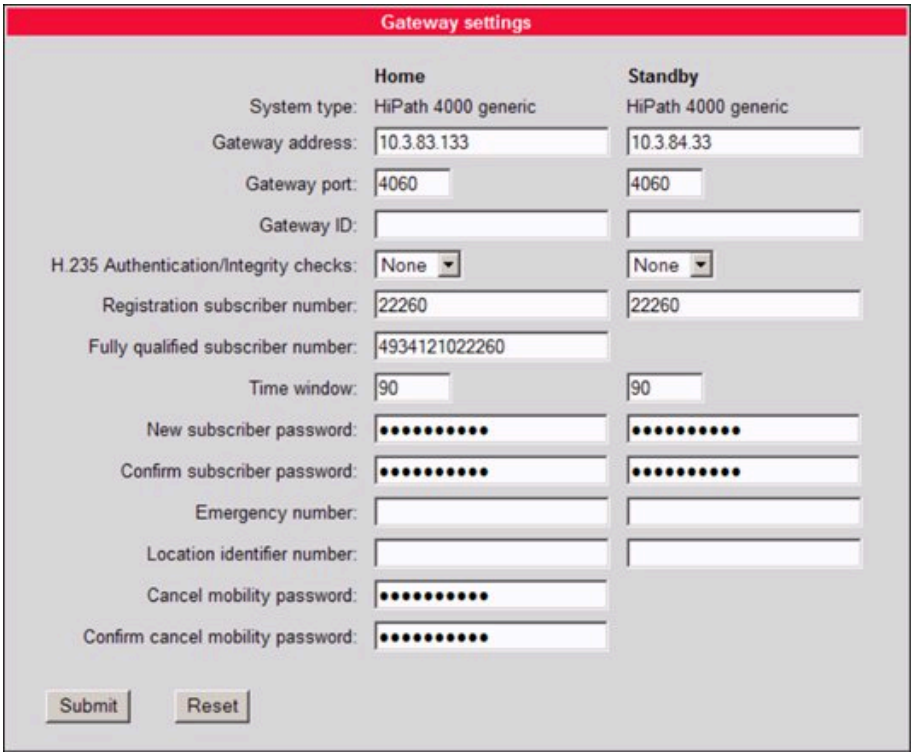


Abbildung 91: optiPoint - Teilnehmerredundanz - Gateways

Administrator > System > SRSR Settings

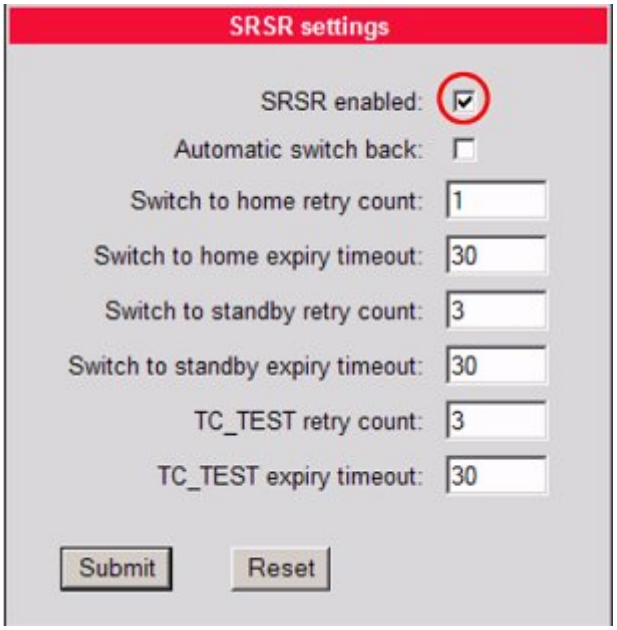
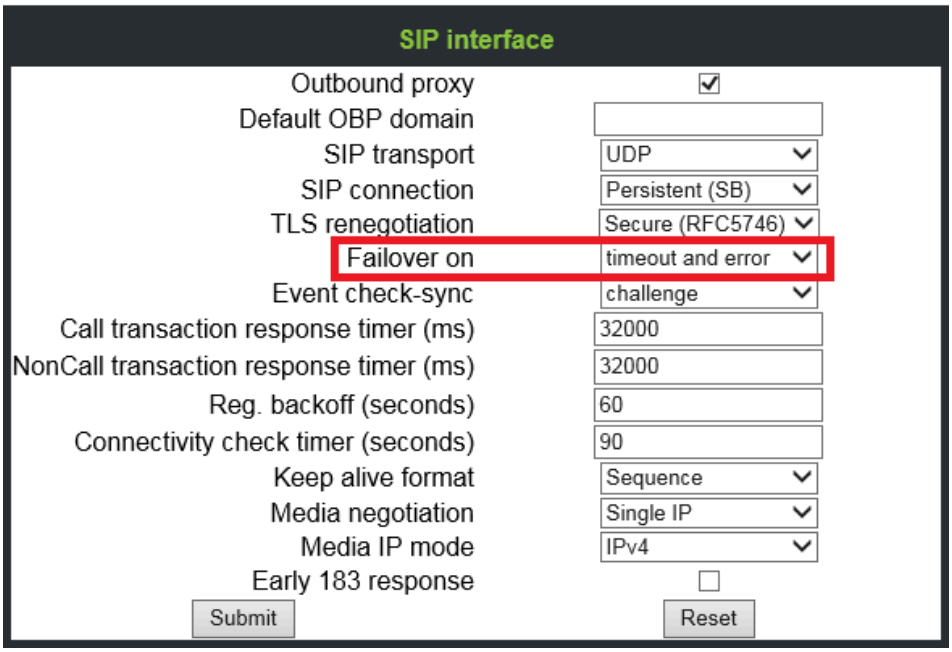


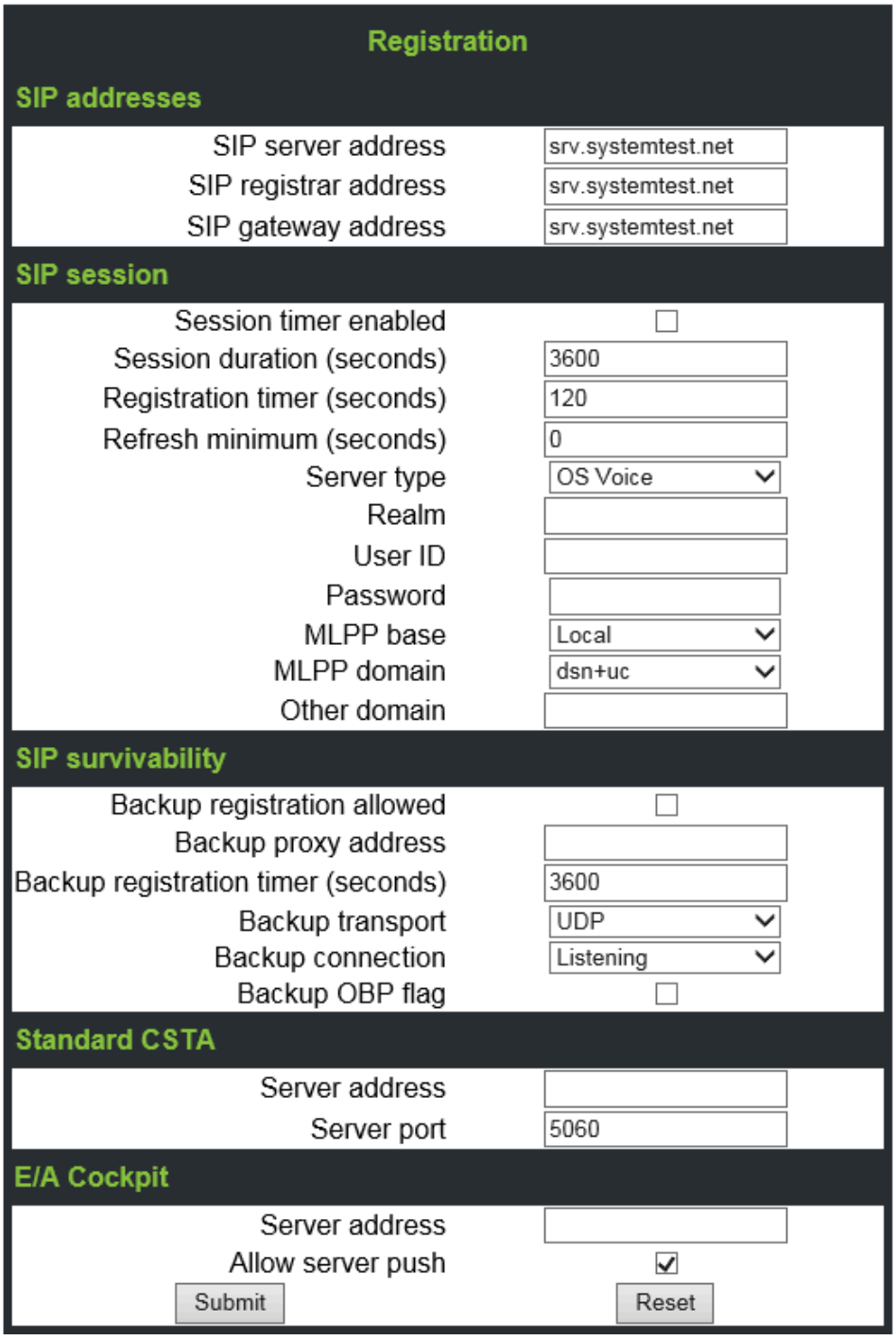
Abbildung 92: optiPoint - Teilnehmerredundanz einschalten

Endgerätekonfiguration (SIP CP-Telefone – siehe offizielle Dokumentation „OpenScape Desk Phone CP Phone Administration“ Kapitel 3.6.10 Resilienz und Überlebensfähigkeit):

„Failover on“ muss auf Timeout und Fehler eingestellt sein



Für CP-Telefone kann zur Verbesserung der Survivability nur die DNS-SRV-Methode verwendet werden.



Konfiguration von AP1120

Das AP1120 muss so konfiguriert sein, dass es ein alternatives Ziel versucht, wenn der Anruf abgelehnt wird.

Der Ursachenwert „21“ muss zu den Ursachen des Sammelanschlusses addiert werden. Weitere Informationen finden Sie in der AP1120-Service-Dokumentation.

Manuelles Umschalten

Umschaltung von OpenScape 4000 SoftGate 18 nach OpenScape 4000 SoftGate 20

```
EXEC-USSU:ART=SGRED,LTU=18,SWTYPE=<param>;
```

SWTYPE=ALLE bewirkt eine Umschaltung aller vHG 3530 vHG 3500-Baugruppen.

SWTYPE=HOME schaltet nur die vHG 3530 / vHG 3500-Baugruppen um, die im Normalzustand nicht auf das im Befehl genannte OpenScape 4000 SoftGate gehören („Nach Hause schalten“). In diesem Fall werden alle vHG 3530 / vHG 3500-Baugruppen umgeschaltet, die nicht auf das OpenScape 4000 SoftGate 18 gehören.

3.6.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BFDAT	FUNCTION=STANDBY	d	Funktionsblock für Standby konfigurieren
	FUNCTION=STANDBY	e	Configure function block for standby
BCSU	FCTBLK	d	Konfiguration der Funktionsblöcke für Normal-Betrieb und Standby
	FCTBLK	e	Function block configuration for main board and standby board
CGWB	SMODE	d	Eine vHG 3530 vHG 3500 im normalen Modus (**NORMAL**) konfigurieren und eine im Standby-Ready-Modus (**STDBYRDY**) konfigurieren
	SMODE	e	Konfigurieren Sie ein vHG 3530 / vHG 3500 für den Normalbetrieb (**NORMAL**) und ein vHG 3530 / vHG 3500 für den Standby-Betrieb (**STDBYRDY**)
BPOOL	LTUA	d	LTU der Haupt-Baugruppe
	LTUA	e	LTU of main board
	LTUB	d	LTU der Standby-Baugruppe
	LTUB	e	LTU of standby board
	EBTA	d	Einbauteilung der Haupt-Baugruppe
	SLOTA	e	Slot of main board
	EBTB	d	Einbauteilung der Standby-Baugruppe

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SLOTB	e	Slot of standby board
USSU	ART=SGRED	d	SoftGate Redundancy
	MODE=SGRED	e	SoftGate Redundancy
	SWTYPE	d	Art der Umschaltung ALLE: Umschaltung aller vHG 3530 / vHG 3500-Baugruppen HOME: Umschaltung der vHG 3530 / vHG 3500-Baugruppen, die im Normalzustand nicht auf diesem OpenScape 4000 SoftGate „Zuhause“ sind
	SWTYPE	e	Switch type ALL: Umschalten aller vHG 3530 vHG 3500-Baugruppen HOME: Umschaltung aller vHG 3530 / vHG 3500-Baugruppen, die im Normalzustand an diesem OpenScape 4000 SoftGate nicht zu Hause sind

3.7 Survivable OpenScape 4000 SoftGate

3.7.1 Leistungsmerkmalbeschreibung

Eine optionale Survivability Einheit kann ein OpenScape 4000 SoftGate zu einem „Survivable“ Access Point machen.

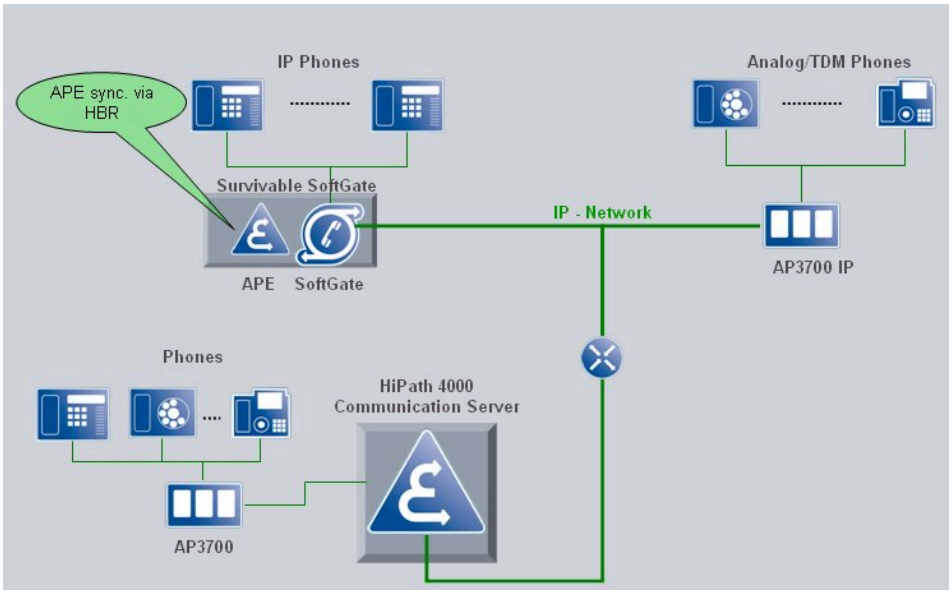


Abbildung 93: Survivable OpenScape 4000 SoftGate - Szenario

Die Survivability Einheit übernimmt die Steuerung des eigenen OpenScape 4000 SoftGates und jedes ausgewählten anderen IP Access Points/OpenScape 4000 SoftGates ohne eigene Survivability Einheit, wenn die zentrale Steuerung ausfällt (durch den Verlust der IP-Verbindung zur zentralen Steuerung oder wegen eines Ausfalls der zentralen Steuerung).

Die Synchronisation des APE wird mit OpenScape 4000 Assistant > Backup & Restore durchgeführt.

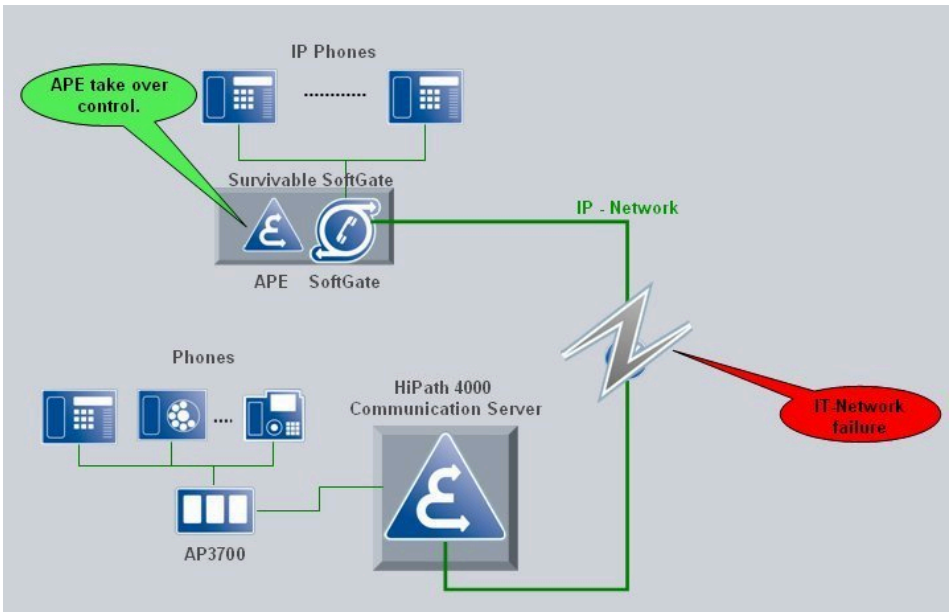


Abbildung 94: Survivable OpenScape 4000 SoftGate - IT-Netzwerk-Ausfall

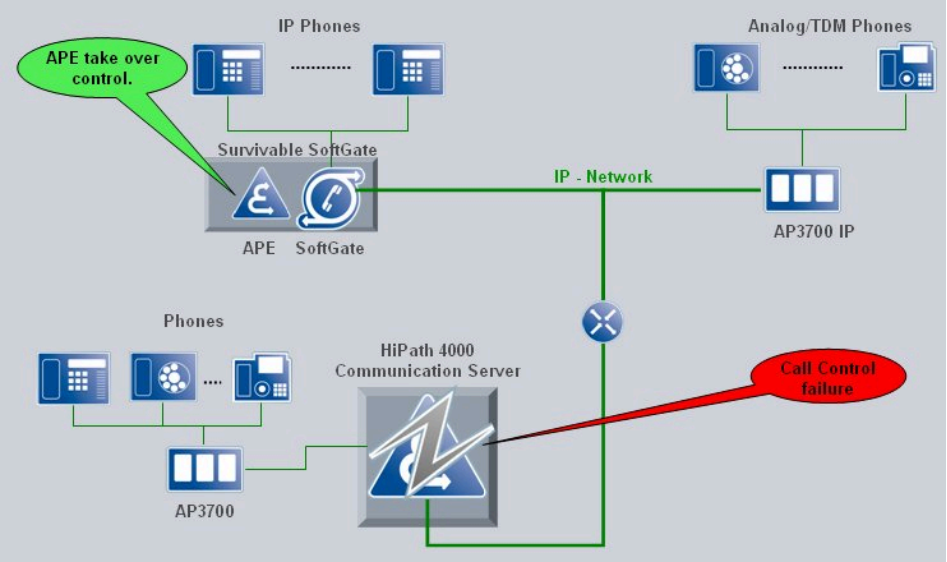


Abbildung 95: Survivable OpenScape 4000 SoftGate - Ausfall der zentralen Steuerung

3.7.2 Serviceinformationen

Das Leistungsmerkmal ist auf Standard Server und OpenScape Access freigegeben.

Mögliche Konfigurationen:

- Zwischen 1 und 83 OpenScape 4000 SoftGates / AP 3700 IP mit AP Emergency (eigener Survivability Einheit).
- Eine Gruppe von AP 3300 IP, AP 3700 IP und OpenScape 4000 SoftGate (ohne Survivability Einheit) können sich mit einem AP 3700 IP / OpenScape 4000 SoftGate mit Survivability Einheit verbinden.

3.7.3 Generierung (Beispiel)

1) First Installer

Deployment „Survivable OpenScape 4000 SoftGate“ auswählen.

Wichtig: Bei Atlantic LAN darf keine Schnittstelle ausgewählt werden. Sonst funktioniert Xlink nicht!

---

2) Weitere Konfigurationsdetails finden Sie unter „Access Point Emergency (APE)“, Kapitel 2, „Einrichtung des Leistungsmerkmals APE (Access Point Emergency)“.

3.8 IPv6

3.8.1 Leistungsmerkmalbeschreibung

In naher Zukunft soll IPv4 durch IPv6 ersetzt werden. Damit sollen zahlreiche Einschränkungen und Probleme in Verbindung mit der Nutzung von IPv4 behoben werden. Der Einsatz von IPv6 für VoIP bietet eine Reihe deutlicher Vorteile:

- Bei IPv6 wird NAT (Network Address Translation) nur noch für das Netzwerk-Masquerading benötigt, da insgesamt genügend IP-Adressen zur Verfügung stehen werden. Bei aktivierter NAT können Audiopakete nur mithilfe von Behelfslösungen über VoIP-Verbindungen ausgeliefert werden und daher Probleme mit der Audioübertragung auftreten.
- IP-Pakete sollen effizienter geroutet werden.
- IPv6 verfügt über integrierte Dienstgüte (QoS)-Funktionen, insbesondere für Echtzeitanwendungen.
- Signalisierungs (TLS)- und Sprachverschlüsselung (SRTP) wird auch mit IPv6 unterstützt (siehe **„Signalisierungs- und Sprachverschlüsselung (SPE)“**).

3.8.2 Service-Informationen

- IPv6 kann in OpenScape 4000 Softgate auf den vHG3500 SIP- und STMIX/ STMIY-Trunking-Routen (SIP-Q und natives SIP) verwendet werden.
- SIP-Trunking kann zwischen verschiedenen HiPath 4000 V6-/OpenScape 4000-Systemen (SIP-Q) oder zwischen einem HiPath 4000 V6-/OpenScape 4000-System und einem externen IPv6-Partner, z. B. OpenScape Voice oder SIP Service Providern (native SIP), genutzt werden.
- Für interne Konnektivität kann IPv6 zwischen der OpenScape 4000 Zentrale und den OpenScape 4000 SoftGates (TCP-Signalisierung), sowie zwischen den OpenScape 4000 SoftGates untereinander (RTP-Payload) eingesetzt werden.
- Common Gateways (HG 3500) und IPDA-Baugruppen (NCUI) unterstützen IPv6 nicht.

3.8.3 Generierung (Beispiel)

3.8.3.1 Wichtiger Hinweis

Wichtig: Nach Änderungen der IPv6 Konfiguration muss ein APE Backup/Restore zeitnah erfolgen, so dass der APE im Notfall auch mit den aktuellen/gültigen IP-Adressen agiert und somit die Funktion gewährleistet ist.

3.8.3.2 IPv6-Netzwerkanbindung für OpenScape 4000 SoftGate und STMIX/STMIY (Trunking)

Die Trunking-Gateways (virtuelles HG 3500) an einem OpenScape 4000 SoftGate und STMIX/STMI unterstützen IPv6-Networking für SIP-Q und natives SIP-Trunking. Die freigegebenen IPv6-Partner sind in Vertriebsfreigabe / Release Notes aufgeführt.

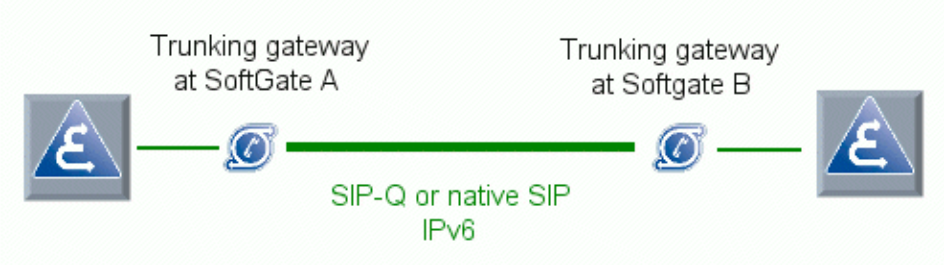


Figure 96: IPv6 für OpenScape 4000 SoftGate und STMIX/STMI (Trunking)

Die Konfiguration einer IPv6-Verbindung erfolgt in drei Schritten:

Trunking-Gateways in OpenScape 4000 einrichten

Konfigurieren der IPv6-Adresse für OpenScape 4000 SoftGate und STMIX/STMIY Trunking Gateway (AMO CGWB)

Konfiguration im virtual HG 3500 SIP WBM

3.8.3.2.1 Trunking-Gateways in OpenScape 4000 einrichten

Das Hinzufügen eines IPv6-Trunking-Gateways zu OpenScape 4000 SoftGate und STMIX/STMI erfolgt wie das Hinzufügen eines IPv4-Trunking-Gateways über AMOs, mit Ausnahme der Konfiguration des IP-Modus.

Für jedes IPv6 Trunking-Gateway eines OpenScape 4000 SoftGate können die Trunking-Modi „Dual Stack“ und „IPv6 only“ ausgewählt werden, allerdings nur, wenn es sich um eine reine Trunking-Baugruppe (HG3550) handelt. Die Auswahl erfolgt mit AMO CGWB.

`CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPCONF,IP` **`MODE=DUALSTCK`** ; oder

`CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPCONF,` **`IPMODE=IPV6`** ;

Der IPMODE-Standard ist **IPV4**.

Der „Dual Stack“-Modus muss verwendet werden, wenn auf einer für IPv6 konfigurierten SIP-Trunking Strecke sowohl IPv4 als auch IPv6 unterstützt werden muss. In diesem Fall wird IPv6 bevorzugt. Alle IPv6 Dual Stack-Partner müssen ausdrücklich freigegeben sein. Die freigegebenen IPv6-Partner sind in Vertriebsfreigabe / Release Notes aufgeführt. Das Interworking mit Full-ICE-Devices wird nicht unterstützt.

In Verbindung mit reinen IPv6-Partnern muss der Modus „IPv6 only“ verwendet werden.

Bemerkungen

- Um zu vermeiden, dass die IPv6-Route von IPv4-Direktmedienverbindungen umgangen wird, stellen Sie bitte sicher, dass **DMCEND** für das IPv6-Trunking-Gateway konfiguriert ist.

AEND-LDAT:LRTG=<lroute>,LATTR=DMCENDE;

- IPv6 wird für Signalisierung und Payload genutzt.
- Alle IPv6-Adressen werden über AMO CGWB konfiguriert.
- Dual Stack/IPv6 Baugruppe auf IPv4 umschalten:
- Die Umschaltung einer Baugruppe von Dual Stack/IPv6 auf IPv4 geschieht mit AMO CGWB:

  AENDERN-CGWB:MTYP=CGW,LTU=<ltu>,EBT=<slot>,TYP=IPCONF,IPMODE=IPv4;

  Wenn eine IPv6- oder Dual Stack-Karte wieder auf IPv4 umgestellt wird, werden alle IPv6-Einstellungen, die sich auf diese Karte beziehen, automatisch deaktiviert (IPv6-Adresse, Trunk-Profil-Konfiguration). Das bedeutet, dass bei einem weiteren Wechsel zurück zu IPv6 oder Dual Stack die IPv6-Adresse erneut mit AMO CGWB konfiguriert werden muss.

3.8.3.2.2 Konfigurieren der IPv6-Adresse für OpenScape 4000 SoftGate und STMIX/STMIY Trunking Gateway (AMO CGWB)

Die Konfiguration der IPv6-Adresse für das OpenScape 4000 SoftGate Trunking Gateway erfolgt über AMO CGWB: `CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYPE=IPV6IF,IPADRV6=<IPv6-Adresse>,PREFIXV6=<IPv6-Präfixlänge>,DEFRTV6=<IPv6-Default-Router>, DNSIPADR=<DNS-IPv6-Adresse>,DNSIPADR2=<DNS-IPv6-Adresse 2>`; Für das vHG 3500 (RES-BSSU) muss ein Neustart durchgeführt werden.

3.8.3.2.3 Konfiguration im virtual HG 3500 SIP WBM

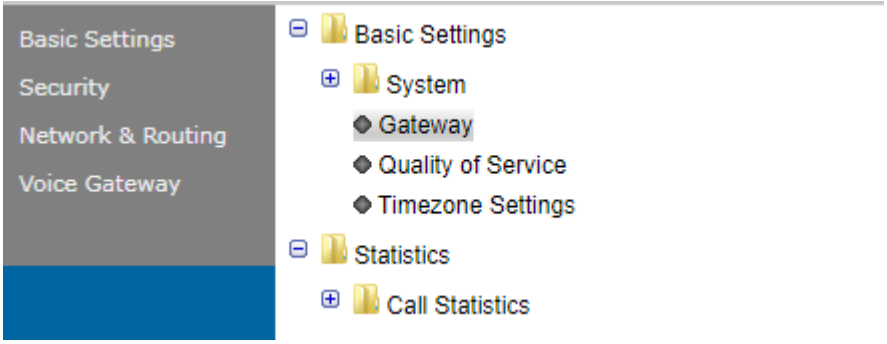
IMPORTANT: Jedes IPv6 Trunking-Gateway muss für Administrationszwecke nach wie vor über eine IPv4-Adresse verfügen.

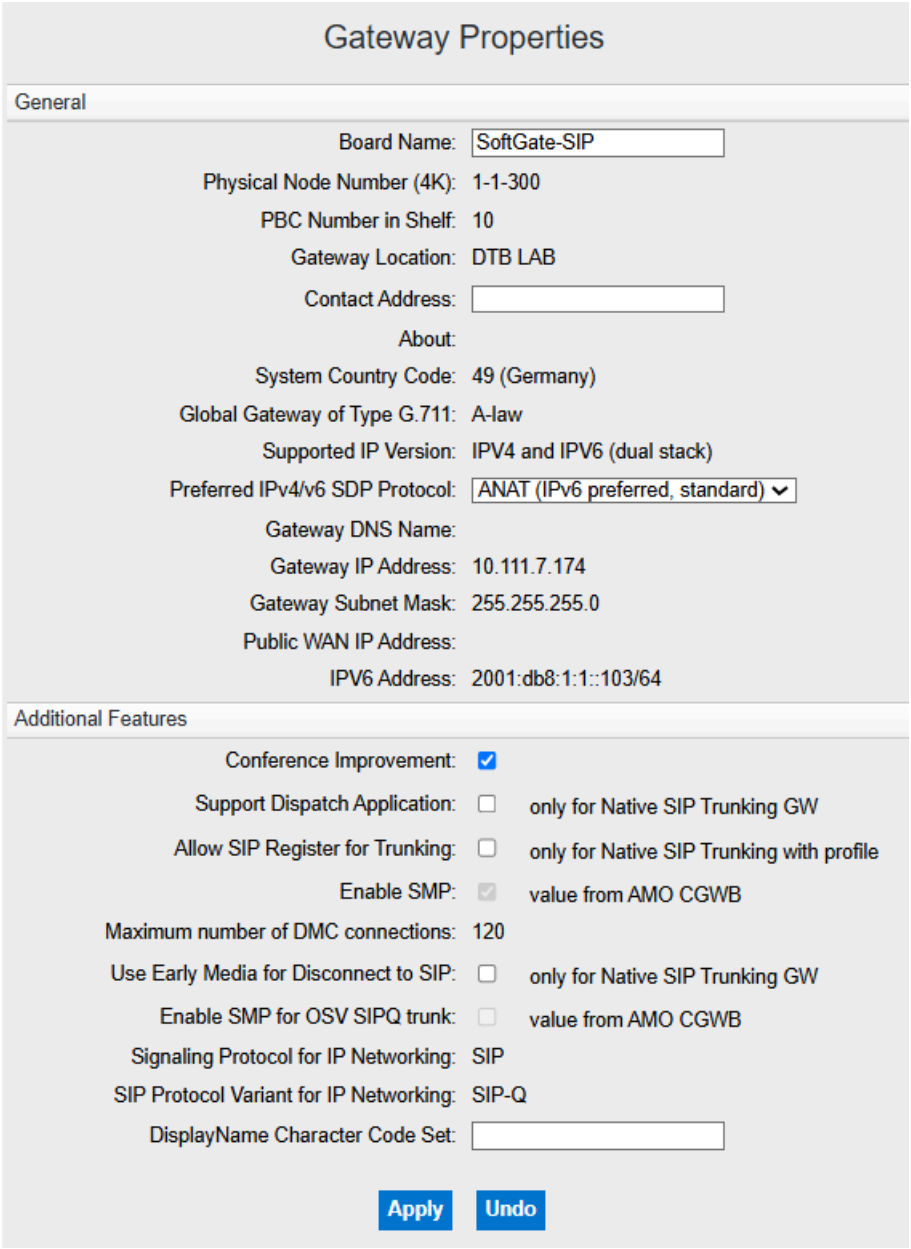
---

1) Konfiguration des lokalen Gateways

Der ausgewählte IP-Modus eines IPv6 Trunking-Gateways kann über WBM überprüft werden.

WBM vHG 3500 SIP > Konfiguration > Basic-Einstellungen > Gateway





IP-Modus eines IPv6-Trunking-Gateways

Nach dem Restart kennt das OpenScape 4000 SoftGate die IPv6-Adresse. Sie kann über WBM überprüft werden.

WBM vHG 3500 SIP > Konfiguration > Grundeinstellungen > System > Gateway-Eigenschaften

1) Konfiguration des Trunking-Partners

Nach der AMO-Konfiguration des IP-Modus und der Zuweisung der IPv6-Adresse über den AMO CGWB muss nun der IPv6-Trunking-Partner über das SIP-Trunk-Profil (siehe **SIP-Connect >** Abschnitt 3.3, "SIP-Trunk-Profile") im WBM des SIP-Gateways vHG 3500 konfiguriert werden.

Die Verwendung der Trunking-Profile muss für den verwendeten IP-Networking-Trunk Typ (SIP-Q oder native SIP) aktiviert sein.

WBM vHG 3500 SIP > Konfiguration > Voice Gateways > SIP-Trunk-Profil Parameter



Figure 97: SIP-Trunk-Profilparameter für IPv6-Trunking-Partner

Standardmäßig ist für native SIP Trunks die Verwendung von Profilen aktiviert und für SIP-Q die Verwendung von Profilen deaktiviert.

Im SIP Trunk Profil wird die IPv6-Adresse oder der vollqualifizierte Domänenname (FQDN), unter der bzw. dem der IPv6-Trunking-Partner erreichbar ist konfiguriert. **Registrar** , **Proxy** , **Outbound Proxy** und **Inbound Proxy** können ebenfalls IPv6-Adressen haben.

WBM vHG 3500 SIP > Konfiguration > Voice Gateways > SIP-Trunk-Profil



Figure 98: SIP-Trunk-Profil für IPv6-Trunking-Partner

WBM vHG 3500 SIP > Konfiguration > Voice Gateways > SIP-Trunk-Profil > <Ausgewähltes Trunk-Partner-Profil> **> Aktivieren**

Da SIP-Trunk-Profile verwendet werden müssen, kann pro Gateway nur ein Trunking-Partner konfiguriert werden. Beachten Sie, dass die Anzahl der IPv6-Verbindungen bei einem OpenScape 4000 SoftGate daher von der maximalen Anzahl von SIP-Trunking-Gateways pro OpenScape 4000 SoftGate abhängig und momentan auf 9 begrenzt ist.

Für IPv6/Dual Stack SIP-Q Trunking sind die Profile **SIPQ Trk Without Registration** und **SIPQ Trk With Registration** vorgesehen.

Für IPv6/Dual Stack Native SIP-Trunking werden die Profile der entsprechenden freigegebenen Partner verwendet.

3.8.3.3 Interne IPv6-Konnektivität

3.8.3.3.1 Überblick

Wenn für die interne Konnektivität IPv6 verwendet wird, wird der IP-Verkehr zwischen der OpenScape 4000 Zentrale und den OpenScape 4000 SoftGates (TCP-Signalisierung), sowie zwischen den OpenScape 4000 SoftGates untereinander (RTP-Payload), über IPv6 abgewickelt.

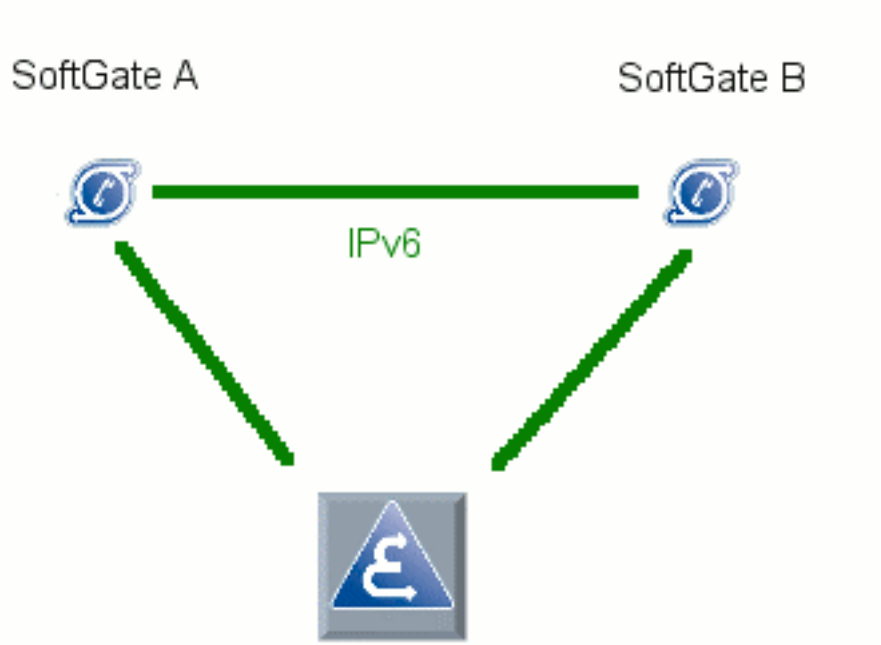


Abbildung 99: IPv6 für OpenScape 4000 SoftGate (interne Konnektivität)

IPv6 wird für Signalisierung (HSR Verbindung) und Payload (IPDA-Masterverbindung) genutzt. Um zu vermeiden, dass die internen IPv6-Verbindungen von IPv4 Direct Media Connections (DMC) umgangen werden, darf DMC an den Endpunkten (IP-Endgerät) nicht aktiviert sein.

Bei einem Anruf zwischen zwei Telefonen am selben OpenScape 4000 SoftGate wird nur für die Signalisierungsdaten (HSR-Verbindung) eine IPv6-Verbindung genutzt. Die Voice-Payload zwischen den Telefonen wird mittels IPv4 übertragen.

Bei einem Anruf zwischen zwei Telefonen an unterschiedlichen OpenScape 4000 SoftGates werden sowohl für die Signalisierungsdaten (HSR-Verbindung) als auch für die Voice-Payload IPv6-Verbindungen genutzt.

3.8.3.3.2 Konfiguration

Voraussetzung ist: Der IPv6-Betrieb zwischen dem OpenScape 4000 Central Switch und allen relevanten OpenScape 4000 SoftGates muss im System konfiguriert sein. Dazu muss für jedes OpenScape 4000 SoftGate in der AMO STMIB der Parameter **IPMODE=DUALSTCK** gesetzt werden.

AENDERN-STMIB:MTYPE=NCUI2,LTU=1,TYPE=IPCONF,IPMODE=DUALSTCK;

Anschließend muss das OpenScape 4000 SoftGate mit der neuen Konfiguration versorgt und neu gestartet werden (`EXEC-USSU:MODE=UPDATAP,LTU=<ap-number>;`)!

Für die Konfiguration der internen IPv6-Verbindungen werden folgende Adressinformationen benötigt:

- Die IPv6-Adressen aller involvierten Hosts, also der OpenScape 4000 Zentrale, der OpenScape 4000 SoftGates und ggf. APE / Survival OpenScape 4000 SoftGates.
- Die IPv4-Adressen der angeschlossenen Geräte für das Routing des IP-Verkehrs über die IPv6-Verbindungen (Tunnel) zwischen den betreffenden Hosts.

Die IPv4-Adressen werden während der Installation mit der OpenScape 4000 Plattform Administration (Portal) sowohl in der OpenScape 4000 Zentrale als auch auf den OpenScape 4000 SoftGate-Hosts lokal bereitgestellt.

3.8.3.4 Sicherung und Wiederherstellung des NGS

Die NGS-Datenbank kann gesichert werden mit:

Export-/Importtool:

OpenScape 4000 Plattform Administration (Portal) > System > IPv6-Adressen

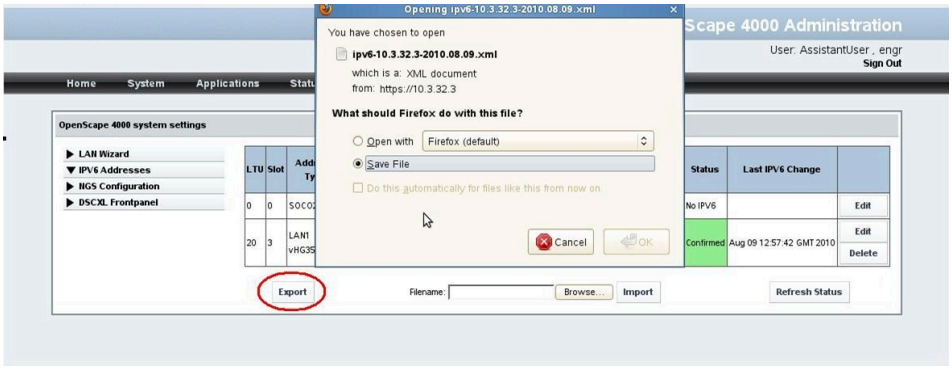


Abbildung 100: NGS-Datenbank: Export

Mit der Exportoption wird die NGS-Datenbank als „.xml“-Datei exportiert, die mit Microsoft Office Excel oder anderen Tools angezeigt, bearbeitet und ausgedruckt werden kann:

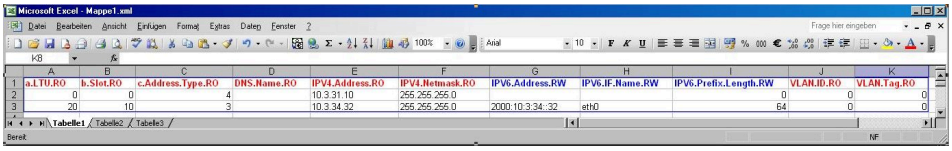


Abbildung 101: NGS-Datenbank: Exportdatei

Die mit RW gekennzeichneten Felder können vor dem Importieren der Tabelle bei Bedarf manuell bearbeitet werden. Die mit RO als schreibgeschützt gekennzeichneten Felder sollten nicht manuell geändert werden.

Nach dem Bearbeiten der Tabelle muss die Datei mit der Option „xml Data“ im XML-Format gespeichert werden.

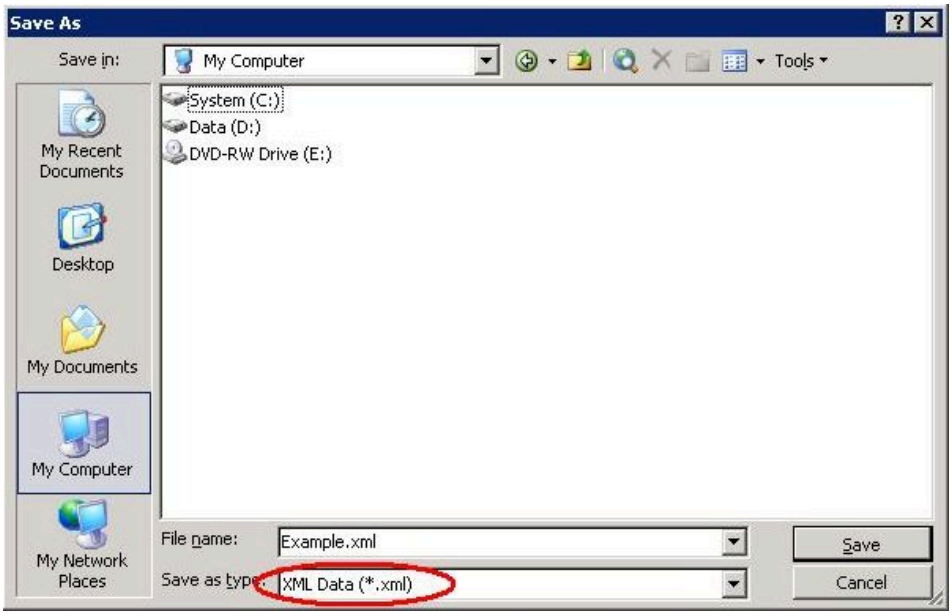


Abbildung 102: NGS-Datenbank: Exportdatei speichern

Der Schlüssel für die Annahme oder Zurückweisung eines Eintrags in der exportierten Tabelle ist die PEN (LTU, Slot) der Baugruppe und der Adresstyp.

Beim Importieren einer Tabelle werden Einträge, die sich auf nicht mehr für IPv6 konfigurierte Baugruppen beziehen, übergangen.

OpenScape 4000 Plattform Administration (Portal) > System > IPv6-Adressen

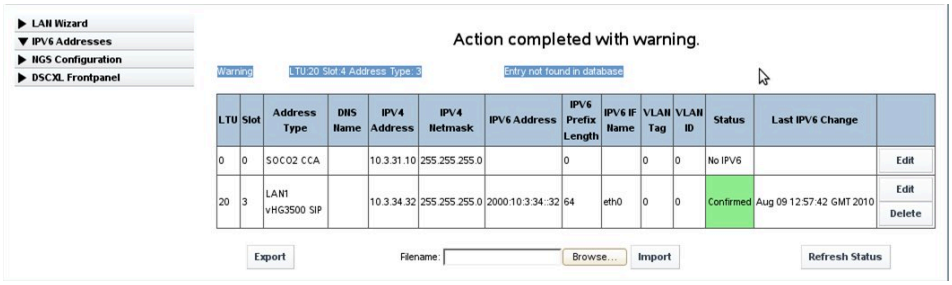


Abbildung 103: NGS-Datenbank: Import fehlgeschlagen mit Warnungen

Wenn während des Importvorgangs eine duplizierte IP-Adresse erkannt wird, schlägt der gesamte Vorgang fehl. In diesem Fall muss die Tabelle manuell überprüft werden, um inkonsistente Datenbankeinträge zu vermeiden.

OpenScape 4000 Platform Administration (Portal) > System > IPv6 Addresses

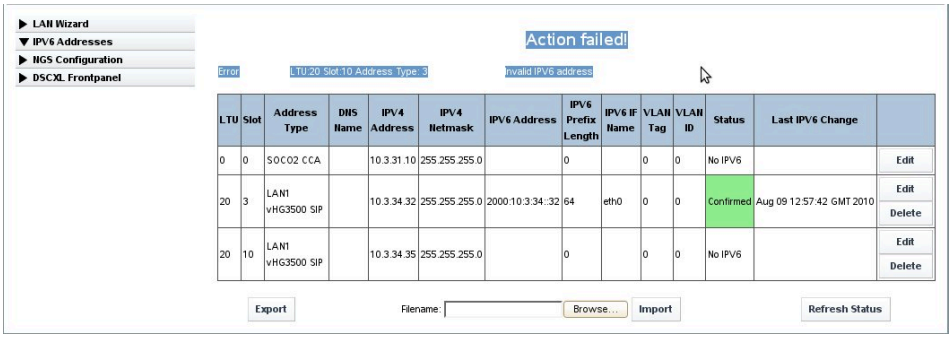


Abbildung 104: NGS-Datenbank: Import fehlgeschlagen

3.8.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
CGWB	TYP=IPCONF	d	IP-Konfiguration
	TYPE=IPCONFIG	e	IP configuration
	IPMODE=DUALSTCK	d	IP-Version 4 und IP-Version 6
	IPMODE=DUALSTCK	e	IP version 4 and IP version 6
	IPMODE=IPV6	d	nur IP-Version 6
	IPMODE=IPV6	e	IP version 6 only
BCSU	TYP=IPCONF	d	IP-Konfiguration
	TYPE=IPCONFIG	e	IP configuration
	IPMODE=DUALSTCK	d	IP-Version 4 und IP-version 6
	IPMODE=DUALSTCK	e	IP version 4 and IP version 6
	IPMODE=IPV6	d	nur IP-Version 6
	IPMODE=IPV6	e	IP version 6 only
SIPCO	IPMODE	d	Possible values: IPV4, DUALSTCK
	IPMODE	e	Possible values: IPV4, DUALSTCK
STMIB	IPMODE	d	Possible values: IPV4, DUALSTCK
	IPMODE	e	Possible values: IPV4, DUALSTCK
	IPMODE=DUALSTCK	d	IP-Version 4 und IP-Version 6
	IPMODE=DUALSTCK	e	IP version 4 and IP version 6

3.9 Load Balancing

3.9.1 Leistungsmerkmalbeschreibung

SIP-Load-Balancing wird zur Lastverteilung des SIP-bezogenen Datenverkehrs im IP-Netzwerk eingesetzt. Damit wirde die Leistung der beteiligten SIP-Server skaliert, eine Überlastung der Server vermieden und eine hohe Verfügbarkeit der SIP-Dienste erreicht.

Load Balancing dient dazu, Rufe von einem Provideranschluss, einer OpenScape UC oder OpenScape Xpressions auf mehrere Gateways zu verteilen, z. B. wenn der Anschluss mehr als die maximalen Kanäle eines Gateways hat. Bei einem Provideranschluss kann nur eine Ziel-IP-Adresse konfiguriert werden, so dass ohne Load Balancing pro Gateway ein Providerderanschluss vorhanden sein müsste.

Anrufe können auch selektiv über ihre Rufnummer von einer Verbindung zu mehreren sogar geografisch verteilten Gateway-Gruppen oder OpenScape 4000-Systemen mit Hilfe einer Routing-Nummer (z. B. Ortsvorwahl) gesendet werden, die für jedes Gateway konfiguriert werden kann. Innerhalb einer Gruppe werden die Rufe an das Gateway mit den meisten freien Kanälen gesendet.

SIP-Load-Balancing kann für jedes SIP-Gateway (HG 3500 oder vHG 3500 SIP) im Netzwerk aktiviert werden. Ist das Leistungsmerkmal korrekt aktiviert, registrieren sich die teilnehmenden Gateways automatisch am SIP Load Balancing Server.

SIP Load Balancing wird auch mit mehreren OpenScape UC Media Servern freigegeben. Diese können sich nicht automatisch beim SIP Load Balancing Server registrieren. Deshalb müssen diese manuell im OpenScape 4000 SoftGate WBM konfiguriert werden.

3.9.2 Serviceinformationen

Der OpenSIPS Load Balancer ist Teil des OpenScape 4000 SoftGate Softwarepaketes und wird mit jedem OpenScape 4000 SoftGate installiert. Er läuft auf dem OpenScape 4000 SoftGate hat aber eine eigene (von dem OpenScape 4000 SoftGate verschiedene) IP-Adresse. Die IP-Adresse wird während der Installation eingerichtet.

Mit Hilfe seiner konfigurierten IP-Adressen holt sich der Load Balancer automatisch seinen eventuell vorhandenen DNS-Server-Namen vom DNS-Server.

Das Leistungsmerkmal Load Balancing ist per default ausgeschaltet und muss über das WBM des OpenScape 4000 SoftGates und das WBM jedes teilnehmenden Gateways eingeschaltet werden.

Leistungsmerkmale

- „Load Balancing“ für Inbound native SIP-Verbindungen zu virtuellen HG 3500 Gateways (OpenScape 4000 SoftGate) und den auf dem Betriebssystem vxWorks basierten HG 3500 Gateways (IPDA) (z.B. bei SIP Provider oder OpenScape UC Anbindung).

- Unterstützt native SIP Trunks ohne Registrierung.
- Virtuelle HG 3500 Gateways unterschiedlicher OpenScape 4000 SoftGates und HG 3500 Gateways in unterschiedlichen Access Points werden unterstützt.
- Error Logging / Tracing mit OpenSIPS.
- Sicherheit in der Datenübertragung zwischen den vHG 3500/HG 3500 und OpenSIPS (über authentifiziertes https).
- Failover Mechanismen für Inbound-Verbindungen, die vom Gateway auf Grund von Fehlermendungen abgewiesen wurden.
- Status Monitoring der konfigurierten Gateways über den Open SIPS Load Balancer.
- Load Balancing für verschiedene Gruppen von Gateways.
- SPE unterstützt das TLS 1.2 Protokoll.
- Zu den SPE-Funktionen gehören: Enforce Secure Renegotiation RFC, TLS-Revokationszertifikatsliste, maximales Wiedereinschaltungsintervall und minimale RSA-Schlüssellänge.

Anforderungen

- Im Netzverbund muss ein OpenScape 4000 SoftGate vorhanden sein.
- SIP-Load-Balancing kann nur aktiviert werden, wenn die Verwendung von SIP-Trunking-Profilen aktiviert ist.
- **WBM > Konfiguration > Voice Gateway > SIP-Trunk-Profil-Parameter**
- Damit SIP-Load-Balancing funktionieren kann, muss sichergestellt werden, dass die (Outbound)-Proxy-Einstellungen im SIP-Trunking-Profil korrekt konfiguriert sind.
- **WBM > Explorer > Sprachgateway > (rechte Maustaste) SIP-Trunk-Profilparameter**

Einschränkungen

Das Leistungsmerkmal „SIP Load Balancing“ kann nur bei einem „Standalone SoftGate“ Deployment verwendet werden. Es steht also zum Beispiel für „Survivable SoftGate“ nicht zur Verfügung.

SIP Load Balancer unterstützt maximal 2000 parallele Kanäle.

3.9.3 Generierung (Beispiel)

Wichtig: Eine Generierung über AMOs ist nicht möglich.

3.9.3.1 SIP Load Balancer Einstellungen

Der SIP-Load-Balance Server wird über das WBM des OpenScape 4000 SoftGates aktiviert. Dazu muss die IP-Adresse des Load Balancers und die Netzwerkmaske eingegeben werden.

Nach jeder Aktivierung/Deaktivierung oder Änderung der IP-Adresse des Load Balancers ist ein Restart des OpenScape 4000 SoftGates notwendig.

WBM > Konfiguration > SIP Load Balancer > Einstellungen

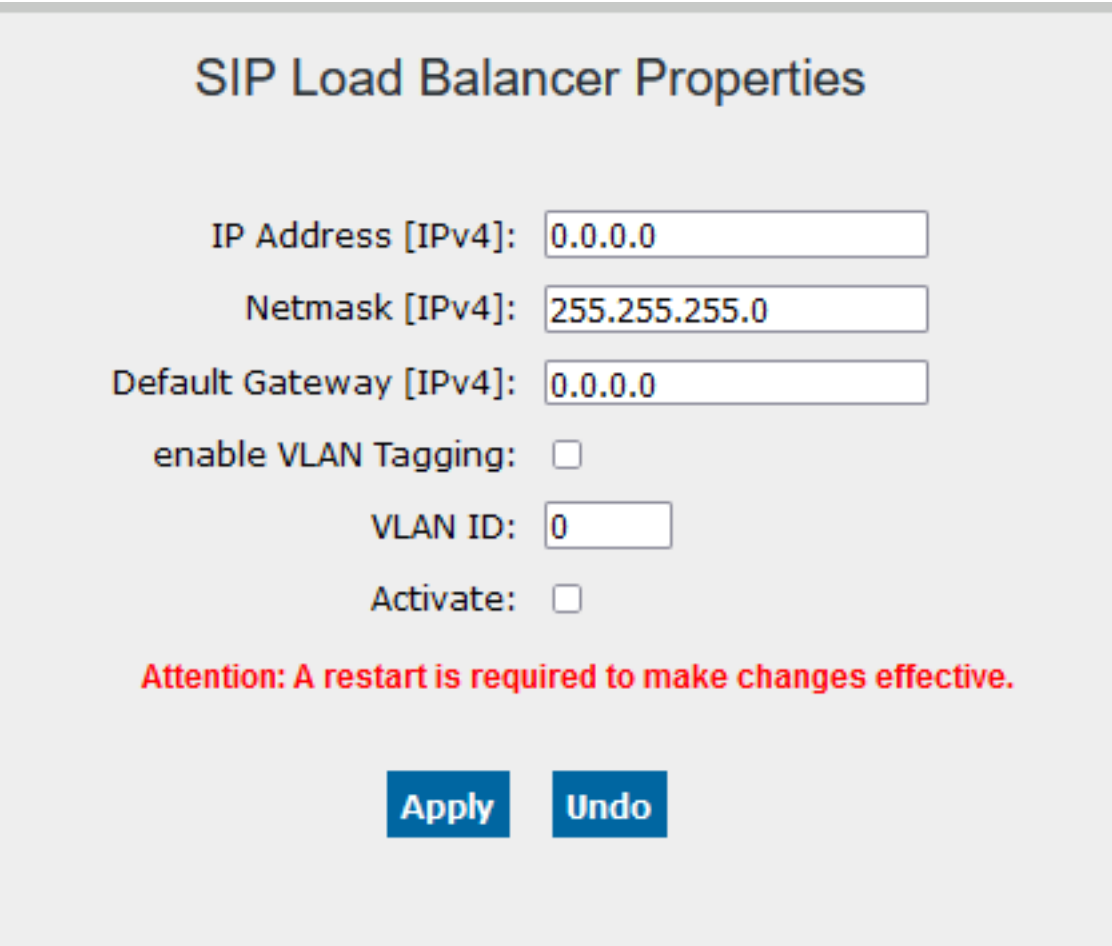


Abbildung 105: SIP-Load-Balance Eigenschaften

3.9.3.2 Ausgehende/eingehende Rufe über SIP Load Balancing Server

WBM > Konfiguration > VoIP-Gateway > SIP-Trunk-Profil-Parameter

Abschnitt **Security**

In diesem Abschnitt werden die folgenden Sicherheitseinstellungen aufgeführt: *Freigegebene Sicherheitsstufe*, *verwendetes TLS* und *verwendete Nutzlastverschlüsselung*

Abschnitt Proxy

Konfigurieren Sie die IP-Adresse des Load Balancer über den Proxy.

Abschnitt **Outbound Proxy**:

Um gehende Rufe von den Gateways über den Loadbalancer z.B. zum Provider zu routen, muss die IP-Adresse des SIP Load-Balance-Servers als gehende Proxy in das jeweilige Trunk-Profil eingetragen werden.

Abschnitt **Inbound Proxy**:

Unter Inbound-Proxy wird bei **IP Adresse/Host-Name** ein DNS-Name konfiguriert. Für diesen DNS-Namen können beim DNS-Server mehrere IP-Adressen hinterlegt werden. Das ist wichtig, da die IP-Adresse kommender Rufe gegen Proxy oder Inbound Proxy Einträge überprüft wird. OpenScape UC

Rufe können von mehr als zwei IP-Adressen kommen und gehen dann über DNS.

Anmerkung: Anstatt der IP-Adresse kann auch der DNS-Server-Name des Load-Balance-Server verwendet werden.

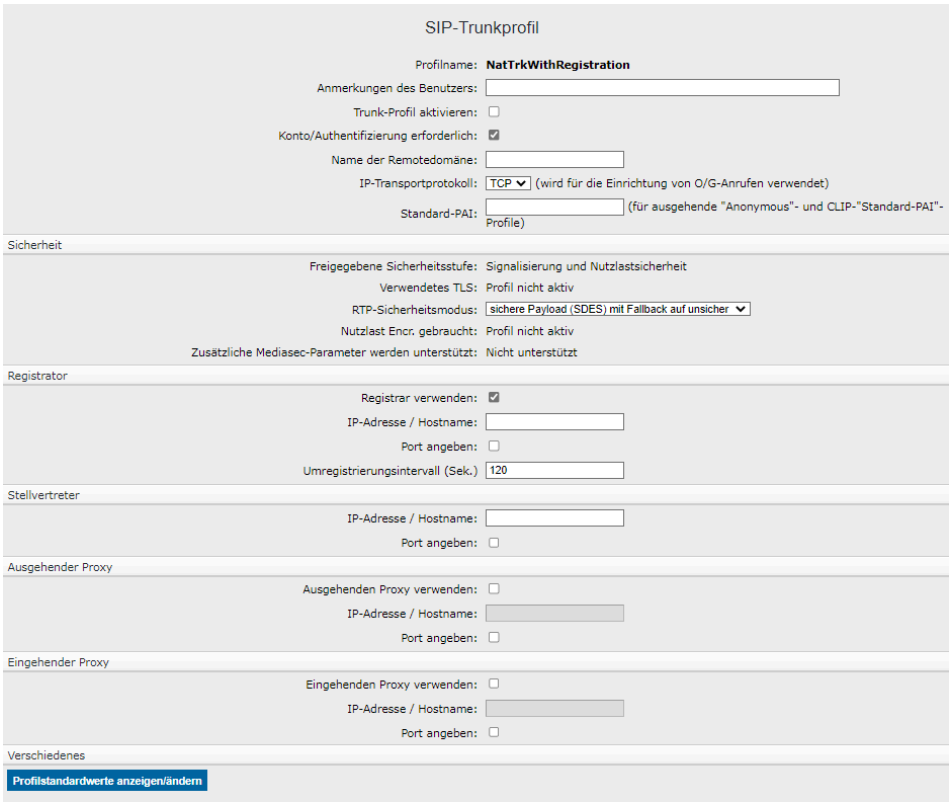


Abbildung 106: SIP Load Balancer Trunk-Profilparameter

Besonderheit im Fall von OpenScape UC Media Server Farmen

Da der SIP Load Balancer die IP-Adressen der OpenScape UC Media Server kennt, muss nicht mehr Outbound und Inbound Proxy verwendet werden. Es reicht, wenn nur der Proxy eingetragen wird (= IP-Adresse des SIP Load Balancer).

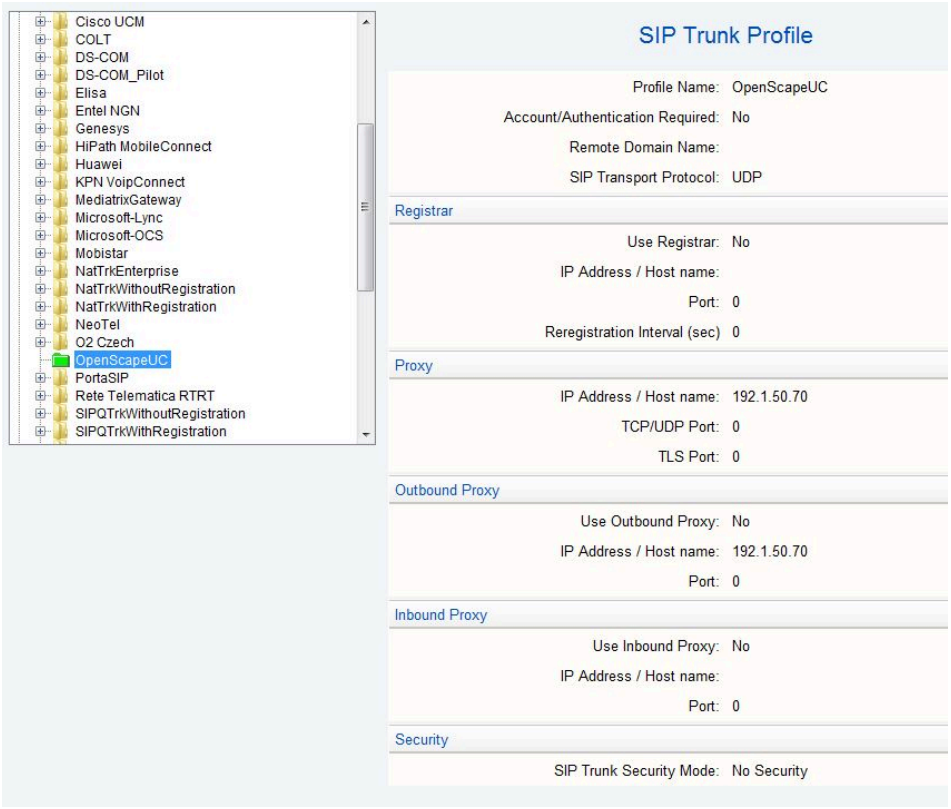


Abbildung 107: SIP Load Balancer Trunk-Profilparameter für OpenScape UC Media Server

3.9.3.3 Registrierung von Gateways

Der folgende Abschnitt enthält eine Kurzbeschreibung der Konfiguration des OpenScape 4000 SIP Load Balancers (SLB) in Verbindung mit Gateways.

Die Gateways müssen manuell hinzugefügt werden. Die Gateway-Konfiguration erfolgt im WBM des OpenScape 4000 SoftGates. Pro Gateway muss ein Eintrag konfiguriert werden.

WBM > Konfiguration > SIP Load Balancer > Einstellungen

- **Eine neue Regel im SLB hinzufügen**

  Geben Sie alle notwendigen/benötigten Parameter in die Textboxen am Ende der Seite ein und klicken Sie auf **Add Rule**.
- **Eine bestehende Regel im SLB ändern**

  Wenn eine bestehende Regel geändert werden muss, geben Sie alle notwendigen/benötigten Parameter wieder in die Textboxen am Ende der Seite ein und klicken Sie auf **Add Rule**. Es wird die bestehende Regel mit den neuen Parametern ersetzt.

Notwendige/benötigte Felder

- **LTU**

  Dieser Parameter gibt die eindeutige Kennung des Baugruppenrahmens an.

- **Slot**

  Dieses Feld kann bei OpenScape 4000 Gateways zur Angabe der Einbauteilung genutzt werden. Technisch gesehen hat es keinen Effekt auf die Funktion, dient jedoch zur Orientierung.
- **Gateway IPv4 Address**

  IP-Adresse des Gateways (z. B. 192.1.11.182)
- **IPv4 Port**

  SIP-Port des Gateways (z. B. 5060)
- **IPv4 TLS Port**

  Der SIP-Port wird für die Signalisierung von Daten verwendet, die mit TLS (Transport Layer Security) verschlüsselt sind (z. B. 5061).
- **Gateway IPv6-Adresse**

  IP-Adresse des Gateways im IPv6-Format.
- **IPv6 Port**

  Der SIP-Port wird für unverschlüsselte Signalisierungsdaten (z. B. 5060) verwendet.
- **IPv6 TLS Port**

  Der SIP-Port wird für die Signalisierung von Daten verwendet, die mit TLS (Transport Layer Security) verschlüsselt sind (z. B. 5061).
- **Routing-Nummer**

  Vorwahl-Präfix einer Telefon-Einwahlnummer (z. B. +498). Es schränkt die Nutzung der registrierten Gateways auf Telefonnummern ein, deren Präfixe mit der Routingnummer übereinstimmen (z. B. 49897000719999).
- **Maximal erlaubte B-Kanalzahl**

  Im Bestfall sollte die maximal mögliche Anzahl paralleler Kanäle eines Gateways verwendet werden. Die maximal zulässige Anzahl von B-Kanälen für Gateways beträgt 120.

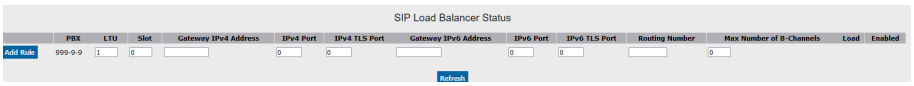


Abbildung 108: Registrierung von Gateways

3.9.3.4 Registrierung einer UC Media Server Farm

Nachfolgend sehen Sie einen ScreenShot für eine typische Konfiguration einer Media Server Farm in einem großen oder sehr großen Deployment. Jeder Media Server hat eine individuelle Konferenz-Einwahl-Nummer, die als **Trunk number** bekannt ist (z.B. +4982700332201) und eine allgemeine Konferenz-Einwahl-Nummer, die als **Additional numbers** bekannt ist (z.B. +4982700332200).

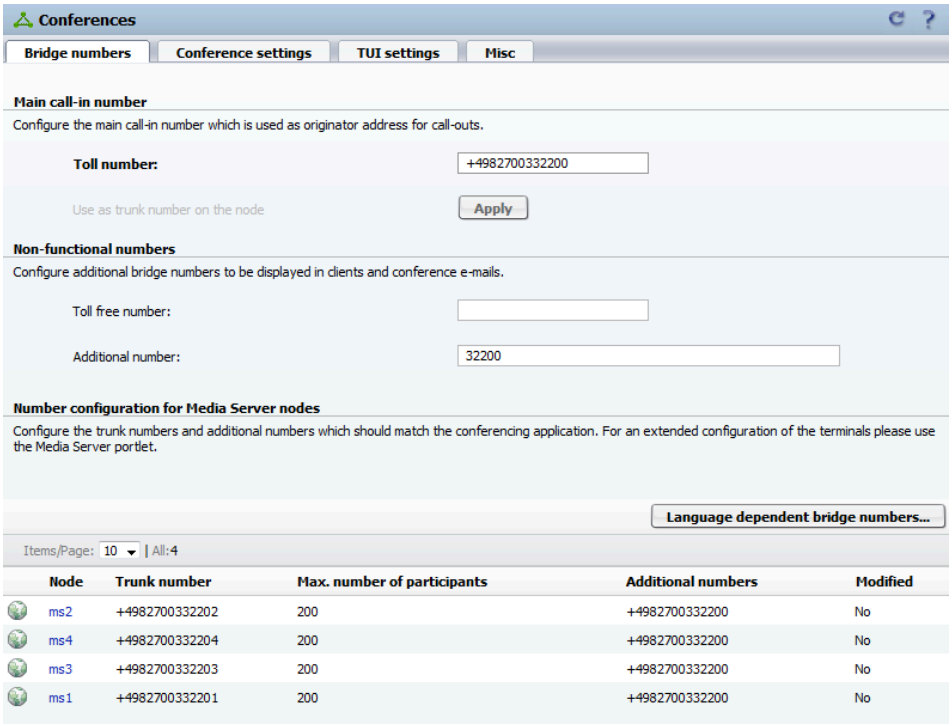


Abbildung 109: Load Balancer Status Abfrage

Der aktuelle Status des Load Balancers kann über das WBM des OpenScape 4000 SoftGates abgefragt werden.

Ein Media Servers muss manuell hinzugefügt werden. Beide Einwahlnummern, die individuell eund die allgemeine, müssen für jeden Media Server im SLB konfiguriert werden. Es werden die aktuell registrierten Gateways (Destinations) angezeigt.

Die Media Server Konfiguration wird im WBM des OpenScape 4000 SoftGate durchgeführt.

WBM > Konfiguration > SIP Load Balancer > Einstellungen

- **Eine neue Regel im SLB hinzufügen**

  Geben Sie alle notwendigen/benötigten Parameter in die Textboxen am Ende der Seite ein und klicken Sie auf **Add Rule**.
- **Eine bestehende Regel im SLB ändern**

  Wenn eine bestehende Regel geändert werden muss, geben Sie alle notwendigen/benötigten Parameter wieder in die Textboxen am Ende der Seite ein und klicken Sie auf **Add Rule**. Es wird die bestehende Regel mit den neuen Parametern ersetzt.

Notwendige/benötigte Felder

- **Slot**

  Dieses Feld wird normalerweise für die Konfiguration der OpenScape 4000-Einbauteilung verwendet. Im Falle eines Media Servers sollte dieser Parameter als eindeutige Kennung verwendet werden. Nützlich wäre die Verwendung von z. B. 1 und 11 für den ersten Medienserver zur Trennung der Konferenzeinwahlnummern, 2 und 22 für den zweiten Medienserver und so weiter.

- **Gateway IPv4 Address**

  IP-Adresse des Media Servers (z.B. 192.1.11.182)
- **IPv4 Port**

  SIP-Port des Media Servers (z.B. 5060)
- **Routing Number**

  Einwahlnummern des Media Servers (z.B. +4982700332200 für „1“ und +4982700332201 für „11“)
- **Max Number of B-Channels**

  Im Bestfall sollte die maximal mögliche Anzahl paralleler Kanäle eines jeden Media Servers verwendet werden. Aufgrund dessen kann eine Beschränkung paralleler Kanäle auf Seiten des Media Servers verhindert werden. Im Beispiel wird 2000 verwendet.

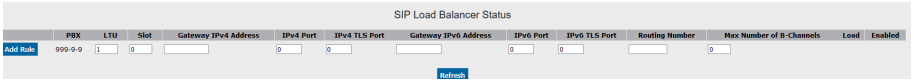


Abbildung 110: Media Server Konfiguration für SIP Load Balancing

---

Anmerkung: Information wie die OpenScape UC konfiguriert wird, finden Sie in der OpenScape UC Dokumentation.

3.10 Secure Remote Subscriber

Das Leistungsmerkmal „Secure Remote Subscriber“ stellt HFA- und SIP/UFIP-Leistungsmerkmale für einen über das Internet angeschlossenen Teilnehmer zur Verfügung. Es wird Signalisierungs- und Sprachverschlüsselung für den Remote-Teilnehmer und die Strecke durch das Internet unterstützt.

3.10.1 Leistungsmerkmalbeschreibung

Der OpenScape 4000 bietet eine IP-basierte Konnektivität zwischen dem OpenScape 4000 SoftGate (Kommunikationsdienst Signalisierung/Media Control Unit) und den Endpunkten. Diese Endpunkte können Folgendes sein:

- Der gesamte OpenScape 4000-Funktionsumfang. In den folgenden Abschnitten wird diese Funktionalität mit der Abkürzung HFA bezeichnet.
- Die Universal Feature Access IP-Sätze. In den folgenden Abschnitten wird diese Funktionalität mit der Abkürzung UFIP bezeichnet.
- Klassische SIP-Geräte (HW- oder SW-Clients), die für die VoIP-Kommunikation (Voice over IP) verwendet werden.

Eine sichere IP-Betriebsart (TLS/SSL-basiert), SPE (Signaling and Payload Encryption, Signalisierungs- und Sprachverschlüsselung), wird unterstützt, das heißt, dass die Sprach- und Signalisierungsverbindungen immer verschlüsselt sind auch wenn SPE nicht aktiviert ist. SIP/UFIP erfordert jedoch, dass SPE aktiv ist.

Die OpenScape 4000-Funktionalität kann auch auf den Telefonen in der Außenstelle des Benutzers verwendet werden. Zu diesem Zweck wird die IP-Konnektivität (HFA, SIP/UFIP) über das öffentliche Internet zum OpenScape

4000 SoftGate eingebunden. Das OpenScape 4000 SoftGate befindet sich mit einer Schnittstelle im öffentlichen Netzwerk (WAN-Schnittstelle) und mit der anderen Schnittstelle in einem Unternehmensnetzwerk (IPDA-Schnittstelle).

Für DNAT (DMZ)-Anwendungen auf SoftGate-Seite wurde auch eine erweiterte Unterstützung implementiert.

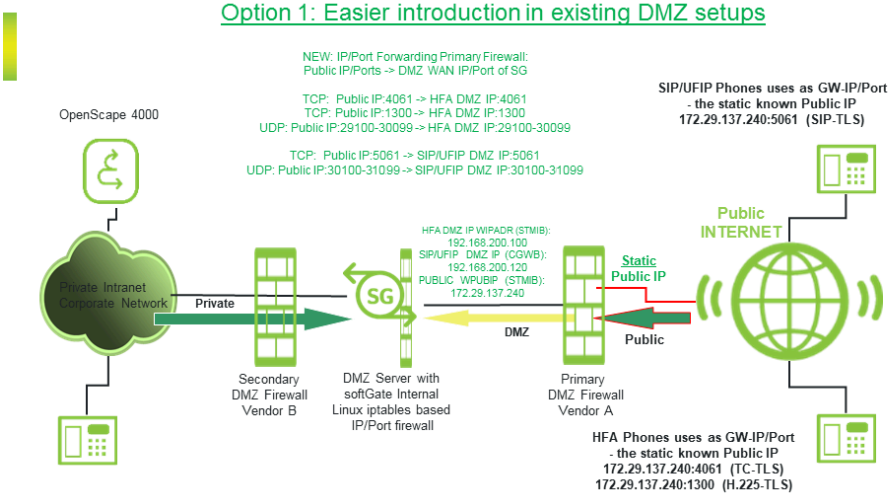
Die neuesten Informationen zu dieser Verbesserung finden Sie in den Versionshinweisen.

Im Abschnitt 14.2.4, „DMZ“ finden Sie weitere Informationen zur Konfiguration der DMZ.

3.10.1.1 Serverseitige SoftGate Destination NAT (DNAT)-Option

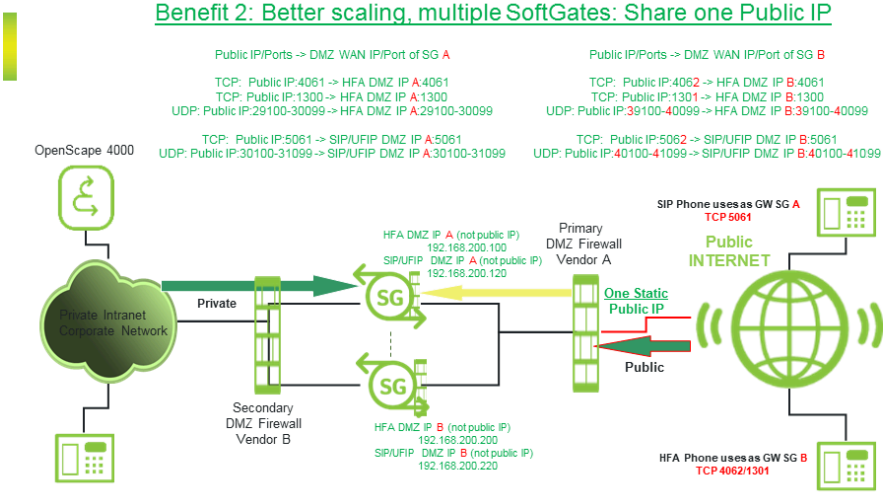
Grundkonfiguration

Option 1: Einfachere Einrichtung bei bestehenden DMZ-Konfigurationen.



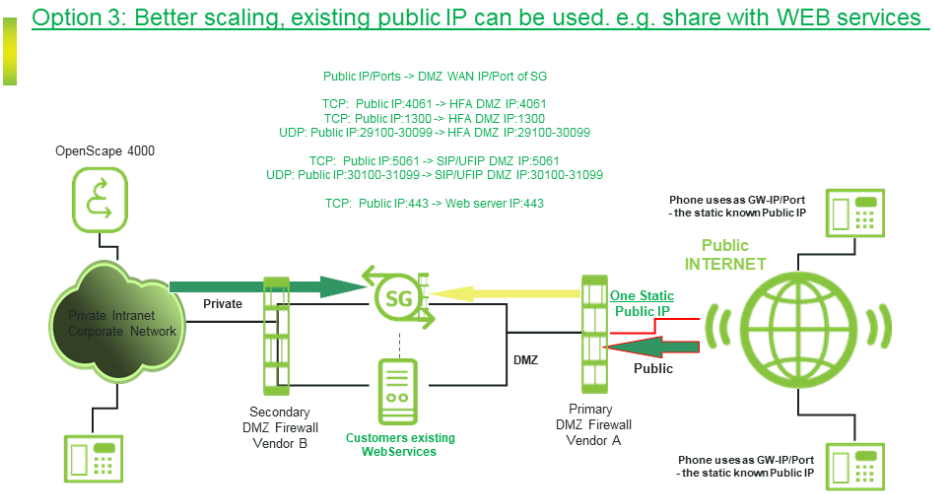
Option 1: DMZ-Szenarioübersicht mit SoftGate-DNAT-Option

Option 2: Besser skalierbar, mehrere SoftGates mit einer gemeinsamen öffentliche IP-Adresse.



Option 2: DMZ-Szenarioübersicht mit SoftGate-DNAT-Option und mehreren SoftGates

Option 3: Besser skalierbar, mögliche Verwendung einer bestehenden öffentlichen IP-Adresse (z. B. gemeinsame Nutzung der Webservices-IP-Adresse)



Option 3: DMZ-Szenarioübersicht mit SoftGate-DNAT-Option und gemeinsam genutzten kundenseitigen Webservices

3.10.2 Serviceinformationen

3.10.2.1 Voraussetzungen

- Das Leistungsmerkmal erfordert uneingeschränkten Internetzugang mit einer statischen öffentlichen IP-Adresse für den OpenScape 4000 SoftGate Server/Dienst.
- Den relevanten Telefonen muss im AMO SBCSU ein IP-Passwort zugewiesen werden.
- Das Telefon im Remote Office muss im secure Mode arbeiten, d.h es muss mit TLS registriert werden.
- Die WAN-Schnittstelle des OpenScape 4000 SoftGate benötigt ein Zertifikat. Für SIP/UFIP ist das Zertifikat für das Gateway erforderlich, an das SIP/UFIP-Teilnehmer angeschlossen sind.
- Das Telefon im Remote Office muss einen NTP-Server (z. B. Internet Pool NTP) für die Zeitsynchronisierung verwenden. Die einfachste Möglichkeit besteht darin, einen NTP-Serverpool zu nutzen (z. B. 0.de.pool.ntp.org).
- Bei Verwendung von Mobile HFA:
- Für den Aufbau eines voll funktionsfähigen Mobile HFA-Szenarios müssen die Visit- und Home-Geräte auf demselben OpenScape 4000 SoftGate konfiguriert werden, wenn das Visit-Telefon das Telefon im Remote Office ist.
- Wenn ein OpenScape Deployment Service (DLS) verwendet wird, müssen beide Dienste, DCMP und DLS, über das öffentliche Netzwerk erreichbar sein. Mehr Informationen zum Thema „Konfiguration von Home User

Endgeräten für DLS/DCMP“ finden Sie in der Administratordokumentation des OpenScape Deployment Service V8.

- Für HFA kann SRS über mehrere vSTMI-Karten in einem SoftGate verwendet werden. Daher gilt für die Funktion keine Begrenzung hinsichtlich der Anzahl der Teilnehmer, die für SRS im SoftGate konfiguriert werden können.
- Für SIP-/UFIP-Telefone ist jedoch eine dedizierte vSTMI-Karte für SRS eingerichtet und deren IP-Adresse muss der primären DMZ-Firewall bekannt sein. Außerdem müssen die entsprechenden Weiterleitungsregeln für SIP-Signalisierung und -Medien konfiguriert werden. Auf weitere vSTMI-SIP-Karten (entweder auf einem einzelnen SG oder über mehrere SoftGates) kann nur zugegriffen werden, wenn in der Firewall separate Weiterleitungsregeln erstellt wurden, die durch verschiedene Ports gekennzeichnet sind, z.B. 5061, 5062, ... etc. (siehe Kapitel 14, „Option 2: DMZ-Szenarioübersicht mit SoftGate-DNAT-Option und mehreren SoftGates“)

3.10.2.2 Allgemein

- Es gibt einen wesentlichen Unterschied zwischen SRS für HFA und SIP/UFIP:
  - HFA: Nach der Aktivierung der WAN-Einstellungen auf dem SoftGate wird bei jedem Anmeldeversuch eines Telefons ein HFA-Proxy verwendet, um die vorhandenen HG3530 vSTMI-Karten abzufragen. (Dies bedeutet, dass die HG3530 vSTMI für dieses Leistungsmerkmal keine besondere Konfiguration benötigt.)
  - SIP/UFIP: Dediziertes SIP vSTMI muss für SRS konfiguriert werden und alle Remote-Teilnehmer müssen auf dieser Karte konfiguriert werden.
- Am Remote Office-Standort werden lediglich ein Endpunkt (Telefon oder SoftClient) und ein DSL-Router (z. B. Netgear, D-Link, FRITZ!Box, etc.) benötigt. HFA-Endgeräte OpenStage, DPIP & CPx00 und die OpenScape Personal Edition Software Clients werden als Endpunkte für HFA SRS unterstützt (Info: OpenScape Personal Edition Software Clients müssen sich zusätzlich mit DLS verbinden – siehe Abschnitt 14.2.3, „Einschränkungen“). Für SIP/UFIP SRS werden OpenScape-SIP-Endgeräte und eine Vielzahl von VoIP-Softclients unterstützt.
- Die Lösung ist NAT-fähig und für mehrere HFA-Geräte hinter einem NAT-Router geeignet. Seit V7R2 unterstützt die Lösung auch eine sog. Near-End-Destination NAT (DNAT)-Option auf dem serverseitigen SoftGate. Dank dieser Option kann das SoftGate bei konfigurierter Port-Weiterleitung auch hinter einer DMZ-Firewall betrieben werden.
- Das OpenScape 4000 SoftGate bietet einen dedizierten Ethernet-Port (WAN-Schnittstelle) für die Internet-Konnektivität einschließlich der erforderlichen Firewall-Konfiguration.
- Die OpenScape 4000 SoftGate-Administration einschließlich dieses Leistungsmerkmals erfolgt vollständig über Intranet/Unternehmens-IP-Konnektivität mit dem OpenScape 4000 Host System/OpenScape 4000 Assistant. Ein externer Zugang über Internet wird nicht benötigt.
- Zentralisierte Bereitstellung über den DLS ist optional.
- Überlegungen zum Bandbreitenbedarf

  Aufgrund der Best-Effort-Eigenschaft des öffentlichen Internet kann eine zuverlässige Bandbreite für den RTP-Verkehr zwischen dem Benutzer im

Remote Office und dem WAN-Zugang des OpenScape 4000 SoftGate nicht garantiert werden.

Basierend auf unseren Erfahrungen während der Tests können wir folgende Empfehlungen abgeben.

– Teilnehmerverbindung

Für einen Benutzer mit privatem Internetzugang wird mindestens eine DSL 6000-Verbindung empfohlen (Download max. 6016 KBit/s, Upload max. 512 KBit/s). Hierbei wird davon ausgegangen, dass dieser Internet Service Provider-Zugang zugleich auch für die üblichen Büroarbeiten (z. B. E-Mail und „normale“ Webanwendungen) genutzt wird.

– OpenScape 4000 SoftGate WAN-Schnittstelle

Die Bandbreite des Internetzugangs für das OpenScape 4000 SoftGate muss sehr sorgfältig bemessen werden. Da die Geräte der Benutzer im Remote Office die DMC-Funktionalität nicht nutzen können, enden alle Anrufe (Payload Voice-Streams) im OpenScape 4000 SoftGate. Für die Berechnung der Bandbreite muss je Gerät ein Payload Voice-Stream/Kanal (gemäß klassischer PBX-Terminologie als b/d-Kanal) mit den entsprechenden Codec-Parametern basierend auf den vorhandenen Bandbreitentabellen (siehe **Gateways HG 3500 und HG 3575** > Abschnitt 2.5, „Bandbreitenbedarf“) und der Verkehrsmodellberechnung (http://intranet.mch4.global-intra.net/syseng/perfeng/tools/nert/index.htm) betrachtet werden.

Rechenbeispiel für die Bemessung des OpenScape 4000 SoftGate WAN-Zugangs mit G./11 (ohne VAD, 20 ms):

– SDSL 1000 KBit/s (Hinweis: Symmetrischer Anschluss Uplink-Geschwindigkeit/Bandbreite = Downlink-Geschwindigkeit/Bandbreite)
– Benutzer im Remote Office verwendet G.711 ohne VAD mit 30 ms Samplingzeit => 85 KBit/s
– Ergibt (1000/85 = 11,7 -> abgerundet um ~5% für Signalisierung und Nicht-Media, z.B. DLS, Picture CLIP) maximal 11 parallele Kanäle
– 11 Kanäle mit 1 % Wahrscheinlichkeit für Blockierung ergibt gemäß Erlang-Rechner 5,1599 Erlang (siehe auch **Gateways HG 3500 und HG 3575** > Abschnitt 2.7, „Verkehrsbezogene Hinweise“)
– Bei 0,15 Erlang pro Benutzer ergibt dies (5,1599/0,15 =>) maximal 34 Benutzer im Remote Office.

Rechenbeispiel für die Bemessung des OpenScape 4000 SoftGate WAN-Zugangs mit G.729 (ohne VAD, 20 ms):

– SDSL 1000 KBit/s (Hinweis: Symmetrischer Anschluss, Uplink- ist gleich Downlink-Geschwindigkeit/Bandbreite)
– Benutzer im Remote Office verwendet G.729 ohne VAD mit 20 ms Samplingzeit => 40 KBit/s
– Ergibt (1000/40 = 25 -> abgerundet um ~5% für Signalisierung und Nicht-Media z. B. DLS, Picture CLIP) maximal 24 parallele Kanäle
– 24 Kanäle mit 1 % Wahrscheinlichkeit für Blockierung ergibt gemäß Erlang-Rechner = 15,2950 Erlang (siehe auch **Gateways HG 3500 und HG 3575** > Abschnitt 2.7, „Verkehrsbezogene Hinweise“)
– Bei 0,15 Erlang pro Benutzer ergibt dies (5.1599/0.15 =>) maximal 102 Benutzer im Remote Office.

Die Kombination von normalen Benutzern und Call Center-Agenten über die WAN-Schnittstelle ist möglich. Um jedoch für Call Center-

Agenten jederzeit eine Verbindung bereitstellen zu können, wird für solche Benutzer ein Verkehrswert von 1 Erlang (36 CCS) angesetzt. Die WAN-Schnittstelle unterliegt denselben Verkehrsmodellberechnungen wie andere Kommunikationsmodelle.

- Hinweise
  - Das OpenScape 4000 SoftGate hat eine eigene Voice Firewall auf HFA-Basis. Es verhält sich also wie eine Voice-Firewall. Wenn vom Kunden aber ein zusätzlicher Schutz des OpenScape 4000 SoftGate Servers und des Unternehmens-IT-Netzwerks gefordert wird, kann dies mit der Einrichtung einer DMZ realisiert werden. Mehr Informationen finden Sie im Abschnitt 14.2.4, „DMZ“.
  - Die meisten Anbieter privater Standard-Internetverbindungen trennen die Verbindung nach Ablauf von jeweils 24 Stunden. Der Zeitpunkt dieser Zwangsabschaltung kann mit vielen der IADs gesteuert werden (z. B. 03:00h). Diese Trennung führt zum Verlust aktiver Anrufe und zur erneuten Registrierung des Telefons. Dieses Verhalten entspricht dem eines „normalen“ L1-Fehlers.
  - Bei Verwendung von Mobile HFA führt die in Anmerkung 2 beschriebene Verbindungstrennung zur Abmeldung des Mobile HFA Gerätes.

3.10.2.3 Beschränkungen

- DMC wird für Remote-Bürotelefone nicht unterstützt.

  Wenn sich das Terminal am OpenScape 4000 SoftGate registriert, wird es als ein Remote-Abonnent erkannt und somit unabhängig vom AMO SDAT Parameter **DMCALLWD** automatisch nicht wie ein DMC Endpunkt behandelt. Um partielle DMC-Routen zum letzten möglichen Endpunkt (in diesem Fall das OpenScape 4000 SoftGate selbst) zu unterstützen, wird empfohlen, **DMCALLWD** in AMO STMIB für das OpenScape 4000 SoftGate zu aktivieren.
- Die typische Plug'n'Play-Funktion wird für Remote-Abonnenten unterstützt, jedoch nicht in Verbindung mit DLS-Synchronisation. Wenn eine Synchronisation zwischen OpenScape 4000 Assistant/Manager und DLS gestartet wurde, werden die Gateway-IP-Adressen der Remote-Abonnenten in der DLS-Datenbank überschrieben. Sie müssen anschließend manuell in die WAN Gateway IP-Adresse geändert werden.
- SIP/UFIP SRS unterstützt kein "mobile HFA"-Merkmal und es ist notwendig, eine eindeutige Telefonnummer für lokale Telefone und eine andere für SRS zu haben.
- Das Merkmal Secure Remote Subscriber ist auf STMIX/STMIY nur für SIP verfügbar.
- HFA ist nur auf SoftGates möglich.
- Parallele Verbindungen von SIP SRS aus LAN und WAN zum selben Gateway sind nicht möglich. Der SRS für SIP-Telefonnummern kann nur über WAN-Schnittstelle angeschlossen werden.
- Abholgruppen werden von SIP Secure Remote Subscriber nicht unterstützt.

3.10.2.4 DMZ

In den meisten Fällen wird, wenn vom Kunden zusätzlicher Schutz gewünscht wird, womöglich eine zusätzliche Primäre DMZ Firewall ausreichen. Zuzüglich

der internen stets aktiven OpenScape 4000 SoftGate Voice Firewall könnte diese zwischen Internet und OpenScape 4000 SoftGate geschaltet werden.

Im folgenden Beispiel betrachten wir ein DMZ Szenario welches sowohl aus einer Primären als auch aus einer Sekundären DMZ Firewall besteht.

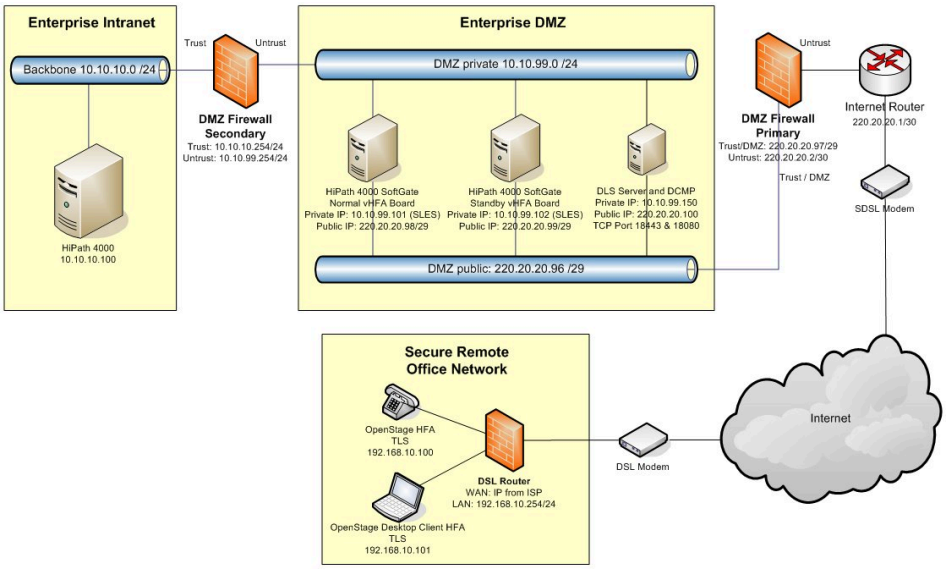


Abbildung 111: DMZ Szenario

Bild 136 zeigt einen Netzplan mit einem DMZ-Szenarios bestehend aus Corporate/Enterprise Network, DMZ Private und DMZ Public/Internet. Sollte so eine DMZ verwendet werden, muss überprüft werden, ob alle benötigten Ports in den DMZ Firewalls freigeschaltet worden sind (typischerweise DMZ Primary und DMZ Secondary Firewalls).

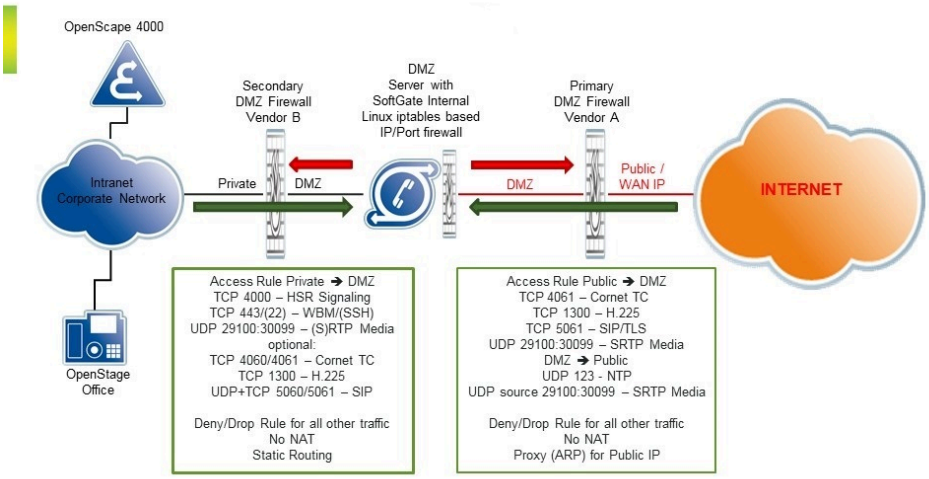


Abbildung 112: DMZ-Szenario - Benötigte Ports

Bild 137 zeigt ein DMZ Szenario aus anderer Sicht in dem genauer auf die benötigten Ports eingegangen wird. Die entsprechenden Ports und weitere Ports sind untenstehend aufgeführt und zusätzlich in der OpenScape 4000, Security Checkliste zu finden.

Die folgenden Ports (bezugnehmend auf Bild 136 und Bild 137) müssen in der Firewall geöffnet sein:

DMZ Firewall Primary

- **Internet/Public (Untrust) => DMZ Public (Trust)**
  - TCP 4061 für Cornet TC/TLS
  - TCP 1300 für H.323/TLS
  - TCP 5061 für SIP/TLS
  - UDP-Ports für SRTP-Medien (Default = 29100-30099, AMO STMIB:WANFD)

  Optional:

  - *TCP 443 für Picture CLIP*
  - *TCP 18080/18443 für DLS und DCMP (z. B. Nutzung SoftClient oder Software Lifecycle)*
- **DMZ Public (Trust) => Internet/Public (Untrust)**
  - UDP 123 für NTP Synchronisation des OpenScape 4000 SoftGates über das Internet
  - UDP-Ports für SRTP-Medien (Default = 29100-30099, AMO STMIB:WANFD)
  - Deny/Drop-Regel für den gesamten übrigen Datenverkehr
  - Keine NAT
  - Proxy (ARP) für Public IP

Anmerkung: Die Sperre des Datenverkehrs DMZ Public (Trust) => Internet/Public (Untrust) dient dazu, Missbrauch des OpenScape 4000 SoftGate-Servers und der öffentlichen IP zu verhindern

---

DMZ Firewall Secondary

- **Corporate/Enterprise Network (Trust) => DMZ Private (Untrust)**
  - TCP 4000 für das HSR-Signalisierungsprotokoll. Im Falle von Signaling Survivability bitte die entsprechenden Ports aus Kapitel „**Signaling Survivability**“ entnehmen.
  - TCP 443/22 für WBM/SSH Administrationsports
  - UDP-Ports für (S)RTP-Medien (Default = 16384-<n - Ports>) - siehe **Gateways HG 3500 und HG 3575** > Kapitel 21, „IP-Ports“.
  - UDP-Ports für (S)RTP-Medien (Default = 29100-30099) - siehe **Gateways HG 3500 und HG 3575** > Kapitel 21, „IP-Ports“.
  - Deny/Drop-Regel für den gesamten übrigen Datenverkehr
  - Keine NAT
  - Statisches Routing

  Optional:

  - *TCP 4060 für Cornet TC/TCP: HFA Endgerät registriert sich aus dem Corporate/Enterprise Network.*
  - *TCP 4061 für Cornet TC/TLS: HFA Endgerät registriert sich aus dem Corporate/Enterprise Network.*
  - UDP und TCP 5060 für SIP-Endgerät registrieren sich aus dem Unternehmensnetzwerk.
  - TCP 5061 für SIP-Endgerät registriert sich aus dem Unternehmensnetzwerk.
  - *TCP 1300 für H.323/TLS: HFA Endgerät registriert sich aus dem Corporate/Enterprise Network.*
  - *TCP 1720 für DMC (z. B. OpenScape 4000 SoftGate vNCUI DMC aktiviert)*
  - *TCP 18443/18444 für DLS Funktionalität. Je nach Nutzungsweise des DLS sind weitere Ports nötig. Siehe Openscape Deployment Service Dokumentation oder Release Note für eine detaillierte Portliste.*

- **DMZ Private (Untrust) => Corporate/Enterprise Network (Trust)**
  - UDP-Ports für (S)RTP-Medien (Default = 16384-<n-Ports>) - siehe **Gateways HG 3500 und HG 3575** > Kapitel 21, „IP-Ports“.
  - UDP-Ports für (S)RTP-Medien (Default = 29100-30099) - siehe **Gateways HG 3500 und HG 3575** > Kapitel 21, „IP-Ports“.

  Optional:

  - *TCP 1720 für H.323/TCP: HFA Endgerät registriert sich aus dem Corporate/Enterprise Network.*
  - *TCP 1720 für DMC (z. B. OpenScape 4000 SoftGate vNCUI DMC aktiviert)*
  - *UDP-Ports für DMC von optiPoints (Default=5004-ff) / OpenStage (Default=5010-ff) Endgeräten (siehe hierzu Dokumentation der Endgeräte).*
  - *TCP 443 für Backup Server (z. B. Nutzung von Automatischem Restore Konzept)*
  - *TCP 8082/8084/8085 für DLS Funktionalität: Je nach Nutzungsweise des DLS sind weitere Ports nötig. Siehe Openscape Deployment Service Dokumentation oder Release Note für eine detaillierte Portliste.*

> **Anmerkung:** Geöffnete Ports in Richtung geschütztem Corporate/Enterprise Netzwerk (sogenannte Firewall Pinholes) sind aus Sicherheitsgründen nach Möglichkeit zu vermeiden, jedoch für obengenannte Ausnahme Szenarien nötig.

3.10.2.5 Software-Lifecycle der IP-Endgeräte via DLS und HTTPS

Die OpenStage Endgeräte-Familie verfügt über zwei Möglichkeiten des Software-Upgrades, zum einen FTP und zum anderen HTTPS. In den nachfolgenden Abschnitten wird die Möglichkeit des HTTPS Verfahrens beschrieben.

3.10.2.5.1 Funktionsweise

Der DLS scannt einen HTTPS-Server, der die Endgeräte-Software bereitstellt. Daraufhin kann dem IP-Endgerät ein Job in Auftrag gegeben werden, eine bestimmte Software herunterzuladen und zu aktivieren.

3.10.2.5.2 Voraussetzung

Der DLS sowie die IP-Endgeräte müssen den HTTPS-Server (standardmäßig) per Port 443 erreichen können.

3.10.2.5.3 Hinweise zur Konfiguration

Es gibt viele verschiedene HTTPS-Server auf dem Markt. Unter Umständen besitzt der Kunde auch einen Eigenen, der mit benutzt werden kann. Der DLS-Software (Installationsdateien) liegt außerdem im Verzeichnis **tools** eine Dokumentation zur Nutzung/Einrichtung eines HTTPS-Servers bei. Ist dem der Fall, so kontaktiert das IP-Endgerät den DLS um den vorliegenden Job auszuführen. Ist dieser abgeschlossen so löscht der DLS den Contact-Me Eintrag im DCMP wieder.

- **Schritt 1: Starten der XAMPP-Software**

  Nach dem Herunterladen und dem Entpacken der XAMPP-Software kann diese mit der Datei **xampp-control.exe** gestartet werden (siehe

weiterführende Dokumentation der XAMPP-Software). Daraufhin erscheint folgendes Hauptfenster der XAMPP-Software:

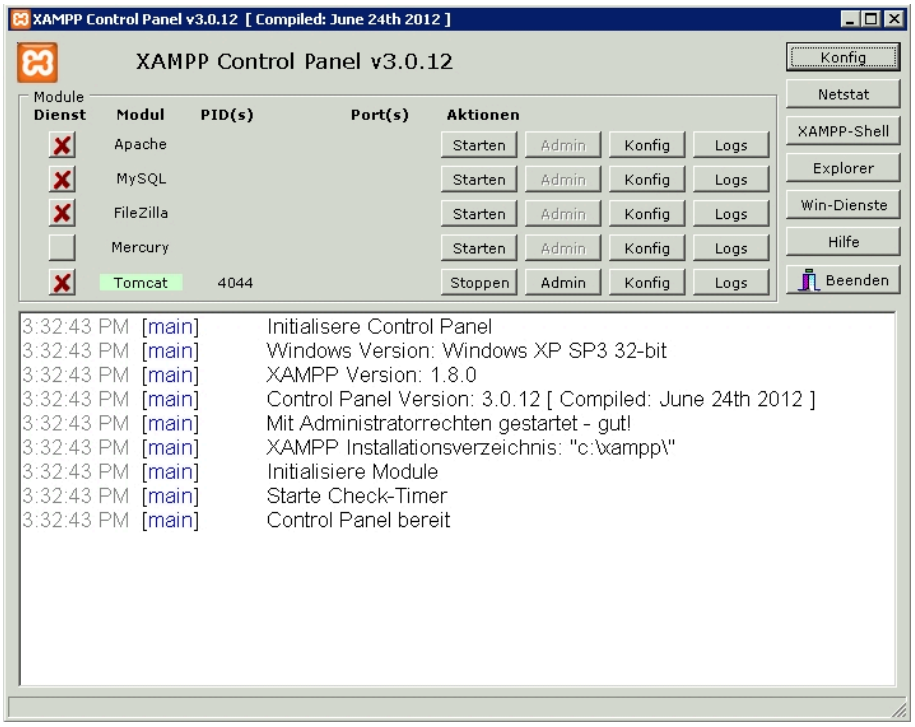


Abbildung 113: XAMPP-Hauptfenster

- **Schritt 2: Konfigurationsdateien bearbeiten**

  Für den HTTPS-Server wird Apache genutzt. Über die Schaltfläche **Konfig** (in der Apache Zeile) können die verschiedenen Konfigurationsdateien (z. B. httpd.conf, httpd-ssl.conf oder httpd-xampp.conf) mit einem Text-Editor bearbeitet werden.

  Wichtig: Folgende Schritte beschreiben nur die minimal nötige Konfiguration für einen funktionierenden HTTPS-

Server ohne Zertifizierung, Security, etc. Sicherheitaspekte werden nicht behandelt.

httpd.conf

– Sinnvoll ist z. B. die Zeile mit Listen 80 auszukommentieren (# davor setzen), da nur HTTPS Port 443 genutzt wird und nicht HTTP Port 80.
– Desweiteren muss der Software-Pfad konfiguriert werden in welchem die Endgeräte-Software auf dem HTTPS-Server liegt, z. B. **DocumentRoot** `"C:/phone_software"`.

Hier wird Slash / genutzt, nicht Backslash \.

– Als nächstes den Ordner im HTTPS konfigurieren, der unter **DocumentRoot** benutzt wird. Das ganze sollte so aussehen (Kommentare sind im folgenden weggelassen).

  <Directory "C:/ phone_software ">

  Options Indexes FollowSymLinks Includes

  AllowOverride All

  Order allow,deny

  Allow from all

  </Directory>
– Das Default Gateway wurde beim DMZ-WAN-Interface konfiguriert. Dies würde dazu führen das der Inhalt des HTTPS-Server **DocumentRoot** bei Aufruf aus einem Web-Browser nicht aufgelistet würde (möglicherweise aus Security-Gründen gewünscht).

  httpd-ssl.conf

  Hier muss ebenfalls das **DocumentRoot** konfiguriert werden, z. B. **DocumentRoot** `"C:/phone_software"`.

  Wichtig: Hier wird Slash / genutzt, nicht Backslash \.

  httpd-default.conf

  Anmerkung: Die **httpd-default.conf**-Datei kann nicht direkt über die **Konfig** Schaltfläche aufgerufen werden. Sie befindet sich unter **.\xampp\apache\conf\extra**.
– Für externe Geräte wird empfohlen die Timeouts hoch zu setzen:

  Timeout 300

  KeepAlive On

  MaxKeepAliveRequests 100

  KeepAliveTimeout 60

- **Schritt 3: Starten des Apche HTTPS-Server**

  Der Apache HTTPS-Server kann nun über die Apache-Schaltfläche **Starten** gestartet werden. Im folgenden Bild kann man sehen das der Apache gestartet wurde und nur auf Port 443 horcht.

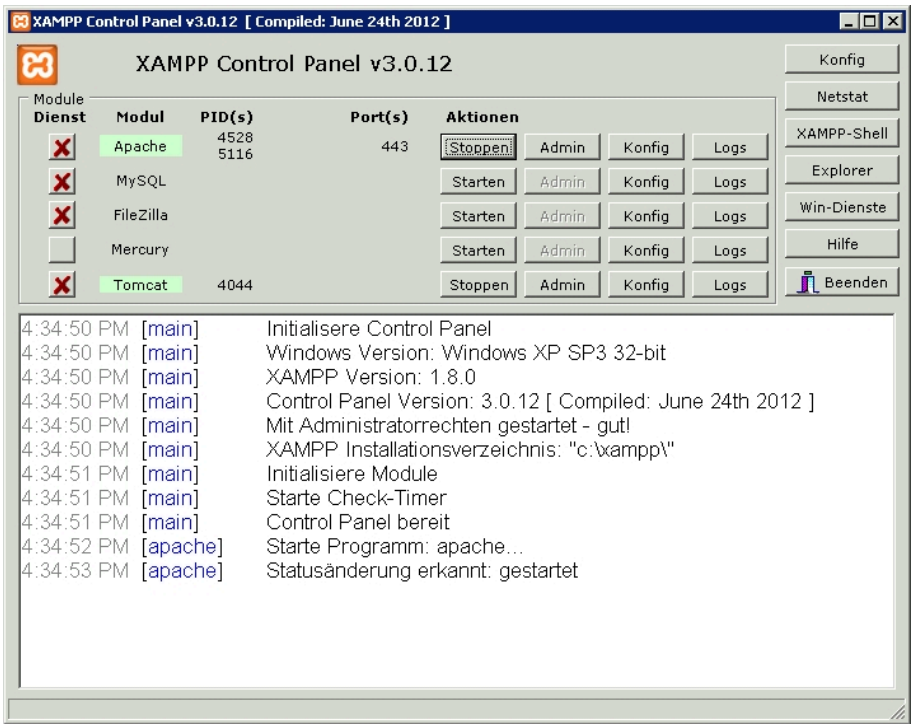


Abbildung 114: XAMPP Hauptfenster nach dem Starten des Apache HTTPS-Servers

---

Wichtig: Damit der DLS beim Scannen des HTTPS-Servers auch die im **DocumentRoot** abgelegten Endgeräte-Software-Dateien auflisten und in seine Datenbank aufnehmen kann, benötigt dieser im **DocumentRoot** die Datei **dls_directory_reader.php**. Diese liegt der DLS-Software (Installationsdateien) im Verzeichnis **tools** bei. Sie muss manuell in das **DocumentRoot** (z. B. `C:\phone_software`) kopiert werden.

Anmerkung: Eine weitere nützliche Funktion von XAMPP befindet sich unter der Schaltfläche **Netstat**. Hier wird in Echtzeit ein Netstat zum Überprüfen der offenen Ports bzw. der hergestellten Verbindungen zu dem Rechner angezeigt.

- **Schritt 4: HTTPS-Server im DLS konfigurieren**

  Der letzte Schritt ist den HTTPS-Server im DLS zu konfigurieren.

  Administration > Server Konfiguration > HTTPS Server Konfiguration

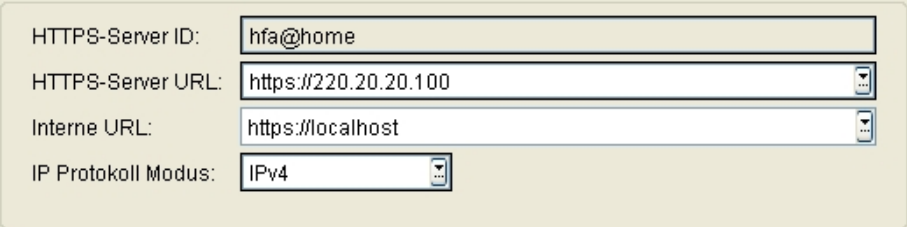


Abbildung 115: HTTPS-Server-Konfiguration bei Secure Remote Subscriber

3.10.3 Generierung (Beispiel)

Das folgende Diagramm zeigt eine grobe Übersicht der IP-Kommunikationsbeziehung zwischen dem SPE-fähigen HFA-Gerät und dem OpenScape 4000 SoftGate.

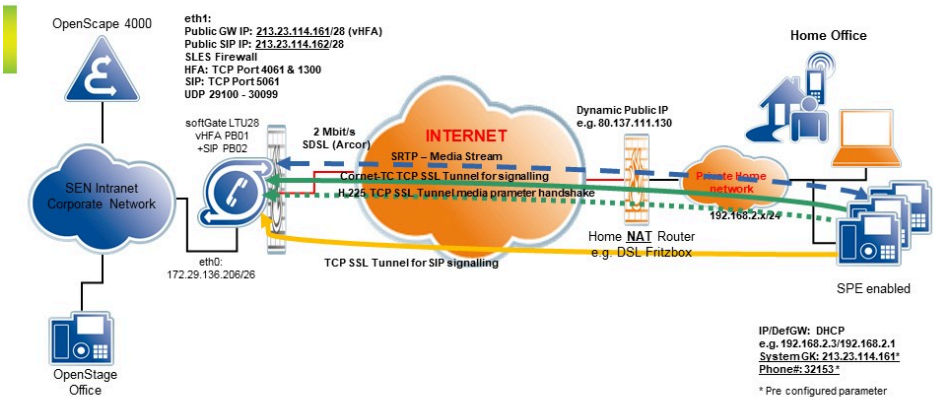


Abbildung 116: Sichere IP-Konnektivität für Remote Subscriber - Generierungsbeispiel

Konfigurationsschritte

Nach der Installation des OpenScape 4000 SoftGate müssen folgende Schritte ausgeführt werden:

1) Generieren der WAN-Schnittstelle mit AMO STMIB (IP-Adresse, Netzmaske und Standard-Router).

WAN-Schnittstellendaten:

AMO STMIB bietet die folgenden zusätzlichen Parameter in einem neuen Zweig **WANFD**:

WIPADR=<IP-Adresse>, **WNETMASK**=<IP-Adresse>, **WVLAN**=<JA/NEIN>, **WVLANID**=<nummer>, **WDEFRT**=<IP-Adresse>, WPUBIP=<IP-Adresse>

Beispiel:

```
AENDERN-
STMIB:MTYPE=NCUI2,LTU=20,TYPE=WANIF,WIPADR=10.80.144.246,WNET
MASK=255.255.248.0,WVLAN=NO,WVLANID=0,WDEFRT=10.80.144.1,WPUB
IP=172.16.1.126;
```

WANIF	WAN-Schnittstelle
WIPADR	IP-Adresse der WAN-Schnittstelle
WNETMASK	Netzmaske der WAN-Schnittstelle
WVLAN	VLAN-Tagging der WAN-Schnittstelle (JA/NEIN)
WVLANID	Virtual LAN-ID der WAN-Schnittstelle
WDEFRT	IP-Adresse des Standard-Routers im WAN-Segment
WPUBIP	Öffentliche IP-Adresse der WAN-Schnittstelle

Nach dem Ändern dieser Parameter muss ein

`EXEC-USSU:UPDATAP,<LTU_des_OpenScape4000_SoftGates>;`

des OpenScape 4000 SoftGates durchgeführt werden. Das OpenScape 4000 SoftGate wird zurückgesetzt und die Änderungen werden aktiviert.

WAN-Leistungsmerkmaldaten:

AMO STMIB bietet die folgenden zusätzlichen Parameter in einem neuen Zweig **WANFD**:

WUDPPRTL=<Nummer>, **WUDPPRTH**=<Nummer>, **WTOSPL**=<Zeichenfolge>, **WTOSSIGN**=<Zeichenfolge>, **WTLSP**=<Nummer>

Beispiel:

```
AENDERN-
STMIB:MTYP=NCUI2,LTU=20,TYP=WANFD,WUDPPRTL=29100,WUDPPRTH=300
99,WTOSPL="184",WTOSSIGN="104",WTLSP=4061;
```

WANFD	Leistungsmerkmaldaten der WAN-Schnittstelle
WUDPPRTL	Untere Grenze für den freigegebenen UDP-Port-Bereich
WUDPPRTH	Obere Grenze für den freigegebenen UDP-Port-Bereich
WTOSPL	TOS, Payload WAN abgehend für HFA
WTOSSIGN	TOS, DiffServ Code Point für HFA-Signalisierung

WTLSP	HFA TLSP-Port

Nach dem Ändern dieser Parameter muss das OpenScape 4000 SoftGate nicht zurückgesetzt werden. Es erhält die Daten sofort, nachdem der AMO die Änderungen vorgenommen hat.

WTOSSIGN	TOS, DiffServ Code Point für HFA-Signalisierung
WTLSP	HFA TLSP-Port

Nach dem Ändern dieser Parameter muss ein

RES-USSU:LTU,<LTU_des_OpenScape4000_SoftGate>;

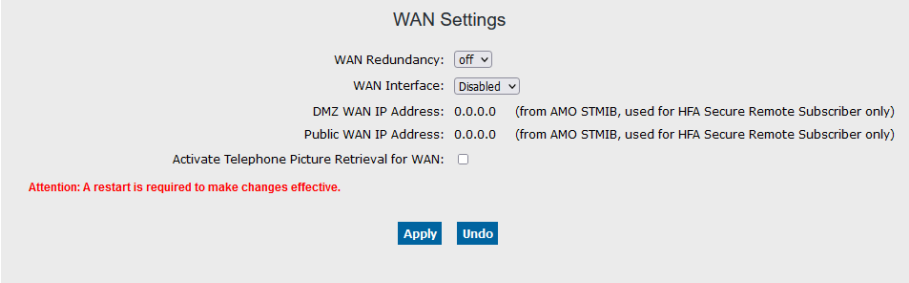
des OpenScape 4000 SoftGates durchgeführt werden. Dies führt zu einem Zurücksetzen des kompletten OpenScape 4000 SoftGates und die geänderten Daten werden aktiviert.

Anmerkung: (nur HFA) Der Standard-UDP-Portbereich von 1000 offenen Ports (Standard = 29100-30099) kann eingeschränkt werden. Hierbei muss beachtet werden, dass für jedes HFA-Endgerät im Remote Office zwei UDP-Ports zur Verfügung stehen müssen. Sollte bei einem Rufaufbau kein UDP-Port zur Verfügung stehen, wird das HFA-Endgerät mit einem L1-Fehler zurückgesetzt. Sogenannte Überbuchungen werden nicht unterstützt.

---

2) Konfigurieren der WAN-Schnittstelle des OpenScape 4000 SoftGate über das Web Based Management (WBM)

OpenScape 4000 SoftGate WBM > Konfiguration > WAN > Einstellungen



Secure Remote Subscriber – OpenScape 4000 SoftGate WAN-Einstellungen

- Wählen Sie ein **WAN Interface** aus (z. B. eth1). **Übernehmen** der Einstellungen mit anschließendem Restart des OpenScape 4000 SoftGates über den **Restart** Button im WBM.

Anmerkung: Sollte das WAN-Interface später, wie in Punkt 3 beschrieben, über AMO STMIB konfiguriert werden, so kann der Neustart aus dem WBM gespart werden. Der nötige EXEC-USSU:UPDATAP,<LTU_des_OpenScape4000_SoftGates>;

Befehl führt nämlich zu einem Zurücksetzen des kompletten OpenScape 4000 SoftGates.

- Wenn das Leistungsmerkmal Picture CLIP (siehe Kapitel 15, „Picture CLIP“) für Teilnehmer im Remote Office gewünscht wird, kann dieses hier aktiviert werden. In dem Fall wird der dafür benötigte TCP Port 443 auf dem WAN Interface geöffnet, jedoch explizit für dieses Leistungsmerkmal. Das WBM ist dadurch weiterhin nicht über das WAN Interface erreichbar.
- Wenn Gatekeeper-Redundanz für HFA-Teilnehmer gewünscht wird, muss diese ebenfalls konfiguriert werden (siehe Gatekeeper-Redundanz für HFA/SIP-Teilnehmer auf Seite 360).

3) Für die WAN-Schnittstelle des OpenScape 4000 SoftGate muss ein SPE-Zertifikat importiert werden.

OpenScape 4000 SoftGate WBM > Konfiguration > WAN > SPE > Keycert importieren

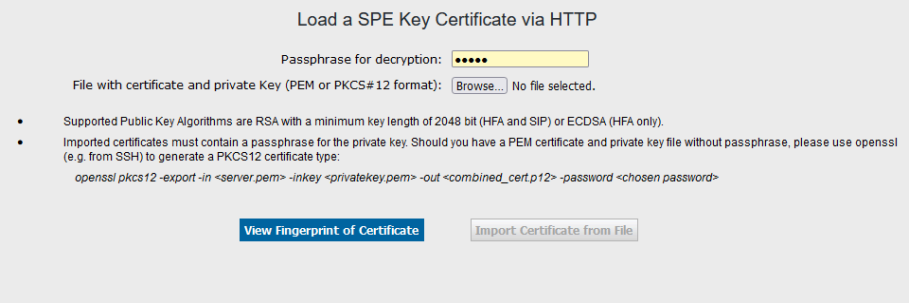


Abbildung 117: Secure Remote Subscriber - OpenScape 4000 SoftGate SPE-Zertifikat

- Der Dialog **Laden eines SPE-Schlüsselzertifikates über HTTP** wird angezeigt.

Geben Sie das Entschlüsselungskennwort ein, und suchen Sie dann das SPE-Zertifikat. Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**. Importieren Sie das Zertifikat nun, indem Sie auf die Schaltfläche **Zertifikat aus Datei importieren** klicken.

- Die Datei mit dem SPE-Zertifikat stammt entweder von einer vom Kunden festgelegten PKI-Zertifizierungsstelle (RA/CA) oder kann (sollte diese beim Kunden nicht existieren) mit dem OpenScape 4000 Assistant generiert werden. Siehe hierzu Dokumentation **Signalisierungs- und Sprachverschlüsselung** > Kapitel 5, „Generieren von SPE-Zertifikaten mit OpenScape 4000 Assistant“. Das SPE-Zertifikat muss im Format PEM oder PKCS#12 vorliegen.

4) SIP-STMI-Karte für SIP/UFIP SRS konfigurieren

WAN-Schnittstellendaten für SIP STMI:

AMO CGWB wird erweitert mit den Parametern USEWANIF

Beispiel:

```
AENDERN-
CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYPE=GLOBIF,IPADR=10.80.144.244,
NETMASK=255.255.248.0,DEFRT=10.80.144.190,USEWANIF=YES,WPUBIP
```

```
=172.16.1.126,SIPTLSP=5061;
```

IPADR IP-Adresse der SIP-WAN-Schnittstelle (eth1)

NETMASK Netzmaske der WAN-Schnittstelle

DEFRT IP-Adresse des Standard-Routers im Segment WAN

USEWANIF Aktivierung von SIP SRS auf der SIP STMI-Karte

SIPTLSP TCP/TLS-Port für sichere SIP-Kommunikation

WPUBIP Öffentliche IP-Adresse der WAN-Schnittstelle

Nach dem Ändern dieser Parameter muss ein
`RESTART-BSSU:ADDRTYPE=PEN,LTU=<LTU_of_OpenScape4000_SoftGate>,SLOT=<SIP_STMI_slot>;`

des OpenScape 4000 SoftGates durchgeführt werden. In diesem Szenario wurde der HTTPS-Server mit auf dem DLS installiert.

MANLANIF-Schnittstellenrekonfiguration für SIP STMI:

AMO CGWB unterstützt die zusätzliche Konfiguration der Management LAN-Schnittstelle (WBM), was bei der WAN-Konfiguration sehr wichtig ist, da der Zugriff auf das Webmanagement über die WAN-Schnittstelle standardmäßig durch die iptables-Regeln der internen SoftGate Firewall verboten ist. Daher sollte die zusätzliche IPDA LAN-IP-Adresse für das SIP STMI-Board-Management konfiguriert werden.

Beispiel:
```
AENDERN-CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYPE=MANLANIF,MIPADR=10.80.170.244,MNETMASK=255.255.240.0,MDEFRT=10.80.160.1;
```

MIPADR IP-Adresse, die für das WBM-Management verwendet wird (eth0)

MNETMASK Netzmaske der MANLANIF-Schnittstelle

MDEFRT IP-Adresse des Standard-Routers im Segment IPDA/MANLANIF

ASC-Konfigurationsdaten für SIP-STMI-Medienports:

AMO CGWB ermöglicht die Definition einer Reihe von SRTP-Medienports, die als Quell-/Zielports für Medienströme verwendet werden, die gegenüber SIP-Teilnehmern eingerichtet wurden.

Wenn SIP/UFIP SRS zusammen mit HFA SRS verwendet wird und sie eine einzige öffentliche IP-Adresse auf der primären DMZ-Firewall (AMO STMI WIPADR) teilen, MUSS der für den vHFA-Proxy konfigurierte Medienportbereich vom Portbereich für SIP STMI abweichen. D.h. Standardbereich 29100:30099 für vHFA und 30100:31099 für SIP STMI

Beispiel:
```
AENDERN-CGWB:MTYPE=CGW,LTU=24,SLOT=4,TYP=ASC,UDPPRTLO=30100,UDPPRTHI=31099;
```

UDPPRTLO Niedrigster UDP-Port für SRTP-Medienströme

UDPPRTHI Höchster UDP-Port für SRTP-Medienströme

Anmerkung: Die WAN-Schnittstelle ist nicht über SoftGate SIP STMI WBM konfigurierbar, aber die korrekte

Konfiguration kann in SIP STMI WBM wie folgt überprüft werden:

OpenScape 4000 SoftGate SIP STMI WBM > Konfiguration > Grundeinstellungen > Gateway



Abbildung 118: SIP-STMI-Karte für SIP/UFIP SRS konfigurieren

SPE-Zertifikat-Import in SIP-STMI-Karten:

SIP/UFIP SRS erfordert Signalisierung und Nutzlastverschlüsselung (SPE), weshalb sich entfernte SIP/UFIP-Teilnehmer nicht am OpenScape 4000 SoftGate anmelden können, wenn SPE nicht korrekt auf der für SRS vorgesehenen SIP-STMI-Karte konfiguriert ist. Es beinhaltet, beschränkt sich aber nicht auf die richtige SPE-Zertifikatskonfiguration.

OpenScape 4000 SoftGate SIP STMI WBM > Konfiguration > Sicherheit > Sicherheit > SPE importieren...

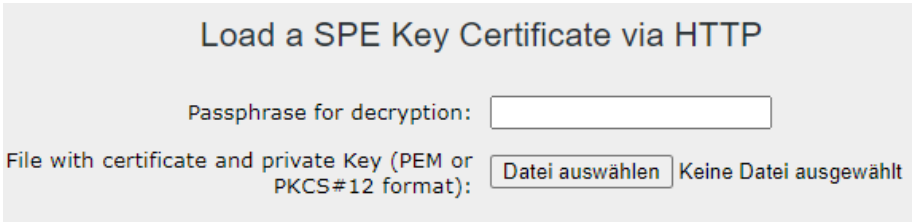


Abbildung 119: SIP-STMI-Karte für SIP/UFIP SRS konfigurieren

- Der Dialog „Laden eines SPE-Schlüsselzertifikates über HTTP“ wird angezeigt. Geben Sie das Entschlüsselungskennwort ein, und suchen Sie dann das SPE-Zertifikat. Klicken Sie auf „Fingerabdruck des Zertifikats anzeigen“. Importieren Sie das Zertifikat nun, indem Sie auf die Schaltfläche „Zertifikat aus Datei importieren“ klicken.
- Die Datei mit dem SPE-Zertifikat stammt entweder von einer vom Kunden festgelegten PKI-Zertifizierungsstelle (RA/CA) oder kann (sollte diese beim Kunden nicht existieren) mit dem OpenScape 4000 Assistant generiert werden. Siehe Dokumentation Signalisierung und Nutzlastverschlüsselung > Kapitel 5, "Generation SPE-Zertifikate mit OpenScape 4000 Assistant". Das SPE-Zertifikat muss im Format PEM oder PKCS#12 vorliegen.
- Wenn sich die HFA und die SIP/UFIP SRS die gleiche primäre DMZ-Firewall mit einer öffentlichen IP teilen, dann sind beide Zertifikate identisch - eines auf das SoftGate heruntergeladen (siehe Schritt 2.) und dieses auf das SIP STMI heruntergeladen.

5) Generieren Sie das Telefon für das Remote Office mit AMO SBCSU.

Wichtig: In AMO SBCSU muss ein IP-Passwort konfiguriert werden.

6) Konfigurieren Sie das Telefon für das Remote Office über dessen eigenes Menü.

Im Menü des Telefons müssen folgende Einstellungen vorgenommen werden:

- Gateway-IP-Adresse (=WAN-IP-Adresse des OpenScape 4000 SoftGates)
- Teilnehmerrufnummer (AMO SBCSU)
- IP-Passwort (AMO SBCSU)
- Konfigurationsschritte
- NTP-Server

Die Adresse eines NTP-Serverpools (z. B. 0.de.pool.ntp.org) sollte als NTP-Adresse eingetragen werden. Auf diese Weise erhält das Telefon stets eine Liste der aktiven NTP-Server.

Die Verwendung eines Serverpools setzt voraus, dass ein DNS-Server verfügbar ist, damit der DNS-Name aufgelöst werden kann. Wenn die Telefone über DHCP mit den Standard-Routern verbunden sind, wird der DNS normalerweise automatisch eingegeben und der Name kann aufgelöst werden. Wenn dem OpenStage-Telefon im Remote Office hingegen eine statische IP-Adresse zugewiesen ist, muss auch der DNS eingegeben werden.

Für die Zeitumstellung von Sommerzeit auf Normalzeit ändern Sie den Wert **Timezone offset (hours)** (Abweichung Zeitzone in Stunden) am Telefon von 2 in 1.

Service-Menü > Admin > ok > (Passwort = 123456*) ok > Date and time (Datum und Uhrzeit) > ok > Time source (Zeitquelle) > ok > (Zeitquelle = SNTP, SNTP IP = <IP-Adresse des NTP-Serverpools oder des NTP-Servers>**, Timezone offset (hours) (Abweichung Zeitzone in Stunden) = 1) > Save & exit (Speichern und Beenden) > ok**

*bitte beachten Sie, dass ein nicht voreingestelltes Passwort verwendet werden sollte.

- Optional: DLS-IP-Adresse

3.10.3.1 Deployment Service (DLS) und DLS Contact-Me Proxy (DCMP) - Tipps & Tricks

3.10.3.1.1 Hintergrund

Im Normalfall kontaktiert der Deployment Service (DLS) nach Joberstellung die IP-Endgeräte über Ihre IP Adresse. In unserem Remote Office Fall befinden sich die IP-Endgeräte jedoch sozusagen im Internet hinter einem NAT-Router mit lokaler IP Adresse, ergo kann der DLS diese nicht erreichen. Der DLS und die IP-Endgeräte unterstützen hierfür eine eigens entwickelte Lösung mit der IP-Endgeräte hinter einem NAT-Router administriert werden können. Diese heißt DLS Contact-Me Proxy (DCMP). In dieser Lösung wird die Kommunikation immer vom IP-Endgerät eröffnet.

3.10.3.1.2 Hintergrund

Die IP-Endgeräte pollen hierzu in einer festgelegten Poll-Time den DCMP und prüfen, ob dieser einen Job beim DLS für das jeweilige IP-Endgerät an hand der Device-ID vorliegen hat. Ist dem der Fall, so kontaktiert das IP-Endgerät den DLS um den vorliegenden Job auszuführen. Ist dieser abgeschlossen, so löscht der DLS den Contact-Me Eintrag im DCMP wieder.

3.10.3.1.3 Anforderungen

IP-Voraussetzung:

Damit die IP-Endgeräte den DLS und den DCMP erreichen können, müssen beide über eine öffentliche IP-Adresse für die IP-Endgeräte erreichbar sein. Im Falle vom Remote Office Szenario also aus dem Internet erreichbar sein.

Hardware-Voraussetzung:

Der DLS-Server benötigt für diese Lösung zwei Netzwerkkarten. Die eine Netzwerkkarte stellt die Verbindung in das Corporate/Enterprise Network her und die zweite ist für die Verbindung zu den IP-Endgeräten im Internet / NAT-Router gedacht.

3.10.3.1.4 Konfigurationshinweise

Die folgenden Beispiele/Hinweise beziehen sich auf die Konfiguration des DLS aus dem Beispiel DMZ Szenario (Bild 137) im Abschnitt 14.2.4, „DMZ“.

- Zunächst müssen unter Windows die beiden Netzwerkkarten konfiguriert werden.

```
C:\Documents and Settings\dls-dmz>ipconfig
Windows IP Configuration
Ethernet adapter DMZ WAN:
        Connection-specific DNS Suffix  .
        IP Address. . . . . . . . . . . . : 220.20.20.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.248
        Default Gateway . . . . . . . . . : 220.20.20.97
Ethernet adapter DMZ LAN:
        Connection-specific DNS Suffix  .
        IP Address. . . . . . . . . . . . : 10.10.99.150
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

- Das Default Gateway wurde beim DMZ-WAN-Interface konfiguriert. Deshalb muss für das DMZ-LAN eine permanent statische Route konfiguriert werden um das Corporate/Enterprise Network zu erreichen.

```
C:\Documents and Settings\dls-dmz>route ADD -p 10.10.0.0 MASK
255.255.0.0 10.10.99.254
C:\Documents and Settings\dls-dmz>route print
===========================================================
WUDPPRTH
0x1 ........................... MS TCP Loopback interface
0x2 ...00 1b 21 15 3d 7b ...... Intel(R) PRO/1000 MT Server Adapter - Packet
Scheduler Miniport
0x3 ...00 19 99 19 95 09 ...... Broadcom NetXtreme Gigabit Ethernet - Packet
Scheduler Miniport
===========================================================
===========================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     220.20.20.97   220.20.20.100       20
```

```
        127.0.0.0        255.0.0.0         127.0.0.1       127.0.0.1       1
        10.10.0.0      255.255.0.0      10.10.99.254    10.10.99.150       1
       10.10.99.0    255.255.255.0      10.10.99.150    10.10.99.150      20
    10.10.99.150  255.255.255.255        127.0.0.1       127.0.0.1      20
    10.10.255.255  255.255.255.255     10.10.99.150    10.10.99.150       20
     220.20.20.96  255.255.255.248    220.20.20.100   220.20.20.100       20
   220.20.20.100  255.255.255.255        127.0.0.1       127.0.0.1      20
   220.20.20.255  255.255.255.255    220.20.20.100   220.20.20.100       20
        224.0.0.0        240.0.0.0     10.10.99.150    10.10.99.150       20
        224.0.0.0        240.0.0.0    220.20.20.100   220.20.20.100       20
  255.255.255.255  255.255.255.255     10.10.99.150    10.10.99.150       1
  255.255.255.255  255.255.255.255    220.20.20.100   220.20.20.100       1
Default Gateway:    220.20.20.97
===========================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
        10.10.0.0      255.255.0.0     10.10.99.254       1
```

- Installieren Sie den DLS auf dem Windows-Rechner mit DCMP (in diesem Beispiel ist der DCMP mit auf demselben Rechner installiert). Sollte der DLS bereits ohne DCMP installiert worden sein, so kann dieser nachträglich installiert werden. Eine detaillierte Servicedokumentation finden Sie in der Administratordokumentation zu **OpenScape Deploymentservice V8 > Installation und Erstkonfiguration > DCMP einrichten**.
- Konfigurieren Sie den DCMP indem Sie mit einem Web-Browser auf **http://<ip address>:18080/dcmp** gehen. Der Benutzername ist “admin". Wenn das DCMP zusammen mit dem DLS installiert wurde, ist das Passwort das gleiche wie das Admin-Passwort für das DLS.
- Bitte überprüfen bzw. konfigurieren Sie unter Cluster Setup das Feld **Local Host**. Dieses enthält die IP-Adresse des DCMP-Servers. In diesem Beispiel wird nur ein Standalone DLS ohne DLS Cluster betrachtet. Weiterführende Informationen entnehmen Sie bitte der Administratordokumentation zu **OpenScape Deploymentservice V8**.

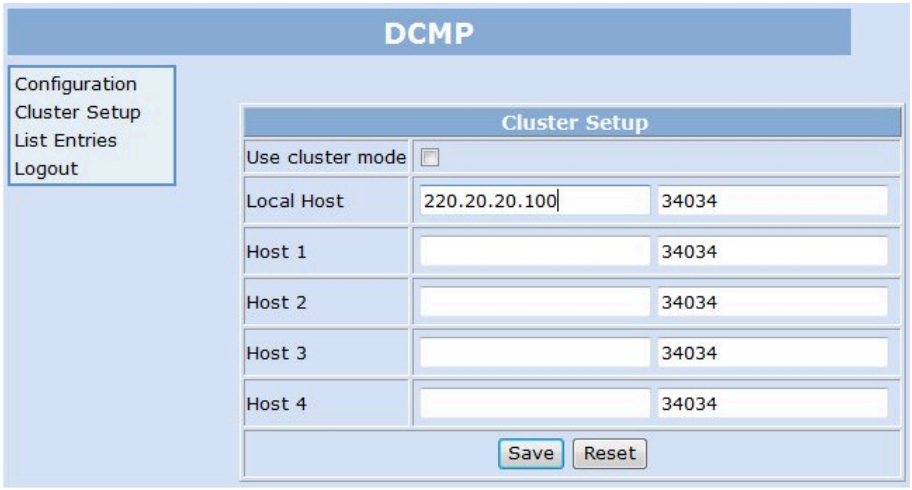


Abbildung 120: DCMP-Konfiguration für Secure Remote Subscriber

- Im nächsten Schritt muss der DLS für DCMP konfiguriert werden.

Klicken Sie auf die Schaltfläche **Toggle DCMP** unter **Administration > Workpoint Interface Configuration > DCMP**, um das DCMP zu aktivieren.

Wenn das DCMP auf dem DLS-Computer läuft, wird die IP-Adresse des DCMP-Servers im Feld **DLS-DCMP Host** (oder localhost) angezeigt, andernfalls muss sie hier eingegeben werden.

Um die Kommunikation zwischen DLS und DCMP zu testen, klicken Sie auf die Schaltfläche **Test**.

Die IP-Adresse, die von den IP-Terminals kontaktiert werden soll, muss im Feld **Device - DCMP Host** eingetragen werden (also die IP-Adresse, die von außen zugänglich sein soll).

Definieren Sie einen oder mehrere **Device IP Bereiche**. Jedes IP-Endgerät innerhalb der IP-Bereiche, die durch **IP Adresse von** und **IP Adresse bis** definiert sind, wird über den DCMP aktualisiert. Somit sendet der DLS immer dann, wenn eine Änderung an einem Telefon innerhalb einer der aufgelisteten IP-Bereiche vorgenommen wird, eine Nachricht an den DCMP mit der Aufforderung, den Contact-Me-Eintrag für dieses Telefon zu setzen. In unserem Beispiel ist die Problematik das nicht immer klar ist von welchem Internet Service Provider das jeweilige IP-Endgerät seinen IP-Adressbereich erhält. Somit haben wir den gesamten IP-Adressbereich, mit Ausnahme des Corporate/Enterprise Network, eingetragen. Sollten genaue IP-Adressbereiche bekannt sein, können natürlich nur die benötigten eingetragen werden. Beispiel: IP-Endgeräte melden sich nur von einem einzelnen ISP an bei welchem der IP-Adressbereich bekannt ist.

Dem jeweiligen IP-Adressbereich muss außerdem ein **Poll Intervall** zugewiesen werden. Es beinhaltet, beschränkt sich jedoch nicht auf die ordnungsgemäße Konfiguration des SPE-Zertifikats. Für Testzwecke kann ein sehr kurzes Poll-Intervall gewählt werden (z. B. 1 Minute). Im Live-Betrieb werden längere Intervalle empfohlen.

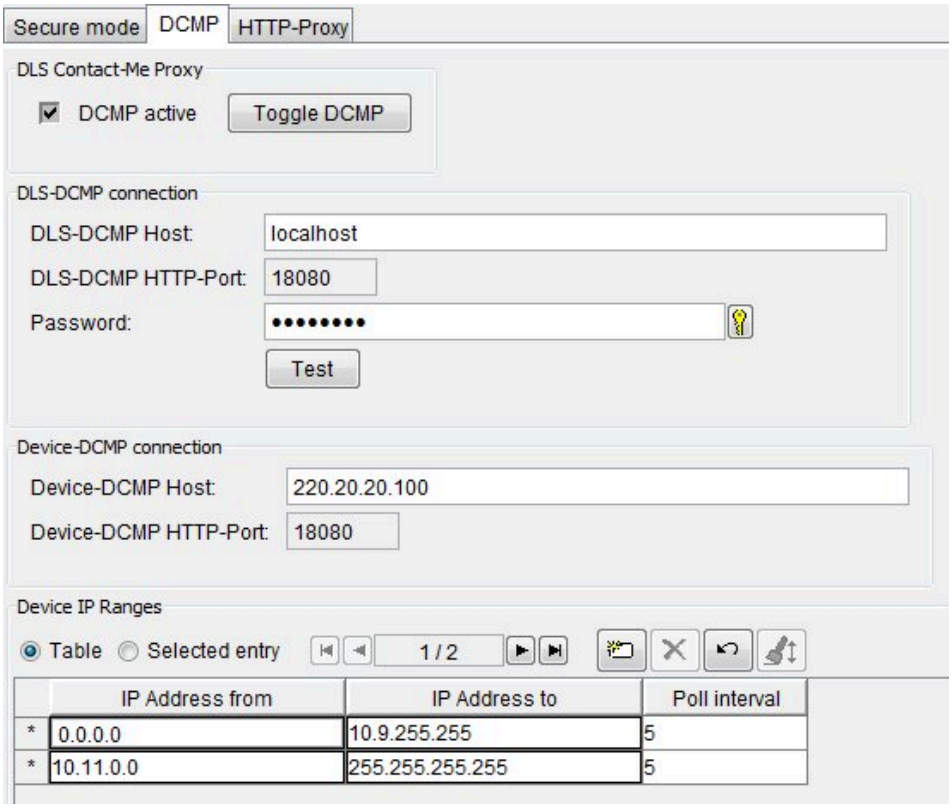


Abbildung 121: DLS für DCMP konfigurieren

- Geben Sie das Entschlüsselungskennwort ein, und suchen Sie dann das SPE-Zertifikat.
- Nach Eintragen der DLS/DCMP IP-Adresse (im Beispiel die 220.20.20.100) an einem Endgerät im Remote Office, meldet sich das IP-Endgerät am DLS an. Da die IP des IP-Endgerätes aus einem IP-Adressbereich stammt (öffentliche Internet-IP-Adresse des Remote Office NAT-Routers) welches zuvor unter der DCMP-Konfiguration eingegeben wurde, bekommt das IP-Endgerät mitgeteilt dass dies ein DCMP-Endgerät ist.

  Gehen Sie auf **IP Devices > IP Device Verwaltung > IP Device Konfiguration >** Register **DCMP**. Die Checkbox **DCMP aktiv** sollte aktiviert sein.

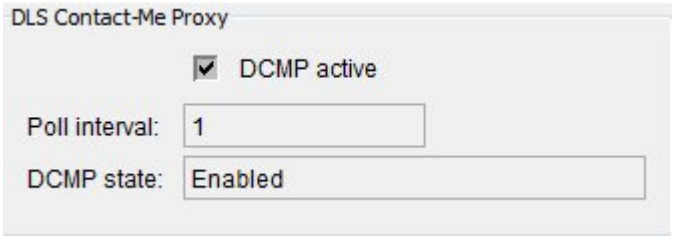


Abbildung 122: DLS-/DCMP-Konfiguration mit einem IP-Endgerät im Remote Office testen

Um die Funktion zu testen, gehen Sie zu **IP Devices > IP Phone Konfiguration > Gateway / Server** des zuvor neu angemeldeten IP-

Endgerätes und starten sie ein Lesen der Konfiguration. Hiermit wurde ein Job erstellt. Zu sehen in **Job Koordination > Job Kontrolle**.

Auf der DCMP-Benutzeroberfläche klicken Sie auf das Menü **List Entries**. Sie sollten den Contact Me-Auftrag in der Liste sehen. Die **Device ID** sollte die MAC-Adresse des Telefons sein.

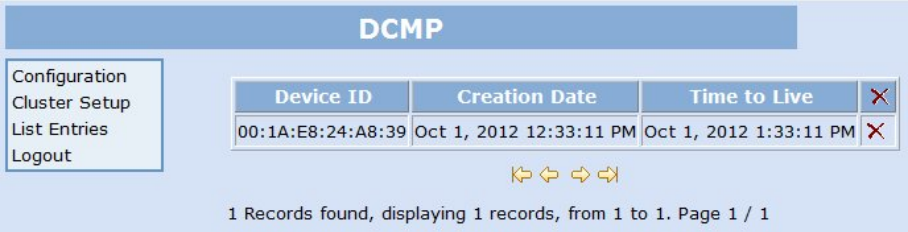


Abbildung 123: DCMP - List Entries Menü vor Abholung des Contact-Me-Auftrages

Der Job sollte dann, nachdem das IP-Endgerät sich den Auftrag vom DCMP abgeholt hat, abgeschlossen werden. Im DCMP **List Entries** Menü verschwindet der Auftrag ebenfalls nach dem Abholen.

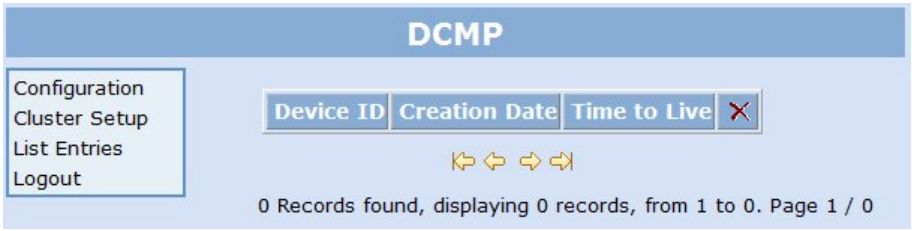


Abbildung 124: DCMP - List Entries Menü nach Abholung des Contact-Me-Auftrages

---

Anmerkung: Sollte der Job nicht ausgeführt/abgeholt werden, kann ein Wireshark Trace auf DLS bzw. DCMP Seite zur Fehlerdiagnose helfen. Im Wireshark Trace müssen eingehende Pakete auf dem standardmäßigen Port 18080 vom IP-Endgerät (IP-Adresse des Remote Office NAT-Routers) eingehen. Dies ist das Pollen des IP-Endgerätes zum DCMP. Anschließend muss die Kommunikation vom IP-Endgerät zum DLS über dem standardmäßigen Port 18443 erfolgen zur Job-Ausführung.

- Eine weitere DLS-Einstellung welche in unserem Beispiel sinnvoll ist, ist die Standard Job Ausführungsart unter **Job Koordination > Job Konfiguration**. Standardmäßig ist hier **Sofort ausführen** eingestellt. Im Falle von Secure Remote Subscribern kann es unter Umständen sein, dass die Nutzer Ihre IP-Endgeräte im Remote Office ausschalten bzw. vom Netz trennen. Somit würden die Jobs nach einer gewissen Zeit nicht ausgeführt und mit „Zeit überschritten“ ablaufen. Hier empfiehlt sich auf **Sofort oder nach Registrierung** umzustellen.

3.11 Picture CLIP

3.11.1 Leistungsmerkmalbeschreibung

Das Leistungsmerkmal „Picture CLIP“ bietet die Möglichkeit, zentral gespeicherte Kontaktdaten (Name und Bild) des Gesprächspartners im Display eines IP-Telefons anzuzeigen.

Für die Anzeige zentral gespeicherter Kontaktdaten fordern die OpenStage-Telefone die Daten von einem OpenScape 4000 SoftGate an. Dieser leitet die Anfrage an einen zentralen Verzeichnisserver weiter, ruft die Daten ab und stellt sie anschließend den OpenStage-Telefonen zur Verfügung.

Das Anzeigeformat (Position, Darstellung, Größe usw.) der Kontaktdaten entspricht dem beim Nachschlagen im lokalen Telefonbuch verwendeten Anzeigeformat, da in beiden Fällen derselbe Mechanismus genutzt wird.

Der Verzeichnisserver wird für alle Nummern abgefragt. Wenn auf dem LDAP-Verzeichnisserver ein Eintrag zu der Nummer gefunden wird, werden der Name und das Bild vom Verzeichnisserver angezeigt. Wenn auf dem Verzeichnisserver kein Eintrag zu der Nummer gespeichert ist, wird der Name aus dem lokalen Telefonbuch angezeigt.

Anmerkung: Bei einem vom Telefon abgehendem Ruf wird im Rufzustand das Bild für den angerufenen Kontakt nicht angezeigt, da hier das Ruf-Symbol (z. B. Frei-, Besetzt-, Umleitungs-Symbol, etc.) dargestellt werden muss. Bei Zustandekommen des Gesprächs wird das Bild dann angezeigt.

Derzeit werden zwei verschiedene Modi für den Abruf von Bildern unterstützt:

Direkter Abruf von Bildern:

Vorbedingungen:

- Direkter Abruf von Bildern konfiguriert.
- Kontaktdaten mit Bild auf dem LDAP-Server gespeichert.

=> Dem Benutzer werden der Name und das Bild des Gesprächspartners aus dem LDAP-Verzeichniseintrag angezeigt.

Das OpenStage-Telefon führt einen sogenannten lookup (Nachschlagen) zum OpenScape 4000 SoftGate durch. Das OpenScape 4000 SoftGate leitet die Anfrage weiter zum LDAP-Server und empfängt Name und Bild der abgefragten Rufnummer. Name und Bild werden dann zusammen vom OpenScape 4000 SoftGate zum OpenStage-Telefon weitergeleitet und im Display angezeigt.

Indirekter Abruf von Bildern:

Vorbedingungen:

- Indirekter Abruf von Bildern konfiguriert.
- Kontaktdaten auf dem LDAP-Server gespeichert, mit gültigem Verweis auf ein Bild, das auf einem anderen Webserver gespeichert ist.

=> Dem Benutzer werden der Name des Gesprächspartners aus dem LDAP-Verzeichniseintrag und das auf dem Webserver gespeicherte Bild angezeigt.

Das OpenStage-Telefon führt einen sogenannten lookup (Nachschlagen) zum OpenScape 4000 SoftGate durch. Das OpenScape 4000 SoftGate leitet die Anfrage weiter zum LDAP-Server und empfängt Name und eine URL des Webservers mit zugehöriger Photo-ID wo das Bild gespeichert ist. Im nächsten Schritt empfängt das OpenScape 4000 SoftGate das Bild anhand der zuvor

erhaltenen URL und Photo-ID. Name und Bild werden dann zusammen vom OpenScape 4000 SoftGate zum OpenStage-Telefon weitergeleitet und im Display angezeigt.

3.11.2 Serviceinformationen

- Dieses Leistungsmerkmal wird für OpenScape 4000 SoftGate und OpenScape Access 500 unterstützt.
- Wenn kein Bild verfügbar ist, werden nur der Name und die Nummer aus dem LDAP-Verzeichniseintrag angezeigt.
- Wenn der LDAP-Verzeichnisserver nicht erreichbar ist, wird nach Ablauf einer bestimmten Zeitspanne der PBX-Name angezeigt.
- Dieses Leistungsmerkmal wird nur von OpenStage 60 HFA und OpenStage 80 HFA unterstützt.
- Die OpenStage-Telefone müssen das OpenScape 4000 SoftGate oder die OpenScape Access 500, welche für Picture CLIP konfiguriert ist, erreichen können. Die OpenStage-Telefone müssen also nicht zwingend auf dem jeweiligen OpenScape 4000 SoftGate oder OpenScape Access 500 eingerichtet sein.
- Die OpenStage-Telefone akzeptieren nur im jpg-Format codierte Bilder mit einer Größe von maximal 50 KB.
- Für die zentrale Speicherung der Kontaktdaten und Bilder wird ein LDAP-Verzeichnisserver benötigt. Für den indirekten Abruf von Bildern ist zusätzlich ein Webserver erforderlich.
- Die Kontaktdaten werden auf dem LDAP-Verzeichnisserver mit den per WBM im OpenScape 4000 SoftGate konfigurierten Schlüsseln gespeichert.
- Es wird empfohlen, Telefonnummern im vollqualifizierten Format mit Landeskennzahl und Ortskennzahl zu speichern (z. B. 4989700754321). Wenn die Rufnummern mit Trennzeichen wie Klammern, Bindestrichen oder Pluszeichen gespeichert werden (z. B. +49 (89) 7007-54321), muss der LDAP-Verzeichnisserver bei der Rufnummernabfrage Umsetzungsregeln anwenden. Das OpenStage-Telefon verwendet für eine LDAP-Abfrage reine Ziffernfolgen ohne Trennzeichen.
- Die Kontaktdaten des LDAP-Verzeichnisservers werden unter Umständen erst nach kurzer Verzögerung angezeigt, da eine sichere Verbindung über https zum OpenScape 4000 SoftGate aufgebaut werden muss. Während dieser Zeit könnte der im OpenScape 4000 System hinterlegte Displayeintrag kurz angezeigt werden. Im Modus des indirekten Abrufs ist ein weiterer Request/Response-Zyklus erforderlich um das Bild abzurufen.

3.11.3 Generierung (Beispiel)

3.11.3.1 Konfiguration des OpenScape 4000 SoftGate

Die OpenScape 4000 SoftGate-Konfiguration stellt die für den Zugriff auf den LDAP-Verzeichnisserver benötigten Informationen bereit. Es muss möglich sein, vom OpenScape 4000 SoftGate aus über IP auf den LDAP-Verzeichnisserver zuzugreifen.

Die Konfiguration des OpenScape 4000 SoftGate erfolgt über WBM.

Konfiguration > Picture CLIP

- Direkter Abruf von Bildern:

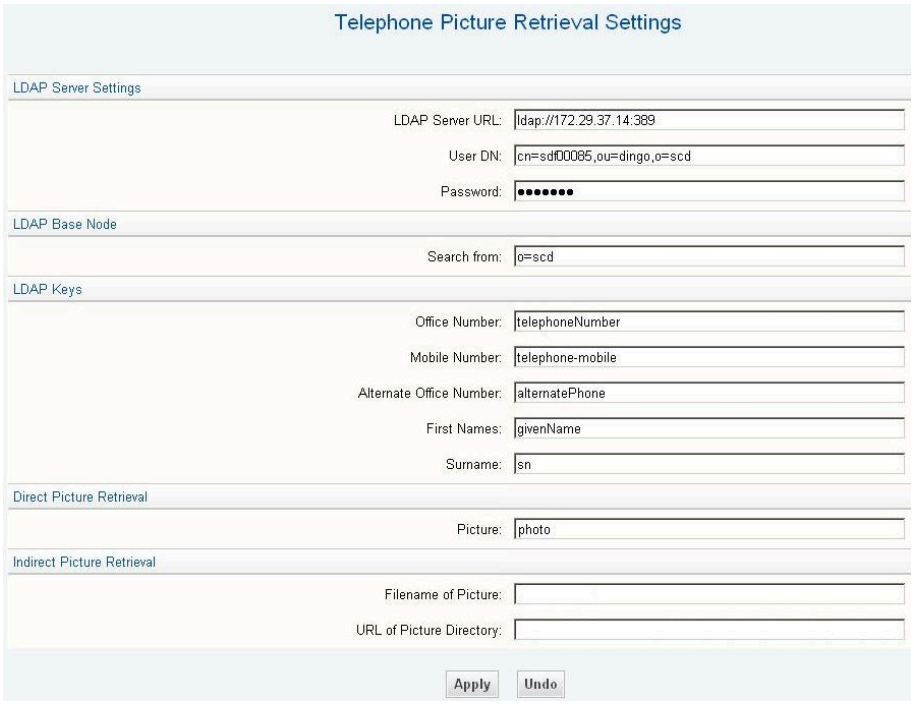


Abbildung 125: Konfiguration des direkten Abrufs von Bildern in OpenScape 4000 SoftGate

- Indirekter Abruf von Bildern:

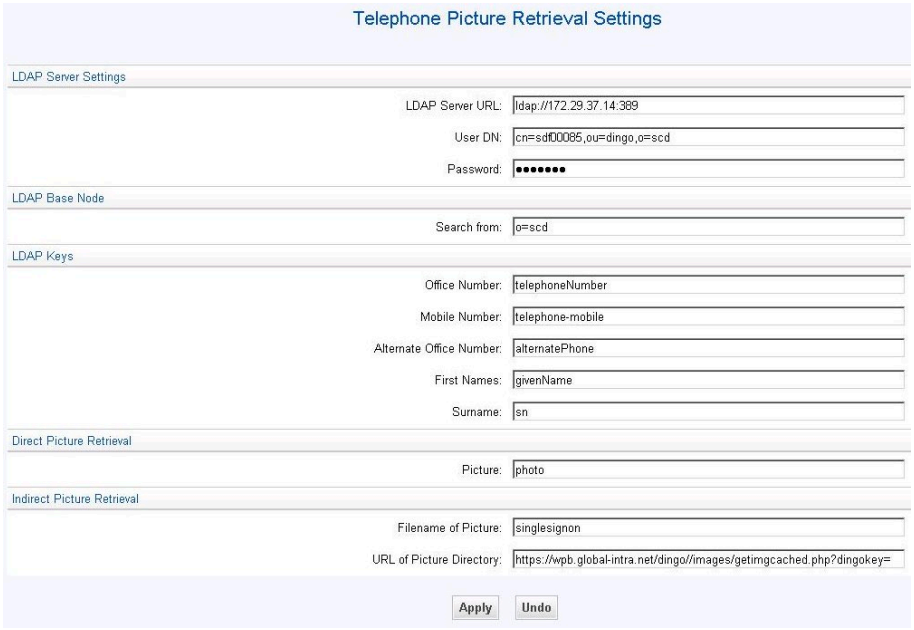


Abbildung 126: Konfiguration des indirekten Abrufs von Bildern in OpenScape 4000 SoftGate

---

Wichtig: Die unter **Einstellungen für Picture CLIP** konfigurierten Einträge müssen mit den Einträgen auf dem LDAP-Verzeichnisserver übereinstimmen.

Die Felder **Bild** (für den direkten Abruf von Bildern) und **Bilddateiname** (für den indirekten Abruf von Bildern) enthalten die passenden Schlüssel auf dem LDAP-Verzeichnisserver für das Bild, das angezeigt werden soll.

Weitere Informationen zur LDAP-Konfiguration finden Sie unter LDAP-Verzeichnisserver-Konfiguration.

3.11.3.2 Telefonkonfiguration

Die Telefonkonfiguration stellt die für den Zugriff auf das OpenScape 4000 SoftGate benötigten Informationen sowie Informationen zur Betriebsart bereit.

Die Konfiguration kann über das Menü des lokalen Telefons, die Webschnittstelle (WBM) oder den OpenScape Deployment Service (DLS) erfolgen.

Konfiguration über das Menü des Telefons

Admin > Applications (Applikationen) >XML applications (XML-Applikationen) > Add application (Applikation hinzufügen)

Dies sind im Wesentlichen die Daten für die Konnektivität zu dem Server, auf dem das Leistungsmerkmal gehostet wird (in der Regel das OpenScape 4000 SoftGate), und die Betriebsart.

- **Display name** (Anzeigename):

  Der im Anwendungsregister des Telefondisplays angezeigte Name der Applikation. Geben Sie **ldap** ein.
- **Application name** (Applikationsname):

  Wird intern zur Identifikation der auf dem Telefon ausgeführten XML-Applikation verwendet. Geben Sie **ldap** ein.
- **Server address** (Serveradresse):

  Die IP-Adresse des OpenScape 4000 SoftGate (z. B. 172.29.136.224).
- **Server port** (Serverport):

  Die Nummer des vom Server zur Bereitstellung der XML-Dokumente für die Applikation verwendeten HTTP-Ports. Hängt vom konfigurierten Protokoll ab, OpenScape 4000 SoftGate lässt jedoch nur **443** zu.
- **Protocol** (Protokoll):

  Das für die Kommunikation mit dem Server verwendete Protokoll. Wählen Sie **https**, da OpenScape 4000 SoftGate nur **https** zulässt.
- **Program name** (Programmname):

  Geben Sie **ldap** ein.
- **Use Proxy** (Proxy verwenden):

  Muss auf **Nein** gesetzt werden.

Anmerkung: Die übrigen Konfigurationselemente werden für das Leistungsmerkmal derzeit nicht ausgewertet.

Wichtig: Wenn das Leistungsmerkmal **deaktiviert** werden soll, müssen die LDAP-Einstellungen gelöscht werden.

Kanonische Telefoneinstellungen

Für den Abruf von Kontaktdaten beim LDAP-Verzeichnisserver wird bei einem ankommenden Anruf die Rufnummer des Anrufers gemäß den kanonischen Wähleinstellungen (**Admin > Local functions (Lokale Funktionen)> Locality (Ort)> Canonical settings (Kanonische Einstellungen)**) konvertiert. Das Format der resultierenden Nummer sollte mit dem Format der auf dem LDAP-Verzeichnisserver gespeicherten Rufnummern übereinstimmen. Es wird empfohlen, die Rufnummern in das vollqualifizierte Format umzuwandeln, der Teilnehmernummer also die Landeskennzahl und die Ortskennzahl voranzustellen. Dadurch ist sichergestellt, dass die nachgeschlagene Nummer eindeutig ist.

Beispiel:

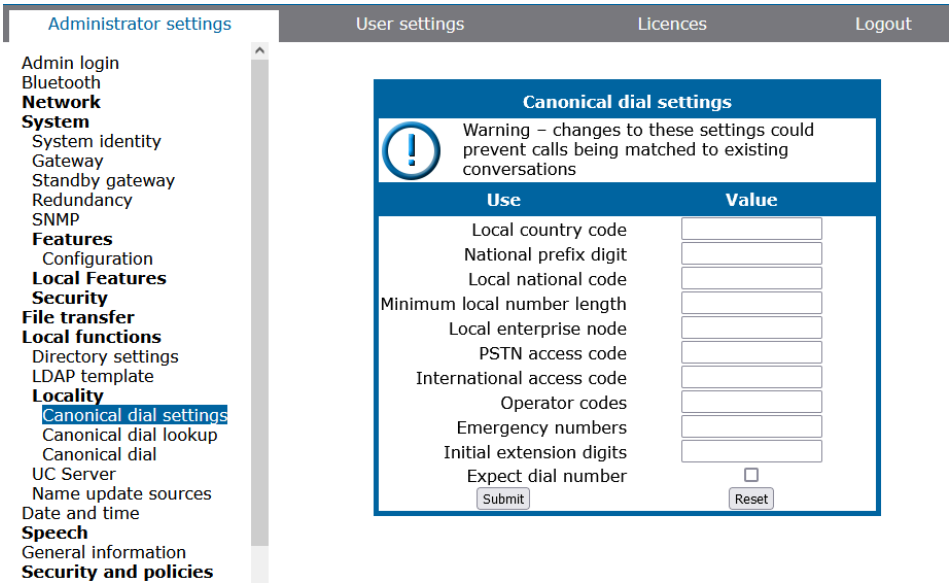


Abbildung 127: Kanonische Einstellungen für den Abruf von Bildern

Telefonkonfiguration per OpenScape Deployment Service

IP Devices (IP-Geräte)> IP Phone Konfiguration (IP-Telefonkonfiguration)> Applications (Applikationen)

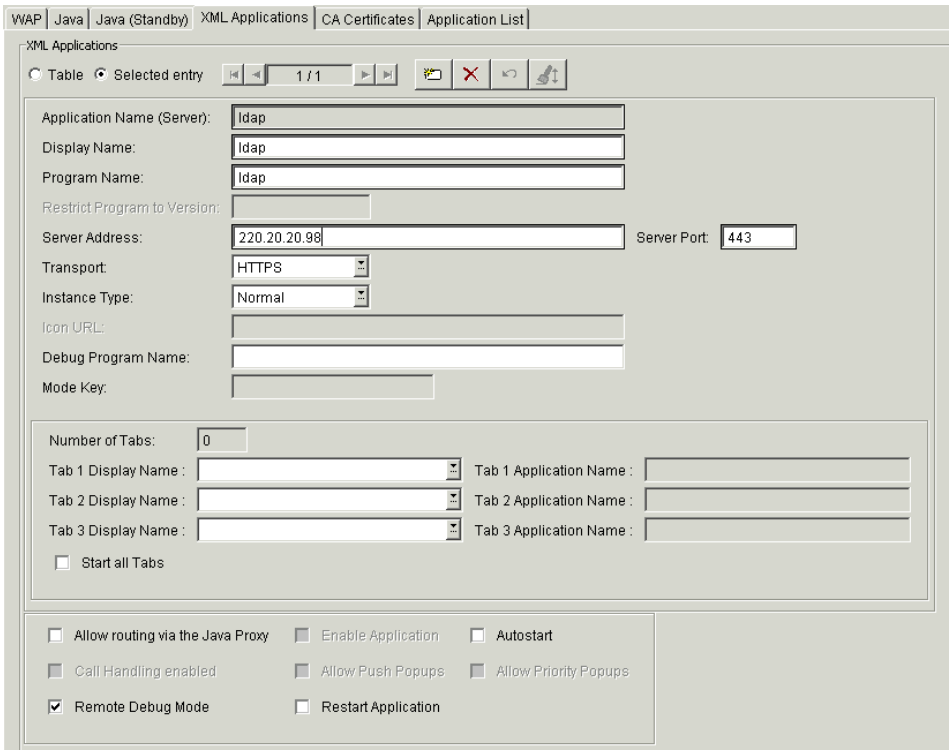


Abbildung 128: Konfiguration des Abrufs von Bildern per DLS

Registerkarte **XML Applications** (XML-Applikationen):

- **Application name** (Name der Applikation):

  Geben Sie **ldap** ein.

- **Display name** (Anzeigename):

  Geben Sie **ldap** ein.
- **Program name** (Programmname):

  Geben Sie **ldap** ein.
- **Server address** (Serveradresse):

  Geben Sie die IP-Adresse des OpenScape 4000 SoftGate ein.
- **Server port** (Serverport):

  Geben Sie den Serverport des OpenScape 4000 SoftGate ein.
- **Transport**:

  Wählen Sie die Einstellung **http** oder **https**. OpenScape 4000 SoftGate unterstützt nur **https**.

3.11.3.3 LDAP-Verzeichnisserver-Konfiguration

Der LDAP-Verzeichnisserver muss eine LDAP V2- oder V3-Schnittstelle bereitstellen und den Zugang mit passwortbasierter („einfacher“) Sicherheit ermöglichen.

Die Kontaktdaten werden auf dem LDAP-Verzeichnisserver mit den per WBM im OpenScape 4000 SoftGate konfigurierten Schlüsseln gespeichert.

Es wird empfohlen, Telefonnummern im vollqualifizierten Format mit Landeskennzahl und Ortskennzahl zu speichern (z. B. 4989700754321). Wenn die Rufnummern mit Trennzeichen wie Klammern, Bindestrichen oder Pluszeichen gespeichert werden (z. B. +49 (89) 7007-54321), muss der LDAP-Verzeichnisserver bei der Rufnummernabfrage Umsetzungsregeln anwenden. Das OpenStage-Telefon verwendet für eine LDAP-Abfrage reine Ziffernfolgen ohne Trennzeichen.

Beispiel für eine LDAP-Struktur:

Die Einträge in der Spalte **Attributtyp** (rot gekennzeichnet) müssen per WBM-Konfiguration für das OpenScape 4000 SoftGate bereitgestellt werden (siehe Konfiguration des OpenScape 4000 SoftGate).

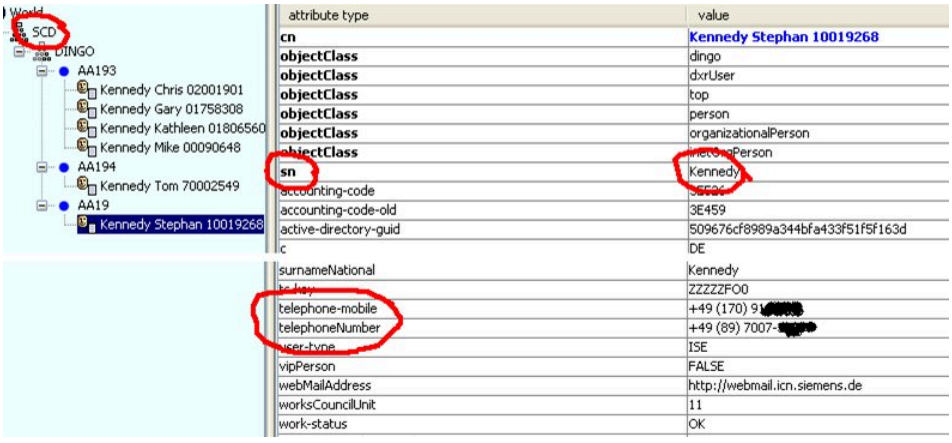


Abbildung 129: LDAP-Server - OpenScape 4000 SoftGate-Daten

Die unten stehende Abbildung zeigt die Knoten, in denen die Telefonkontaktdaten zu finden sind.

Der Ausgangsknoten für die Suche wird mit o=scd ausgewählt.

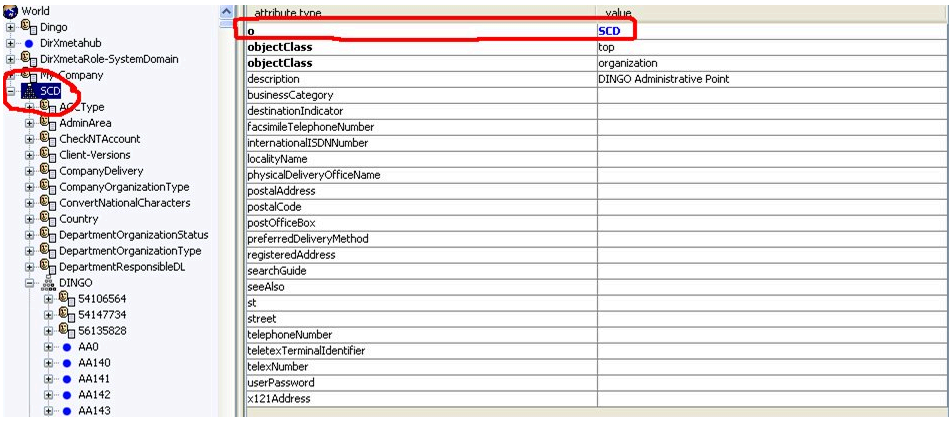


Abbildung 130: LDAP-Server - Telefonkontaktdaten

Ein weiteres Beispiel mit einem anderen LDAP-Verzeichnisserver im direkten Modus:

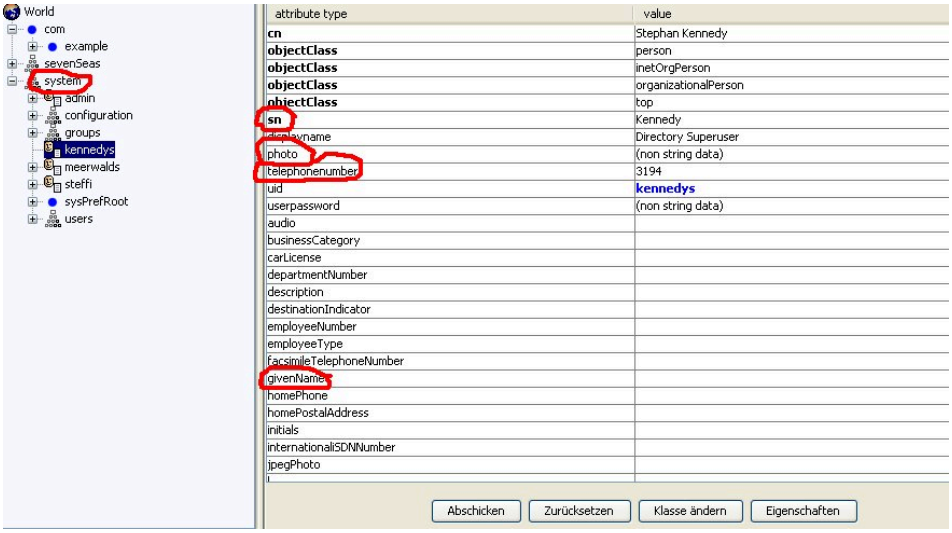


Abbildung 131: LDAP-Server - Beispiel für den direkten Abruf von Bildern (01)

Wie Sie sehen, ist die Knotenstruktur auf diesem Server sehr einfach. Der Ausgangsknoten wird mit ou=system ausgewählt.

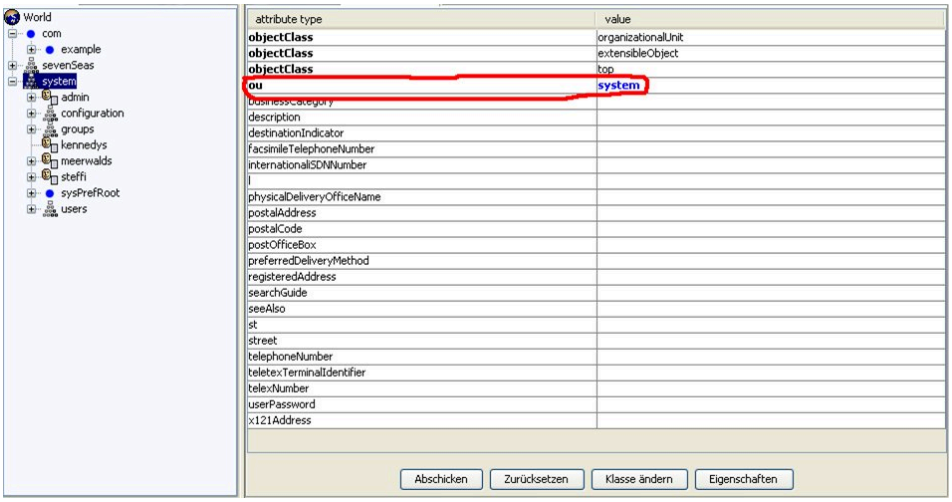


Abbildung 132: LDAP-Server - Beispiel für den direkten Abruf von Bildern (02)

3.11.3.4 LDAP-Zugang testen

Man kann im WBM des OpenScape 4000 SoftGate prüfen, ob der LDAP-Server-Zugang korrekt konfiguriert ist.

Hierfür muss man die Funktion **Picture Clip > Test** im Menü **Konfiguration** aufrufen.

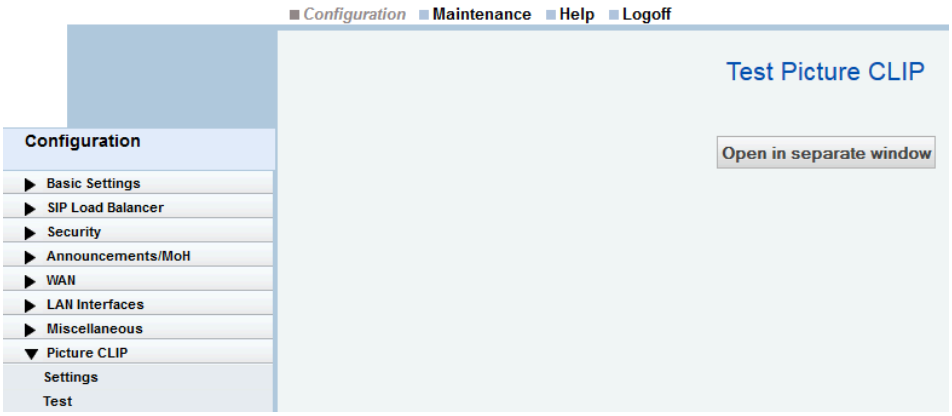


Abbildung 133: LDAP-Server-Zugangstest aufrufen

Nun klicken Sie auf die Schaltfläche **In separatem Fenster Öffnen**.

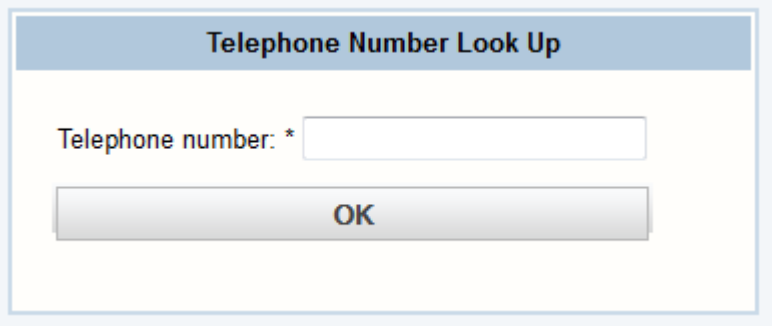


Abbildung 134: Telefonnummernsuche über LDAP-Server

Geben Sie nun eine Rufnummer ein und klicken Sie auf **Ok**.

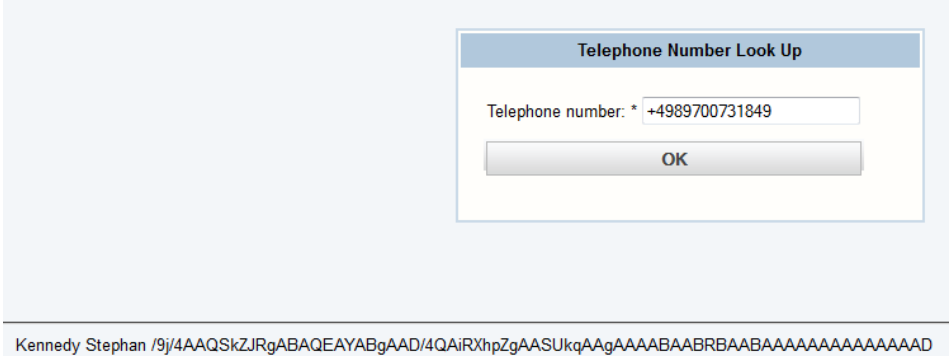


Abbildung 135: LDAP korrekt konfiguriert

Wenn der LDAP-Server-Zugang korrekt konfiguriert ist und zu der Rufnummer im LDAP ein Eintrag existiert, wird am unteren Rand ein „Ergebnis“ angezeigt.

Man kann den Nachnamen und Vornamen erkennen. Die Zeichen danach bedeutet, dass außerdem ein Bild vorhanden ist.

Wenn der LDAP-Server-Zugang falsch konfiguriert ist, kommt eine eindeutige Fehlermeldung.

Beispiel:

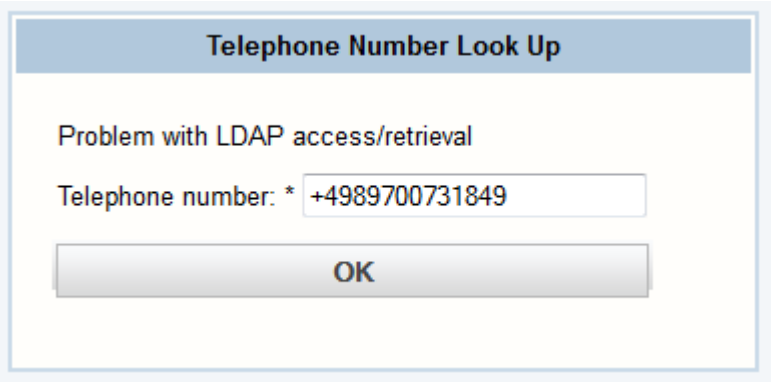


Abbildung 136: LDAP nicht korrekt konfiguriert

Somit kann man also direkt nach dem Einrichten der LDAP-Server-Konfiguration testen ob die Parameter richtig sind.

3.12 MFC-R2

3.12.1 Leistungsmermalbeschreibung

MFC/R2 ist ein Signalisierungsprotokoll für die Bereitstellung der Signalisierung zwischen Telefonanlagen. Die Signalisierung kann über analoge (TMxxx) oder digitale (DIUx) Amtsleitungen mit kanalgebundener CAS-Signalisierung erfolgen.

MFC-R2-Signale werden von vSIUX2 bereitgestellt. Die SIUX-Funktionalität wurde in Form einer virtuellen Baugruppe für OpenScape 4000 SoftGate/ OpenScape Access 500 eingeführt.

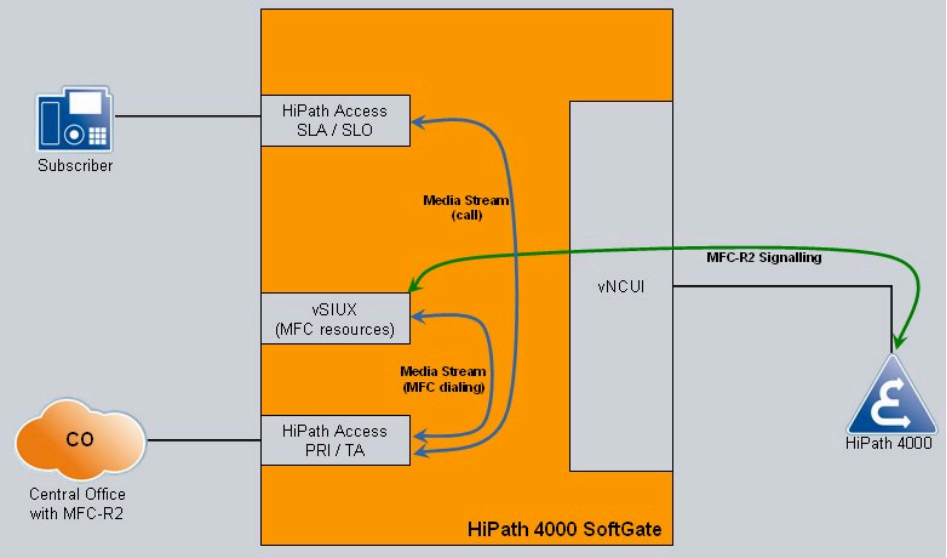


Abbildung 137: MFC-R2

Weitere Informationen zu MFC-R2 finden Sie in der Servicedokumentation:

- OpenScape 4000, Band 3 - Anwendungsfälle für Leistungsmerkmale > Netzwerke > MFC-R2-Signalisierung.

3.12.2 Serviceinformation

MFC-R2 in Verbindung mit OpenScape 4000 SoftGate/OpenScape Access 500 wird unterstützt.

3.12.3 Generierung (Beispiel)

Die in ITU-T Q.400-Q490 beschriebene digitale Version der MFC-R2-Leitungssignalisierung kann in OpenScape Access mit dem OpenScape Access PRI-Modul konfiguriert werden.

Die DIUT-Baugruppe muss mit der E1/CAS-Funktionalität (FCTID=2) konfiguriert werden. Beispiel:

```
EINRICHTEN-BCSU:MTYP=DIU, LTG=1, LTU=19,
 EBT=3, SACHNR="Q2335-
X", LWVAR=0, FCTID=2, HWYBDL=A, ALARMNR=0, MACADR=00-1A-
E8-32-60-
5E, TDMLAW=0;
```

Außerdem muss eine vSIUX2 konfiguriert werden. vSIUX2-Baugruppen werden genauso konfiguriert wie Standard-SIUX2-Baugruppen. Die MFC-R2-Funktionalität wird durch Konfigurieren der Q2341-X-Funktion ID3 ausgewählt. Im Rahmen der ID3-Funktion stellt vSIUX nur einen MFC-Teilbereich von R2 bereit, d. h. die MFC-R2 Forward- und Backward-Funktionalität (andere MFC-Varianten wie R1, SOCOTEL oder MFP werden nicht unterstützt).

Je nach Konfiguration können Sie auf dieser Baugruppe maximal 8 MFC-R2-Empfänger und MFC-Sender einrichten. Diese arbeiten immer paarweise und werden ebenso paarweise konfiguriert. Beispiel:

```
EINRICHTEN-BCSU:MTYP=SIUP, LTG=1, LTU=19,
 EBT=5, SACHNR="Q2341-
X", MFCTYP=R2B&R2B&R2F&R2F&R2F&R2F&R2F&R2F,
 LWVAR=0, FCTID=3;
```

Dies ist die Konfiguration für 2 Backward-Sender (mit 2 Forward-Empfängern) und 6 Forward-Sender (mit 6 Backward-Empfängern).

Andere SIUX-Funktionalitäten (z. B. MVF, ANI ...) sind in vSIUX2 nicht implementiert. Wenn die Baugruppe durch AMO konfiguriert wird, bleibt sie nicht verfügbar.

Wichtig: Die Initialisierung kann in einem aktiven System durchgeführt werden, wird aber erst beim erneuten Laden (AMO USSU) des Rahmens aktiviert. AMO BCSU gibt keinen Hinweis darauf, dass ein Neustart durchgeführt werden muss.

Initialisierung von MFC-Signalen

Eine Standardinitialisierung der MFC-Signale (Frequenz und Dämpfung) wird im vSIUX2-Code durchgeführt. Hierbei wird die Frequenz aller Signale gemäß Q.441 von ITU-T Q.400-Q490 festgelegt und die Dämpfung auf -8 dBm0 eingestellt.

Für nationale Applikationen können mithilfe spezieller Initialisierungsdateien besondere Signaldefinitionen bereitgestellt werden. Standardmäßig stehen auf der Festplatte des Systems drei verschiedene Dateien bereit.

- APSP/LTG/LG25/PZJSMFD0 ist die Initialisierungsdatei für Standardsignale, A-Law
- APSP/LTG/LG25/PZJSMFD1 ist die Initialisierungsdatei für Standardsignale, µ-Law
- APSP/LTG/LG25/PZJSMFD2 ist die Initialisierungsdatei für Signale für Brasilien (A-Law, -13 dBm0)

Die Initialisierungsdatei kann durch AMO ZAND ausgewählt werden. Beispiel:

`AENDERN-ZAND:TYP=SIUXPER,PEGMFC=2;` für Brasilien

Standardmäßig ist die Initialisierungsdatei 0 ausgewählt. Ergänzend zur Signalbeschreibung ist in der Datei auch angegeben, welche HWY/TSL für welche SIUX-Leitung verwendet werden muss.

3.13 OpenScape Cordless E-Integration

Das OpenScape 4000 SoftGate unterstützt die DECT-Funktionalität Cordless Multicell Integration (CMI). Dies bedeutet, dass neben HFA- und SIP-Teilnehmern auch schnurlose DECT-Teilnehmer in einem OpenScape 4000 SoftGate konfiguriert werden können.

OpenScape Cordless Enterprise V7 - 3.9.3 Synchronisierung der Taktkette. Diese Informationen sind im WBM verfügbar (OpenScape 4000 V8, vHG 3575 für OpenScape 4000 SoftGate Dokument – Abschnitt 4.8.1.2 Peripheriekarten, 4.8.1.4 OpenScape Access Clocking).

3.13.1 Leistungsmerkmalbeschreibung

Um das Leistungsmerkmal „OpenScape Cordless E Integration“ nutzen zu können, muss im OpenScape 4000 SoftGate eine softwarebasierte Anschlusseinheit „virtual Subscriber Line Cordless“ (**vSLC**) eingerichtet werden. Die vSLC bietet wie auch die SLC24-Leitungskarten die Möglichkeit bis zu 127 Cordless Handsets zu generieren. Die vSLC fungiert als virtuelle Home-SLC für alle verwalteten Teilnehmer. Die Visit-SLCs bilden mit den DECT-Basisstationen die Location Areas auf dem Gelände.

Durch Hinzufügen weiterer vSLC-Baugruppen kann die Anzahl der CMI-Teilnehmer im OpenScape 4000 SoftGate erhöht werden. Bis zu 6 vSLC mit maximal 650 Mobilteilen (0,15 ERL pro Mobilteil) können in einem OpenScape 4000 SoftGate eingerichtet werden.

Anmerkung: Basisstationen können an die vSLC derzeit nicht angeschlossen werden.

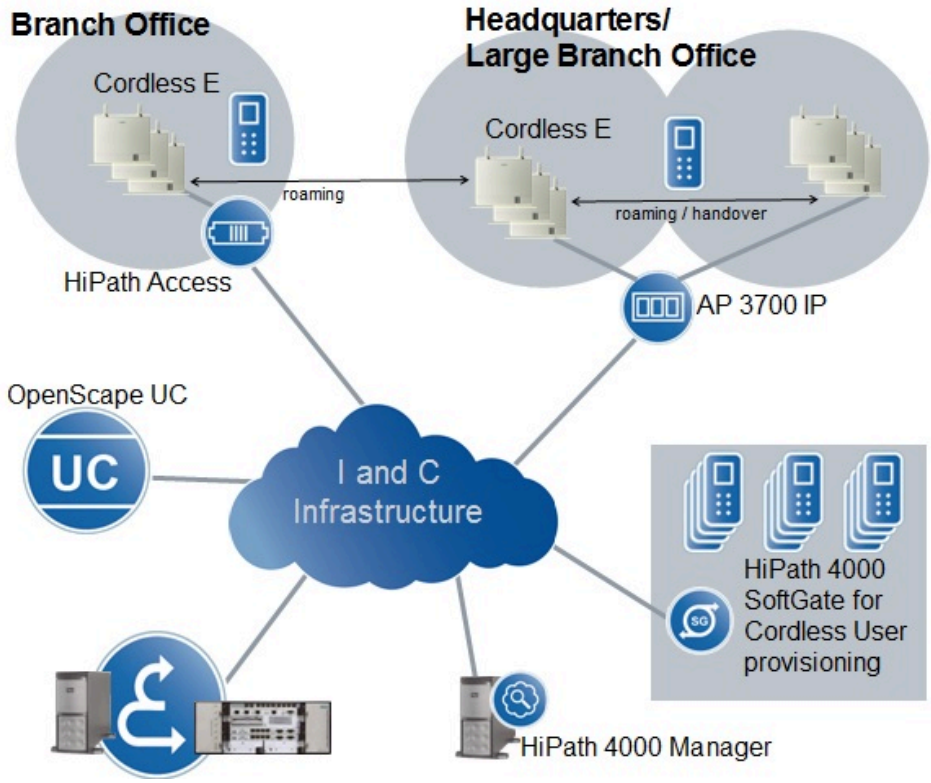


Abbildung 138: OpenScape Cordless E-Integration

Wenn sich ein Teilnehmer nicht im Ortsbereich seiner Home-SLC befindet (gilt bei vSLC immer), ist für die Umsetzung des Mobilitätskonzepts ein Datenaustausch zwischen der Home- und der Aufenthalts-SLC erforderlich. Zu diesem Zweck wird eine Verlängerungsverbindung aufgebaut.

Registrierung von CMI-Teilnehmern

Im aktuellen OpenScape 4000-Cordless-System ist die Registrierung eines Teilnehmers nur im Ortsbereich seines Home-CMI-Knotens möglich. Mit dem Leistungsmerkmal „Relocation“ können CMI-Teilnehmer nach der Registrierung auf eine andere SLC innerhalb des CMI-Netzes umgezogen werden.

Solange keine Basisstation mit IP-Schnittstelle verfügbar ist, muss die Registrierung von CMI-Teilnehmern in einem anderen CMI-Knoten mit realer Basisstation für die vSLC durchgeführt werden. Nach der Registrierung muss der Teilnehmer dann über den OpenScape 4000 Manager/Assistant auf den neuen virtuellen CMI-Knoten umgezogen werden.

Besonderheiten in Verbindung mit OpenScape Access

Wird ein OpenScape Access SLC-Modul an ein OpenScape 4000 SoftGate mit vSLC angeschlossen, soll das Access SLC-Modul nur mit Visit-Funktionalität betrieben werden.

Wenn OpenScape Access SLC-Module an ein OpenScape 4000 SoftGate mit vSLC angeschlossen werden, arbeiten die SLC-Module nur mit Visit-Funktionalität. Die Verwaltung aller registrierten CMI-Teilnehmer erfolgt durch die vSLC im OpenScape 4000 SoftGate.

Dadurch ergeben sich folgende Vorteile:

- Weniger IP-basierte Verlängerungsverbindungen

- Weniger B-Kanäle werden benötigt
- Geringere Umsetzungsverzögerung zwischen OpenScape 4000 SoftGate und dem SLC-Modul

Besonderheiten in Verbindung mit OpenScape 4000 SoftGate und VMware

Wenn ein OpenScape 4000 SoftGate in einer VMware Umgebung betrieben wird, bietet sich dem Kunden die Möglichkeit seine gesamte Cordless E V7 redundant zu betreiben.

Hierzu sind alle Cordless Teilnehmer auf virtuellen SLCen im OpenScape 4000 SoftGate einzurichten. Weiterhin wird an jedem Standort einer Basisstation in ca. 1 - 2m Entfernung eine weitere Basisstation montiert. Diese wird auf einer anderen SLC angeschlossen, die wiederum in einem anderen Shelf (oder auch OpenScape 4000 System) stecken muss. Die zweite Basisstation wird zur Vermeidung zu häufiger BS Wechsel mit reduzierter Sendeleistung betrieben.

Wichtig: Für das beschriebene Redundanzszenario ist zwingend eine projektspezifische Freigabe erforderlich.

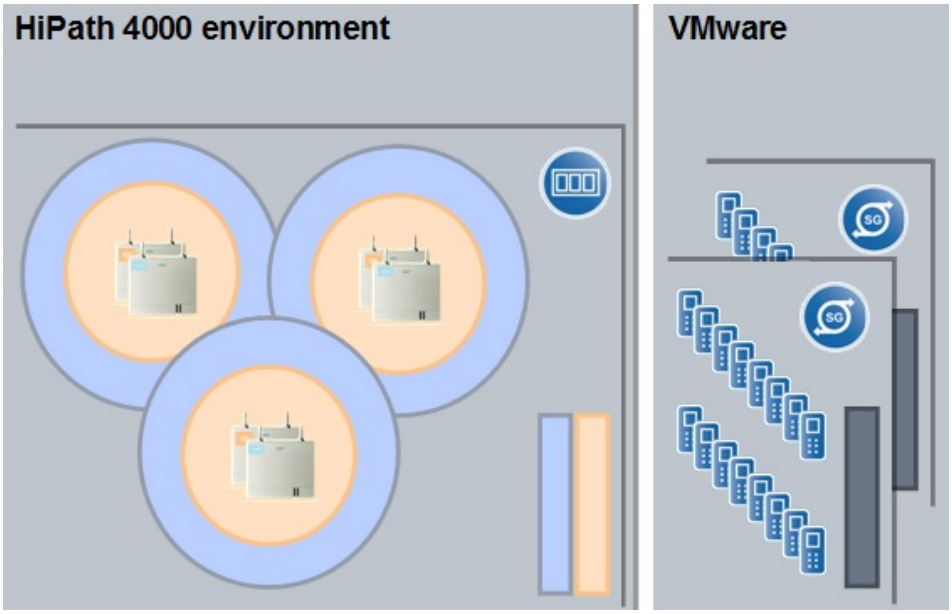


Abbildung 139: Redundanzszenario Cordless E

Dadurch ergeben sich folgende Vorteile:

- SLC / Shelf Ausfall bedeutet keinen Teilnehmerausfall
- OpenScape 4000 SoftGate Redundanz über VMware
- Handsets haben auch im Störfall die gleiche Rufnummer und Leistungsmerkmale.

3.13.2 Serviceinformationen

- Die vSLC-Applikation wird in einer reinen Software-Umgebung ausgeführt und unterstützt daher nur IP-basierte Netzwerkkonnektivität. Eine direkte Steuerung der derzeit verwendeten DECT-Basisstationen mit Up0-Schnittstelle ist nicht möglich.

- Solange keine „IP-Basisstation“ für das CMI-Leistungsmerkmal verfügbar ist bzw. unterstützt wird, müssen die Mobilitätsfunktionen in eine virtuelle Home-Funktionalität (vSLC-Applikation im OpenScape 4000 SoftGate) und eine reale Visit-Funktionalität (SLC24- und SLMC-Leitungskarten mit Up0-Schnittstelle und realen Basisstationen) aufgeteilt werden. Die einzelnen vSLC-Teilnehmer erreichen die DECT-Basisstationen über Verlängerungsverbindungen mit realen Visit-SLC-Karten. Dies bedeutet, dass für den Aufbau von Telefonverbindungen mindestens eine SLC24-Leitungskarte mit angeschlossener Basisstation benötigt wird.
- Alle DECT-Teilnehmer können an einem OpenScape 4000 SoftGate an vSLCen (Heimatknoten) konfiguriert werden.
- OpenScape 4000 SoftGate bietet keine Unterstützung für QDCL. Es wird in der Version V8 R2 unterstützt.
- Weitere Informationen zu OpenScape Cordless E finden Sie
  - auf der TI-Online-Homepage

    https://ti-online.global-intra.net/index.html
  - in der Servicedokumentation in E-Doku oder Partner Portal.

3.13.3 Generierung (Beispiel)

Die Einrichtung der vSLC erfolgt mit dem CATool V7 über den Reiter „Baugruppen und Basistationen“.

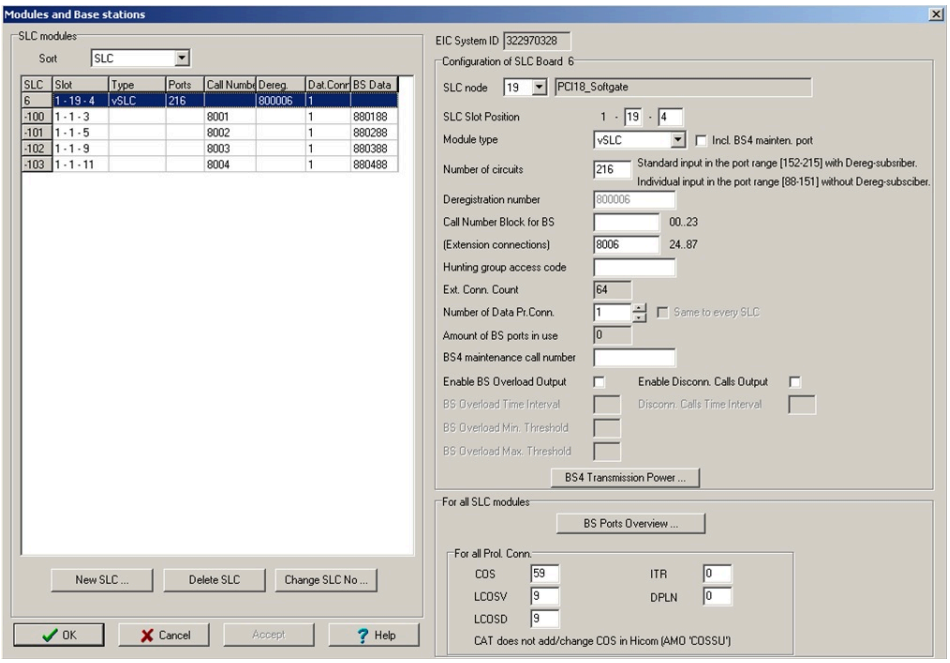


Abbildung 140: vSLC mit CATool einrichten

Hinweis:

Eine Registrierung von CMI-Teilnehmern kann nur auf einer realen SLC24 und SLMC erfolgen.

Anschließend müssen die Teilnehmer über das Leistungsmerkmal „Relocation“ des OpenScape 4000 Manager/Assistant auf die vSLC umgezogen werden.

3.14 WBMs der Baugruppen

Sie finden eine Oberflächenbeschreibung der WBMs zu vHG 3500 HFA, vHG 3500 SIP und vHG 3575 unter den folhenden Links.

vHG 3500 HFA:

http://apps.g-dms.com:8081/techdoc/de/P31003H310M1030100A9/index.htm

vHG 3500 SIP:

http://apps.g-dms.com:8081/techdoc/de/P31003H310M1010100A9/index.htm

vHG 3575:

http://apps.g-dms.com:8081/techdoc/de/P31003H310M1020100A9/index.htm

---

Wichtig: Sie können diese Dokumentation auch als Online-Hilfe im WBM aufrufen.

3.15 Zentralisierte IP für HFA

Ab V11R0 ist es möglich, eine zentrale IP-Adresse für alle HFA-Platinen auf einem SoftGate zu definieren und die Anzahl der erforderlichen IP-Adressen zu reduzieren.

Die zentrale IP-Adresse kann über den Befehl AMO STMIB unter Verwendung des LIDHFA (LAN INTERFACE DATA)-Datentyps konfiguriert werden.

Dieser TYP erfordert die folgenden Parameter:

- **LIPADR** - Für die HFA-Funktion verwendete IP-Adresse.
- **LUDPPRTL** - untere Grenze der Nutzlast-UDP-Port-Nummer.
- **LUDPPRTH** - oberre Grenze der Nutzlast-UDP-Port-Nummer
- **LTCPP** - TCP-Port Server-Port HFA
- **LTLSP** - TLS-Port Server-Port HFA

Beispiel:

```
CHANGE-
STMIB:MTYPE=NCUI2,LTU=36,TYPE=LIDHFA,LIPADR=10.100.111.233,
    LUDPPRTL=29100,LUDPPRTH=30099,LTCPP=4060,LTLSP=4061;

DISP-STMIB:NCUI2,36,,;
H500:  AMO STMIB STARTED
+------------------------------------------------------------
+
  NCUI2 BOARD DATA             SOCO1000
+------------------------------------------------------------
+
  LTU = 36   SOURCE GROUP INDEX = 6

+------------------------------------------------------------
+

=======================OUTPUT
 REMOVED=======================
```

```
  LAN INTERFACE DATA - CONFIGURABLE VALUES:


 ------------------------------------------------------------

  LIPADR    =  10 .100.111.233

  LUDPPRTL  =  29100 (29100)          LUDPPRTH   = 30099
(30099)
  LTCPP     =  4060   (4060)          LTLSP      = 4061
(4061)

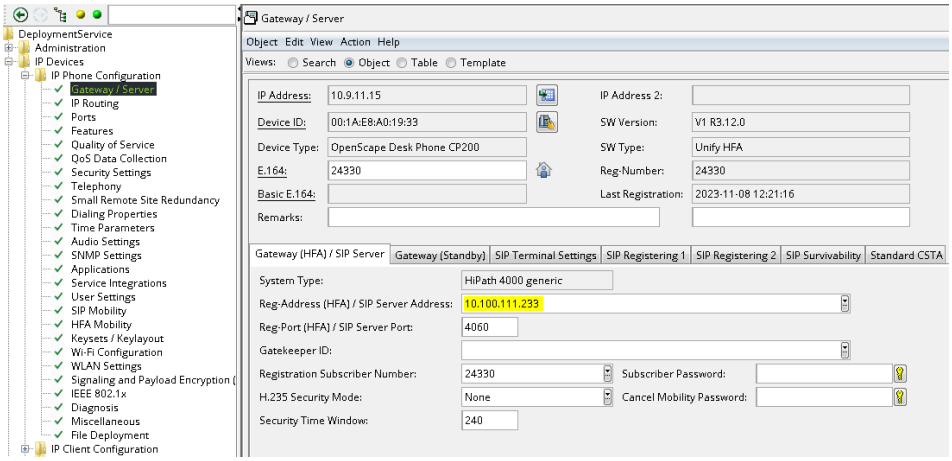
AMO-STMIB-111       CONFIGURATION OF HG3575-2 BOARDS

DISPLAY COMPLETED;
```

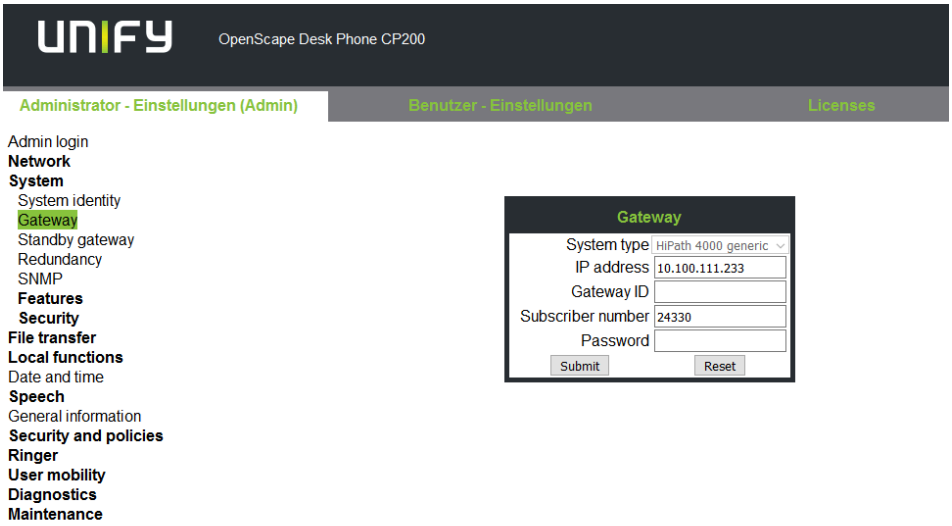
Wenn der LIPADR-Parameter konfiguriert ist und die IP-Adresse der entsprechenden, über CGWB konfigurierten HFA-Platine auf 0.0.0.0 gesetzt ist, wird LIPADR für HFA verwendet.

Es ist möglich, eine Kombination aus dedizierten und zentralisierten IP-Adressen zu verwenden.

Sie können auch die zentrale IP-Adresse konfigurieren, unter der das Telefon über DLS registriert ist, wie in der folgenden Abbildung dargestellt:



Über die WBM-Seite des Telefons können Sie überprüfen, ob sich das Telefon korrekt bei der IP-Adresse der HFA-Platine registriert.



3.15.1 WBM-GUI-Verbesserungen

Konfiguration > SPE

Die WBM-GUI wurde mit neuen Optionen für die Konfiguration von SPE-Zertifikaten verbessert.

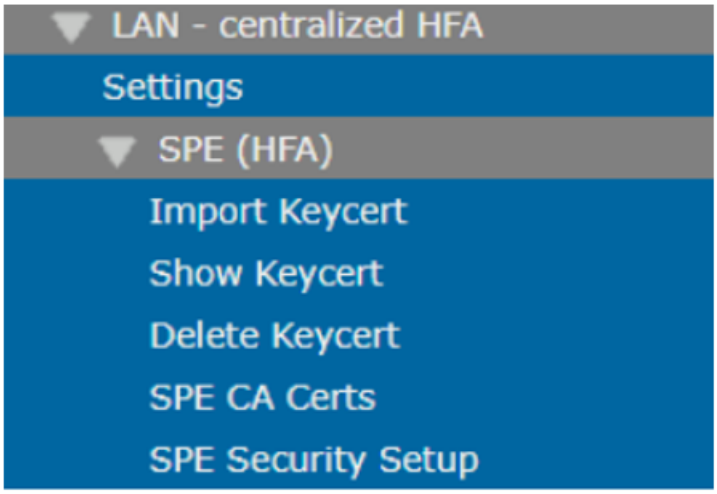


Abbildung 141: SPE-Zertifikate-Konfiguration

Die folgende Tabelle enthält eine Liste der neuen Menüpunkte und ihrer Verwendbarkeit:

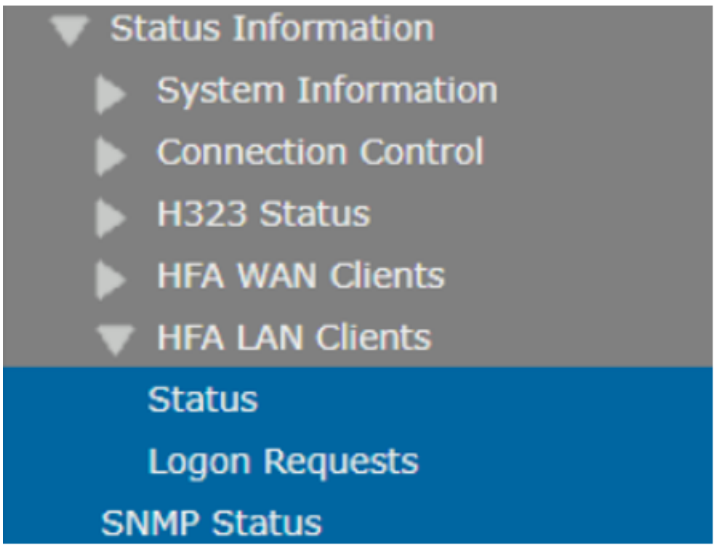
Menüpunkte	Benutzerfreundlichkeit
Einstellungen	Zeigen Sie die für HFA verwendete zentralisierte IP-Adresse an.
Keycert importieren	Importiert das SPE-Zertifikat.
Keycert anzeigen	Druckt das aktuelle SPE-Zertifikat (falls vorhanden)
Keycert löschen	Löscht das aktuelle SPE-Zertifikat (falls vorhanden) **Anmerkung:** Wenn SPE aktiv ist, kann das Zertifikat nicht gelöscht werden.
SPE – CA-Zertifikate	Behandelt das SPE CA-Zertifikat (importieren, anzeigen, löschen).

Menüpunkte	Benutzerfreundlichkeit
SPE Sicherheitseinstellung	Behandelt die TLS-Protokoll-Einstellungen für die zentralisierte sichere HFA-IP-Verbindung

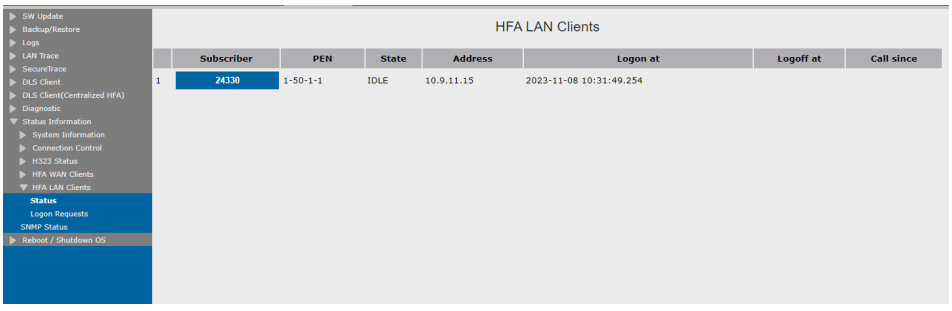
Sie können navigieren

Wartung > Status-Informationen > HFA LAN Clients

Wenn Sie zu diesem Bereich navigieren, können Sie den Status der HFA-Clients und der Anmeldeanforderungen anzeigen, wie in der folgenden Abbildung angezeigt:



Bei der Auswahl der Option **Status**, wird die folgende Ausgabe angezeigt:



4 LAN-Konnektivität (LAN-Trennung / LAN-Redundanz)

NOTICE:

Konfigurations-LAN-Schnittstellenbindung über SoftGate/ Enterprise-Gateway WBM wird ab V10R1 nicht mehr unterstützt.

Stattdessen sollte die über Plattform (firstinstall.xml) konfigurierte LAN-Redundanz verwendet werden.

Weitere Informationen finden Sie in der OpenScape 4000 Installations-, Konfigurations- und Migrationsanleitung.

IMPORTANT:

Kunden, die Mac-basierte Network Access Control (NAC) mit STMIX/STMIY und ohne LAN-Trennung (Sprache- und Management-LAN) verwenden, müssen beide Mac-Adressen des STMIX/STMIY (eth0 und eth1) zu den entsprechenden NAC-Geräten hinzufügen. Falls eine LAN-Trennung verwendet wird (ETH0 für Sprache- und ETH1 für Management-LAN), ist an jedem LAN/ETH-Port nur die entsprechende Mac-Adresse sichtbar.

4.1 Separate LAN-Konnektivität für Administration und VoIP

4.1.1 Leistungsmerkmalbeschreibung

Mit der Einführung dieses Leistungsmerkmals kann das Voice-LAN vollständig vom Management-LAN getrennt werden. Zuvor war es lediglich möglich, das IPDA-LAN vom Kunden-LAN zu trennen.

Wenn Sie das Management-LAN vom Voice-LAN trennen möchten, müssen Sie eine IP-Adresse für das Management-LAN angeben.

Wenn eine IP-Adresse für das Management-LAN angegeben ist, verwendet OpenScape 4000 Assistant diese für die Verbindung zum Gateway-WBM über die Kunden-LAN-Schnittstelle. Wenn die IP-Adresse auf den Standardwert 0.0.0.0 eingestellt ist, verwendet OpenScape 4000 Assistant die IP-Adresse des IPDA-LAN.

Die Trennung der beiden Schnittstellen kann über das Gateway konfiguriert werden.

4.1.2 Dienstinformationen

Wichtig: Wenn eine Platine eine separate Management-LAN-Schnittstelle konfiguriert hat, verwendet DLS-Bootstrapping anstelle der VOIP-IP-Adresse die MAN-IP-Adresse.

- Dieses Merkmal wird für OpenScape 4000 SoftGate, Enterprise Gateway, STMIX, STMIY, HG 3575 und HG 3500 unterstützt.
- Die Management-LAN-Schnittstellendaten werden für jedes OpenScape 4000 SoftGate, HG 3575 und HG 3500 bereitgestellt. Es besteht aus IP-Adresse, Netzmaske, Standard-Gateway, vLan-Tag und vLan-ID.
- Für SoftGate (vHG 3575 und vHG 3500) und Enterprise Gateway müssen Sie in WBM den LAN-Schnittstellennamen konfigurieren, der für Management-LAN verwendet werden soll. Für STMI, NCUI, STMIX und STMIY ist dies nicht notwendig, da LAN2 automatisch für Management-LAN verwendet wird.

4.1.3 Generierung (Beispiel)

Für die Aktivierung des Leistungsmerkmals muss im AMO STMIB/AMO CGWB eine IP-Adresse für die Management-LAN-Schnittstelle zugeordnet werden. Im Fall eines OpenScape 4000 SoftGates muss zusätzlich im WBM des entsprechenden Gateways eine Ethernet-Schnittstelle dem Management-LAN zugewiesen werden.

4.1.3.1 Konfiguration für Common Gateway (HG 3500/ HG 3575), STMIX und STMIY

Der Management-LAN-Schnittstelle muss mit Hilfe von AMO CGWB eine IP-Adresse zugewiesen werden (HG 3500, STMIX, STMIY) oder mit AMO STMIB (HG 3575) eine IP-Adresse zugewiesen werden, um das Merkmal zu aktivieren.

Verwenden Sie den Zweig **MANLANIF** in AMO STMIB und AMO CGWB mit den folgenden Parametern:

MIPADR=<Nummer>, **MNETMASK**=<Nummer>, **MVLAN**=<param>, **MVLANID**=<Nummer>, **MDEFRT**=<Nummer>

Nur für STMI-Platinen: Werden diese Parameter geändert, muss die Platine zweimal zurückgesetzt werden, um die geänderten Daten zu erhalten. Der erste Reset bietet die neuen Konfigurationsdaten an die betroffene Platine und der zweite Reset aktiviert sie.

HG 3500, HG 3575, STMIX und STMIY-Platinen bieten zwei Ethernet-Schnittstellen, LAN1 wird jetzt automatisch dem Sprach-LAN und LAN2 dem Management-LAN zugewiesen.

Anmerkung: Eine statische Route wird automatisch für die unter MGNTIP definierte und die von SIPCO:ASTIP abgeleitete IP erstellt, wenn sie sich in einem anderen Netzwerk als das Management Netzwerk befindet. Für alle anderen IPs müssen statische Routen manuell im HG erstellt werden.

Hinweis für STMI-Platinen:

Statische Routen zum Assistenten werden automatisch für die unter CGWB:MGNTDATA-MGNTIP und -BUSIP definierten IPs, wenn sie sich in einem anderen Netzwerk als dem Management Netzwerk befinden. Für alle anderen IPs müssen statische Routen manuell im HG erstellt werden.

Das Standard-Gateway ist das Gateway für Sprache-IP in LAN1, das über CGWB:GLOBIF-DEFTRT konfiguriert wird.

Assistant Gateway Manager sollte verwendet werden, um über MANLANIF von einem anderen Netzwerk auf die Karte zuzugreifen, wenn keine statische Route hinzugefügt wurde.

4.1.3.2 Konfiguration für OpenScape 4000 SoftGate oder Enterprise Gateway

Es wird empfohlen, zuerst die Änderungen im WBM und dann in AMO STMIB durchzuführen.

Wichtig: Wenn Sie diese Reihenfolge ändern, müssen Sie darauf achten, dass Sie die Platinenliste im Dashboard nicht aktualisieren (**Expertenmodus > Dashboard >** Schaltfläche **Platinenliste aktualisieren**), da die Platine (vHG 3575) weiterhin nur über die alte IP-Adresse für die Administration erreichbar ist, obwohl die neue IP-Adresse bereits dem AMO zugewiesen wurde. Dies gilt so lange, wie die Management-LAN-Schnittstelle im WBM zugewiesen ist.

Schritt 1: Zuweisen der Ethernet-Schnittstelle zum Management-LAN

Die Ethernet-Schnittstelle für das Management-LAN muss im WBM zugewiesen werden. Dazu müssen Sie das Dashboard im OpenScape 4000 Assistant starten.

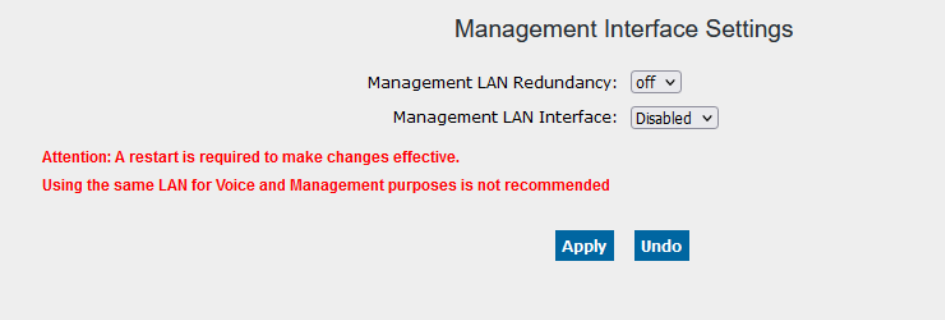
Expertenmodus > Manager



Abbildung 142: Separate LAN-Schnittstellen - Manager

Wählen Sie nun die Platine aus und starten Sie den WBM. Navigieren Sie zu **Konfiguration > LAN-Schnittstellen > Management-Schnittstelle**.

Wählen Sie in der Dropdown-Liste für die **Management-LAN-Schnittstelle** eine Ethernet-Schnittstelle aus und bestätigen Sie Ihre Eingabe mit **Anwenden**.



Management-LAN-Schnittstelle für OpenScape 4000 SoftGate (einschließlich vHG 3500) und Enterprise Gateway

Schritt 2: Zuweisen der IP-Adresse

Sie finden die Management-LAN-Daten für OpenScape 4000 SoftGate (vHG 3575) oder Enterprise Gateway in AMO STMIB und für vHG 3500 in AMO CGWB.

Verwenden Sie den Zweig **MANLANIF** mit den folgenden Parametern:

MIPADR=<Nummer>, **MNETMASK**=<Nummer>, **MVLAN**=<param>, **MVLANID**=<Nummer>, **MDEFRT**=<Nummer>

Wenn diese Parameter geändert werden, müssen die Platinen zurückgesetzt werden, um die geänderten Daten zu erhalten.

4.1.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
CGWB/ STMIB	MIPADR	d	IP Adresse der CGW Baugruppe (Source Adresse)
	MIPADR	e	Source IP address of CGW board
	MNETMASK	d	IP-Netzmaske des LAN-Segmentes Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bzgl. des Netzanteils der IP-Adresse gleich und bzgl. des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	MNETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network addresss part but different host address parts (also the Default Router must fulfill this requirement).

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
	MVLAN	d	Virtuelles LAN
	MVLAN	e	VLAN tagging on LAN-IF
	MVLANID	d	Identifikations-Nummer des virtuellen LAN Spezielle Einstellungen werden von einigen LAN-Einrichtungen (Router...) gefordert, ansonsten ist 0 der übliche Wert (Standardwert)
	MVLANID	e	Virtual LAN Identification Special settings are required by certain LAN equipment (routers...), in other cases the VLAN Id should be set to 0 (default)
	MDEFRT	d	IP-Adresse des Default Routers innerhalb des LAN-Segmentes Der Default Router übernimmt die Weiterleitung der Pakete, die eine Zieladresse außerhalb des eigenen LAN-Segmentes haben. 0.0.0.0 bedeutet, dass kein Default Router konfiguriert ist.
	MDEFRT	e	IP address of the default router within the LAN segment The default router takes care of routing forward all packets with a destination address with a network part different from the own LAN segment. 0.0.0.0 means that no default router is configured.

4.2 Separate LAN-Schnittstellen für HFA und SIP

4.2.1 Leistungsmerkmalbeschreibung

Mit der Realisierung des Leistungsmerkmales **Separate LAN-Schnittstellen für HFA und SIP** ist es möglich die HFA- und SIP-Signalisierung von der IPDA-Schnittstelle zu trennen.

Dieses Leistungsmerkmal ist ab OpenScape 4000 V7 R1 freigegeben.

4.2.2 Generierung (Beispiel)

Im OpenScape 4000 SoftGate WBM können im Menü LAN Interfaces für HFA und SIP separate LAN-Schnittstellen eingestellt werden. Als Standard wird die IPDA-LAN Schnittstelle verwendet (**HFA LAN Interface: Default IPDA** bzw. **SIP LAN Interface: Default IPDA**).

Konfiguration > LAN Interfaces > HFA Interface > Parameter **HFA LAN Interface**

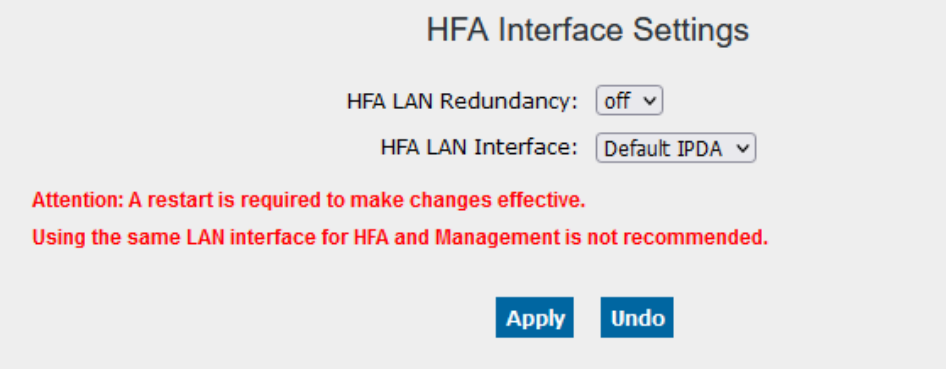


Abbildung 143: OpenScape 4000 SoftGate - HFA-Schnittstelle

Konfiguration > LAN Interfaces > SIP Interface > Parameter **SIP LAN Interface**



Abbildung 144: OpenScape 4000 SoftGate - SIP-Schnittstelle

Es ist möglich für SIP und HFA die gleiche Schnittstelle zu verwenden. Es wird allerdings nicht empfohlen SIP und HFA an der eventuell konfigurierten Management Schnittstelle zu betreiben. Für SIP-Baugruppen gilt außerdem, dass eine konfigurierte WAN-Schnittstelle bevorzugt eingerichtet wird. In diesem Fall würde eine separate SIP-Schnittstelle nicht berücksichtigt.

Für OpenScape 4000 SoftGates, die mit dem Leistungsmerkmal Zero Local Konfiguration eingerichtet wurden, gilt:

Nach einem Hardwaretausch müssen die separaten LAN Schnittstellen für SIP und HFA neu konfiguriert werden, da die Konfigurationsdaten vorerst (geplant mit OpenScape 4000 V7 R2) nqicht an den NGS-Server übermittelt werden.

Im HBR Backup sind die entsprechenden Konfigurationsdaten enthalten.

Zusätzlich können Sie ein redundantes LAN (bonding) für SIP bzw. HFA einrichten. Mehr Informationen finden Sie im Kapitel 19, „Redundante LAN-Schnittstellen (Bonding)“.

Die IP-Adressen, die per AMO CGWB für die entsprechenden Baugruppen eingerichtet wurden, werden nach einem Restart des OpenScape 4000 SoftGates an den entsprechenden LAN-Schnittstellen eingerichtet.

4.3 LAN-Redundanz

4.3.1 Leistungsmerkmalbeschreibung

Für eine erhöhte Ausfallsicherheit kann das OpenScape 4000 SoftGate über zwei LAN-Kabel an zwei verschiedene Switches/Router angeschlossen werden.

Zusätzlich müssen Sie das Leistungsmerkmal „LAN-Redundanz“ im OpenScape 4000 Plattform Administration (Portal) oder direkt in der Datei initialcfg.xml aktivieren.

Szenarien beim Starten des SoftGate-Servers

Szenario 1: Beide LAN-Kabel sind angeschlossen

LAN-Port 1 (1. Slave-Schnittstelle) ist immer aktiviert. LAN-Port 2 (2. Slave-Schnittstelle) ist auf Standby.

Szenario 2: Nur ein LAN-Kabel ist angeschlossen

Der verbundene LAN-Port (LAN1 oder LAN2) wird verwendet.

Szenario bei aktiver Baugruppe

Falls der aktive LAN-Port (bei Anschaltung beider LAN-Ports) durch einen Peer oder die Hardware getrennt/deaktiviert wird:

- Das Linux-OS aktiviert den Standby-LAN-Port.
- Der „neue“ aktive LAN-Port sendet eine GRATUITOUS ARP-Meldung mit derselben MAC- und IP-Adresse wie der „alte“ Port.
- Beim Wechseln der Ports geht die Payload für einen Zeitraum von maximal 2 Sek. verloren. Alle aktiven Verbindungen bleiben bestehen und werden **nicht** getrennt.
- Wenn der „alte“ Port wieder in Betrieb geht, erfolgt keine erneute Port-Umschaltung.

4.3.2 Redundante LAN-Schnittstellen (Bonding)

4.3.2.1 Leistungsmerkmalbeschreibung

Um eine höhere Ausfallsicherheit zu gewährleisten können redundante LAN-Schnittstellen konfiguriert werden.

4.3.2.2 Generierung (Beispiel)

Im OpenScape 4000 SoftGate WBM können in den Menüs **WAN** und **LAN Interfaces** für bessere Ausfallsicherheit redundante LAN-Schnittstellen (Bonding) eingerichtet werden.

- Redundantes LAN für WAN

  Konfiguration > WAN > WAN Einstellungen > Parameter **Redundantes WAN**

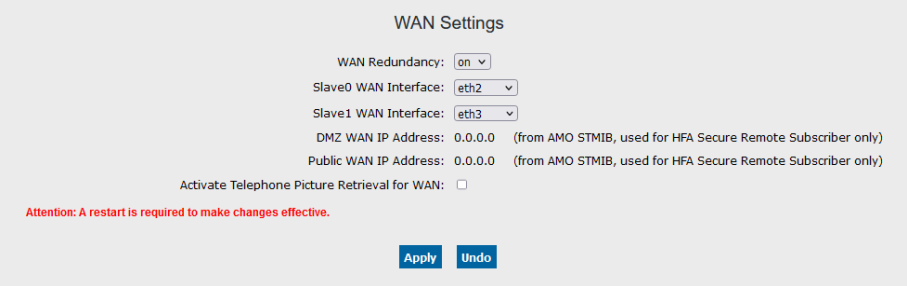


Abbildung 145: OpenScape 4000 SoftGate - Redundantes WAN

- Redundantes LAN für Management Interface

  Konfiguration > LAN Interfaces > Management Interface > Parameter **Redundantes Management LAN**

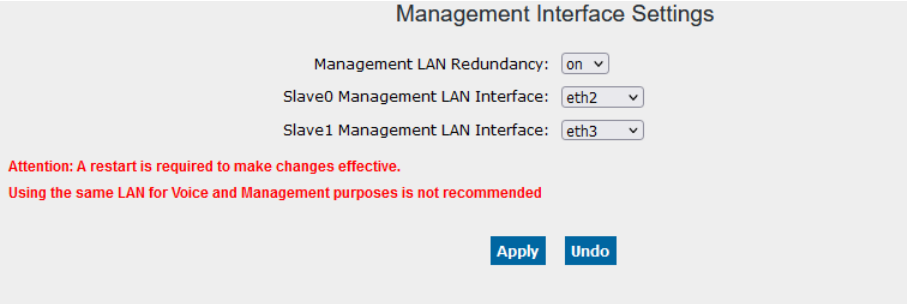


Abbildung 146: OpenScape 4000 SoftGate - Redundantes Management LAN

- Redundantes LAN für Signalling Survivability Interface

  Konfiguration > LAN Interfaces > Signalling Survivability Interface > Parameter **Redundantes LAN**

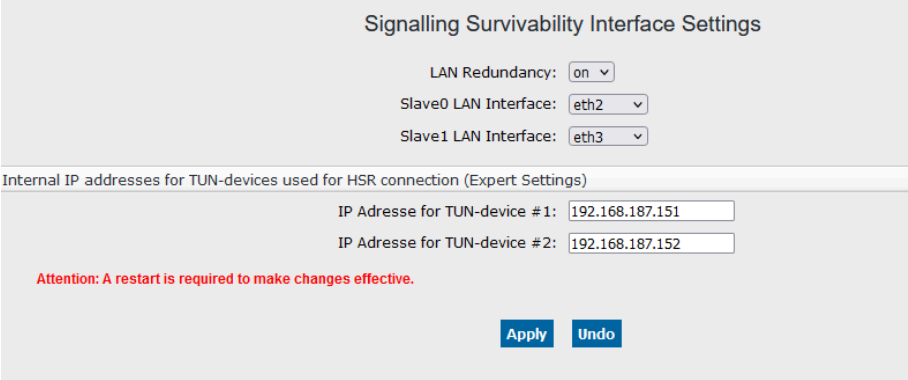


Abbildung 147: OpenScape 4000 SoftGate - Redundantes Signalling Survivability LAN

- Redundantes LAN für HFA Interface

  Konfiguration > LAN Interfaces > HFA Interface > Parameter **Redundantes HFA LAN**

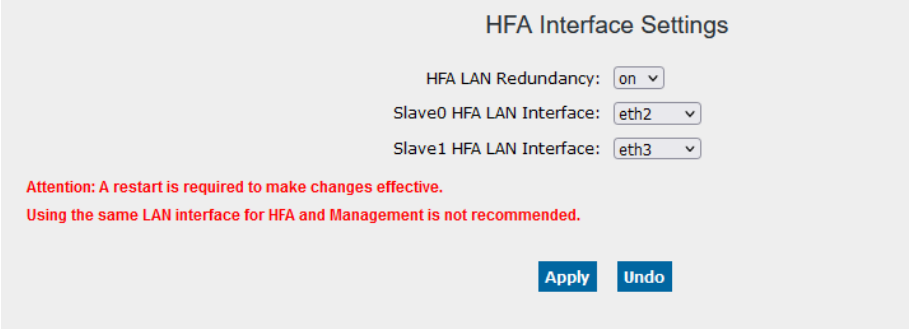


Abbildung 148: OpenScape 4000 SoftGate - Redundantes LAN an der HFA-Schnittstelle

- Redundantes LAN für SIP Interface

  Konfiguration > LAN Interfaces > SIP Interface > Parameter **Redundantes SIP LAN**

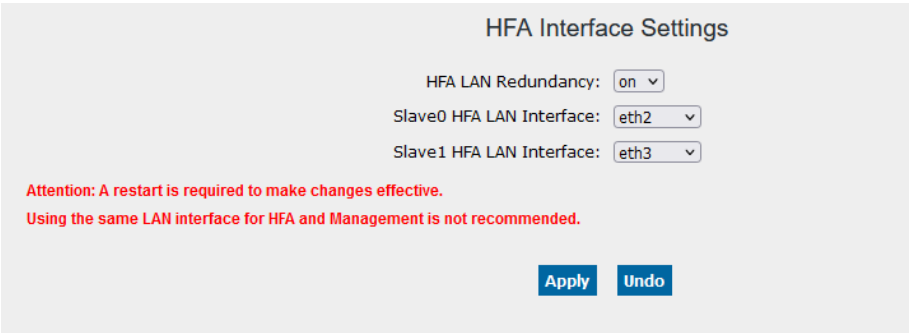


Abbildung 149: OpenScape 4000 SoftGate - Redundantes LAN an der SIP-Schnittstelle

Die IP-Adressen, die per AMO CGWB für die entsprechenden Baugruppen eingerichtet wurden, werden nach einem Restart des OpenScape 4000 SoftGates an den entsprechenden Bonding Netzwerkschnittstellen (z.B. bondhfa0) eingerichtet.

Wichtig: LAN Redundanz kann auch mit Hilfe der firstinstall.xml eingerichtet werden (siehe **OpenScape 4000 V10, Installation, Konfiguration und Migration**).

---

5 OpenScape Access und OpenScape Branch

OpenScape Access basiert auf Hardware und Software der OpenScape 4000. Es bietet eine kostengünstige Alternative für Filiallösungen mit integriertem PSTN Anschluss.

Dokumentation zu OpenScape Access finden Sie in folgendem Handbuch:

OpenScape Access, Servicedokumentation

6 OpenScape Enterprise Gateway

Dem OpenScape Enterprise Gateway liegt Hardware und Software von OpenScape 4000 zugrunde. Es handelt sich um den Nachfolger der AP 3700-9-Baugruppenrahmen mit HG3575. Der gesamte Leistungsmerkmalumfang von IP Distributed Architecture (IPDA) ist damit verfügbar.

Weitere Informationen erhalten Sie in der jeweiligen Servicedokumentation:

OpenScape 4000 V10, Enterprise Gateway, Servicedokumentation

7 Large Enterprise Gatekeeper (LEGK)

7.1 Allgemeine Informationen

7.1.1 Übersicht

Das Leistungsmerkmal ist Bestandteil der Call-Processing Software und stellt eine Gatekeeper- Funktion zur Verfügung. Daher ist der Mechanismus zur IP-Adressauflösung (Gatekeeper Funktion) für IP-Trunking in jedem Netzknoten schaltbar.

Als Hardware ist die Baugruppe STMI2/4 (HG 3500) erforderlich.

Standardmäßig wird für Trunking das SIP-Protokoll verwendet.

Beispiel: IP-Trunking in einem OpenScape 4000 Netzverbund. In jedem Knoten ist der LEGK aktiv.

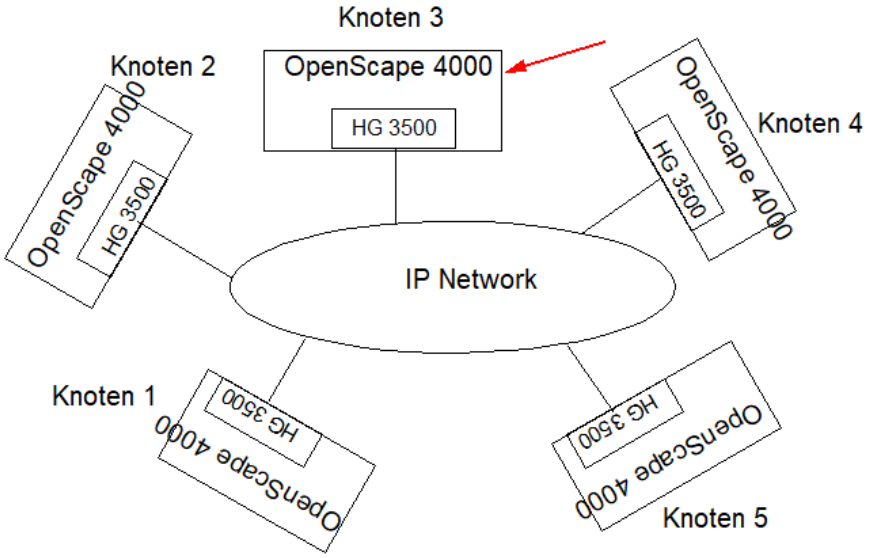


Abbildung 150: IP-Trunking in einem OpenScape 4000 Netzverbund

7.1.2 Gatekeeper Funktionalität

7.1.2.1 Allgemeines

Unter der Gatekeeper Funktionalität versteht man die Zuweisung der IP-Adresse eines Zielgateways zu einer gewählten Rufnummer (IP-Adressauflösung). Der Large Enterprise Gatekeeper (LEGK) verwendet für diese Aufgabe die HG 3500.

Die Gatekeeper-Funktionalität (LEGK) ist komplett ins LCR der OpenScape 4000 integriert. Es handelt sich also beim LEGK nicht um einen externen Server, noch ist er ein Host im IP-Netz, sondern der LEGK ist ein Prozess innerhalb des Call Processings der OpenScape 4000. Die Gatekeeper Funktionalität wird also vollständig über AMOs konfiguriert. Das Web Based Management (WBM) der HG 3500 wird nur für spezielle Einstellungen benötigt, z.B. Codec-Auswahl und QoS. Beim Common Gateway HG3500 sind auch diese Funktionen über AMO einrichtbar, das WBM wird fast nur noch für Wartungsaufgaben verwendet.

Verwendet man IP-Trunking in einem reinen OpenScape 4000 Netzverbund müssen die beteiligten HG 3500 Gateways den LEGK ihres jeweiligen Knotens benutzen. Es darf sich keine HG 3500 an einem LEGK eines anderen Knotens registrieren.

7.1.2.2 Schlüsselbegriffe

7.1.2.2.1 Local Gateway

So wird eine HG 3500 bezeichnet, die in einer OpenScape 4000 mit Gatekeeper für Trunking eingerichtet ist und diesen zur Adressauflösung verwendet.

Bezugnehmend auf das Bild 1 sind alle dort gezeigten HG 3500 Gateways local Gateways.

7.1.2.2.2 Remote Gateway

So wird eine HG 3500 bezeichnet, die in einer OpenScape 4000 für Trunking eingerichtet ist und sich zur Adressauflösung bei einem anderen, externen Gatekeeper oder Registrar registriert.

HG 3500 Gateways düren sich als Remote Gateways nur noch bei Systemen registrieren, die keine OpenScape 4000 sind, wie z.B. OpenScape Voice oder einem Internet Service Provider.

7.1.2.2.3 IP-Adressauflösung

Eine called party number wird mittels LCR in eine IP-Adresse des Zielgateways umgewertet. Die IP-Adressauflösung kann in einer OpenScape 4000 mit LCR eingerichtet werden. Dieser Service steht nur für local Gateways zur Verfügung.

7.1.3 Gatekeeper Einschränkungen

Der Large Enterprise Gatekeeper kann mit der Baugruppe mit HG 3500 betrieben werden.

Höchstmengen:

Ein IP-Trunking Netz mit HG 3500 ist theoretisch limitiert auf maximal 9999 Trunking-Baugruppen (AMO DIMSU). Die genauen Höchstmengen entnehmen Sie bitte den Freigabemitteilungen und/oder Technische Informationen.

7.2 Leitfaden für eine Installation eines IP-Features

- Abbildung des Kunden- IP-Netzes

- Erstellen eines OpenScape 4000 Netzplanes mit allen Gateways, AccessPoints, HFA-Endgeräten
- Festlegen der benötigten Anzahl von LEGKs und HG 3500 Gateways
- Abbilden des OpenScape 4000 Netzplans in das Kunden IP-Netz
- Netzanalyse mit Hilfe des IP-Servicetools zur Ermittelung der VoIP-Fähigkeit des Netzes.
- Bestätigung der Machbarkeit der projektierten IP-Komponenten

7.3 Einrichtung des Leistungsmerkmals

Der Large Enterprise Gatekeeper (LEGK) stellt eine IP-Trunking-Adressauflösung im Rahmen der Datenübertragung in IP-Netzen dar. Die Einrichtung des Leistungsmerkmals wird in folgende Schritte gegliedert, die nacheinander ausgeführt werden sollen:

- Einrichten: Datenbasis flexama Speicher - Abschnitt 3.4, „Einrichten der Flexama Speicher in der Datenbasis“, auf Seite 565
- Einrichten: HG 3500 - Abschnitt 3.5, „Einrichten einer HG 3500 am LAN Segment“, auf Seite 569
- Einrichten: HG 3500 Rufnummern - Abschnitt 3.6, „Einrichten der HG 3500 Rufnummer“, auf Seite 587
- Einrichten: LCR Wahlbewertung - Abschnitt 3.7, „Einrichten des IP-Trunking im LCR“, auf Seite 589
- Einrichten: Teilnehmer-, Amts- und Querverbindungen im lokalen Switch - Abschnitt 3.8, „Einrichten von Sätzen und Endgeräten“, auf Seite 595

Das Leistungsmerkmal LEGK muss bereits im Rahmen der Konfiguration des IP-Trunking berücksichtigt werden. Ist ein IP-Trunking bereits vorhanden, muss dieses neu generiert werden.

In den nachfolgend beschriebenen Kapiteln finden sich AMO-Einrichtebeispiele sowie die ausführliche Erklärung aller erforderlichen AMOs und AMO-Parameter. Dabei wird unterschieden, ob die Einrichtung

	mit dem OpenScape 4000 Manager / Assistant (Configuration Management) oder
	mittels AMO durchgeführt wird.

Der Large Enterprise Gatekeeper kann in allen Ausbaustufen sowie Konfigurationsarten des OpenScape 4000 Systems betrieben werden. Grundsätzlich kann ein LEGK in allen Knoten oder auch nur in einem Knoten eines OpenScape 4000 Netzes betrieben werden.

7.3.1 Wichtige Hinweise

Wichtig: Die Registrierung eines remote HG 3500 Gateways an einem OpenScape 4000 Large Enterprise Gatekeeper wird nicht unterstützt. Verbleibende Lösungen sind die lokale

Registrierung an einem Large Enterprise Gatekeeper und HiPath OpenExchange Lösungen.

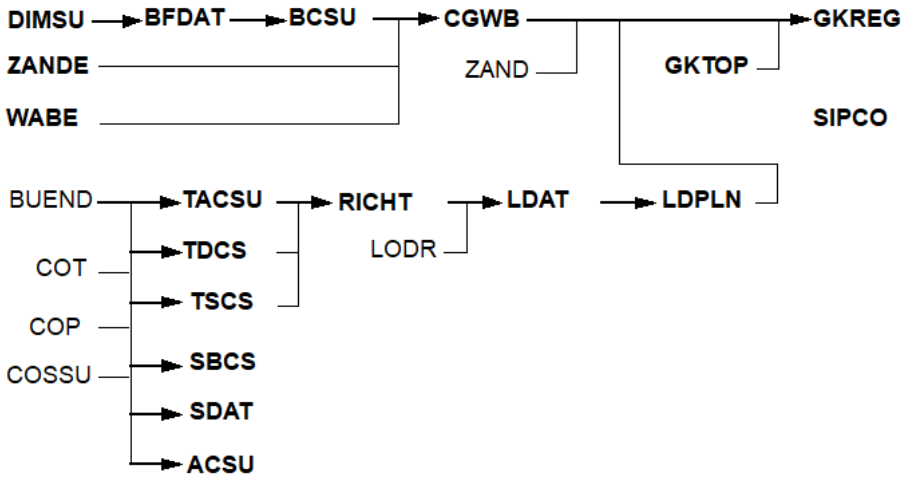
7.3.2 Betriebstechnische Generierungsreihenfolge

Dieser Abschnitt beschreibt den grundsätzlichen Ablauf der bei der Generierung des Leistungsmerkmales „Large Enterprise Gatekeeper“ einzuhalten ist. Dabei werden primär jene AMOs betrachtet, die zur Administration des Leistungsmerkmales erweitert wurden. Diese AMOs sind in Fett-Schrift dargestellt.

Zu den zusätzlich dargestellten AMOs besteht eine Generierungsabhängigkeit, jedoch erhielten sie keine leistungsmerkmalspezifische Erweiterung. Hier gilt die bisher eingeführte Generierreihenfolge.

Beim Einrichten überprüfen die AMOs GKREG und GKTOP nicht, ob verwendete Ressourcen wie z.B. Sektoren, Sektor-Pfade, Cluster, LCR Wählplan Nummern, Knotennummern, externe Gateways, u.s.w. bereits konfiguriert sind.

Für die Konsistenz der adminstrierten Topologieressourcen des IP-Netzes (z.B. Bandbreite, b-Kanäle, etc.) ist der Anwender verantwortlich. Der AMO GKTOP unterstützt dies nicht durch Plausibilitätsprüfen!



Wichtig: Die AMOs prüfen die eingegebenen Gatekeeper Konfigurationsdaten nicht auf Plausibilität und netzweite Konsistenz. Das sicherzustellen obliegt im Rahmen der Netzplanung der Verantwortung des Technikers.

7.3.3 Aktivieren des Large Enterprise Gatekeeper

Dieser Schritt ist nur erforderlich, wenn am lokalen OpenScape 4000 System kein Large Enterprise Gatekeeper zur Wegesuche betrieben werden soll. Standardmäßig ist das Leistungsmerkmal bereits aktiviert.

Ist am lokalen OpenScape 4000 System kein Gatekeeper gewünscht, so muss das Leistungsmerkmal bereits vor dem Einrichten der HG 3500 im System deaktiviert werden. Dazu wird der Schalter **GATEKPR** im AMO ZANDE verwendet.

Wichtig: Es ist nicht möglich auf einem OpenScape 4000 System dessen HG 3500 Generierung bereits abgeschlossen ist nur durch aktivieren/deaktivieren mittels AMO ZANDE nachträglich die Gatekeeper Funktion in oder außer Betrieb zu nehmen. Dazu müssen zuerst alle STMI2/4 HG 3500 Baugruppen gelöscht und nach aktivieren/deaktiveiren des ZANDE Schalters wieder neu eingerichtet werden. Ursache ist die unterschiedliche Konfiguration leistungmerkmalspezifischer Daten.

Generierung

AMO ZANDE

Mit dem AMO ZANDE wird auf jedem OpenScape 4000 System festgelegt, ob das Leistungsmerkmal betrieben wird.

	Das Einrichten mit dem AMO ZANDE kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Open ...<IP> mittels AMO** (siehe AMO Kommando)
	`EINRICHTEN-ZANDE:TYP=DATENALL,GATEKPR=JA;`

Mit diesem Kommando wird festgelegt, das die Funktion LEGK-Adressauflösung (AMO GKREG) am lokalen OpenScape 4000 System betrieben und administriert werden soll.

Tabelle 18: Parameter des AMO ZANDE im ÄNDERN-Zweig unter TYP=DATENALL

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ZANDE	GATEKPR	d	Gatekeeper Konfigurierung Diese Parameter muss auf NEIN gesetzt werden wenn eine PBX ohne Gatekeeper betrieben werden soll. Standardmäßig wird JA, d.h. also ein Gatekeeper wird an der lokalen PBX betrieben, eingerichtet.
	GATEKPT	e	Gatekeeper configuration This Parameter must be set to NO when a PBX has to operate with-out a gatekeeper. Default value is YES, that means a gatekeeper will be configured on the local PBX.

Abfragen

	Das Abfragen mit dem AMO ZANDE kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Open ...<IP> mittels AMO** (siehe AMO Kommando)
	`ABFRAGEN-ZANDE:TYP=DATENALL;`

Mit diesem Kommando werden alle zentralen Schalten im Zweig DATENALL, darunter der Schalter für den Gatekeeper, ausgegeben.

7.3.4 Einrichten der Flexama Speicher in der Datenbasis

Als erster Schritt ist die Bereitstellung einiger leistungsmerkmalspezifischer Speicher erforderlich. Erst wenn diese Speicher mit dem AMO DIMSU angelegt worden sind, kann mit der Konfiguration der Gatekeeper-Daten begonnen werden.

Die mit EINRICHTEN-DIMSU übergebenen Werte werden sofort gültig.

7.3.4.1 Anzahl der internen und externen Gateways

Dieser Schritt dient zum Einrichten einer Tabelle, in der allgemeine Verwaltungsdaten für alle internen und externen Gateways im Netz abgelegt werden. Jedes Gateway benötigt einen Eintrag.

Wichtig: Dieser Abschnitt kann übersprungen werden, wenn am lokalen OpenScape 4000 System kein Gatekeeper konfiguriert wird (AMO ZANDE: **GATEKPR=NEIN**).

Einrichten:

	`EINRICHTEN-DIMSU:TYP=SYSTEM,GWREG=25;`

Mit diesem Kommando wird die Anzahl der Gateways im Netz (im unserem Fall 25) eingerichtet, die der Large Enterprise Gatekeeper adressieren kann.

Abfragen:

	`ABFRAGEN-DIMSU:TYP=SYSTEM;`

Mit diesem Kommando werden alle Systemparameter, darin enthalten auch die Anzahl der zulässigen Gateways, ausgegeben.



```
ABFRAGEN-DIMSU:TYP=ALL,PARAM=GWREG;
```

Mit diesem Kommando wird nur die Anzahl der zulässigen Gateways ausgegeben.

7.3.4.2 Anzahl der internen HG 3500 Gateways eines Systems

Dieser Schritt dient zum Einrichten einer Tabelle, in der Daten für die internen Gateways jedes OpenScape 4000 Systems abgelegt werden. Jedes Gateway benötigt einen Eintrag.

Einrichten:



```
EINRICHTEN-DIMSU:TYP=SYSTEM,CGW=6;
```

Mit diesem Kommando wird die maximale Anzahl der HG 3500 (im unserem Fall 6) festgelegt.

Abfragen:



```
ABFRAGEN-DIMSU:TYP=SYSTEM;
```

Mit diesem Kommando werden alle Systemparameter, darunter die Anzahl der zulässigen internen Gateways, ausgegeben.



```
ABFRAGEN-DIMSU:TYP=ALL,PARAM=CGW;
```

Mit diesem Kommando wird nur die Anzahl der zulässigen internen Gateways ausgegeben.

7.3.4.3 Anzahl der LCR-Waehlmuster für Wählmuster-Pool 1 bis 8

Dieser Schritt dient zum Einrichten der Anzahl zulässiger LCR-Wählmuster in jedem der acht vorhandenen Wählmuster-Pools. Maximal sind 64000 Wählmuster je Pool möglich. Die konfigurierten Wählmuster werden beim IP-Trunking im Rahmen der Wegesuche bewertet.

Wichtig: Dieser Abschnitt kann übersprungen werden, wenn am lokalen OpenScape 4000 System kein Gatekeeper konfiguriert wird (AMO ZANDE: **GATEKPR=NEIN**). In diesem

Fall ist die Standardkonfiguration mit LCR Pool 1 und Wählplan 0 ausreichend.

Einrichten:



```
EINRICHTEN-
DIMSU:TYP=NETZ,LWM1=50000,LWM2=12000,LWM4=5600;
```

Mit diesem Kommando werden die maximale Anzahl der LCR-Wählmuster je Wählmuster-Pool festgelegt, in unserem Fall:

- 50.000 Wählmuster im Wählmuster-Pool 1
- 12.000 Wählmuster im Wählmuster-Pool 2
- 5.600 Wählmuster im Wählmuster-Pool 4

Abfragen:



```
ABFRAGEN-DIMSU:TYP=NETZ;
```

Mit diesem Kommando werden alle Parameter von netzweiten Leistungsmerkmalen, darunter die Anzahl der Wählmusterpläne in den Wählmuster-Pools 1 bis 8, ausgegeben.



```
ABFRAGEN-DIMSU:TYP=ALL,PARAM=LWM2;
```

Mit diesem Kommando wird nur die Anzahl der zulässigen LCR-Wählmusterpläne im Pool 2 ausgegeben.

7.3.4.4 Anzahl der Cache-Elemente für Cache Pool 1 bis 8

Dieser Schritt dient zum Einrichten der Anzahl zulässiger Cache-Elemente in jedem der acht vorhandenen Cache-Pools. Maximal sind 6400 Cache-Elemente je Pool möglich.

Wichtig: Dieser Abschnitt kann übersprungen werden, wenn am lokalen OpenScape 4000 System kein Gatekeeper konfiguriert wird (AMO ZANDE: **GATEKPR=NEIN**).

Einrichten:



```
EINRICHTEN-
DIMSU:TYP=NETZ,LWMC1=5000,LWMC2=120,LWMC4=100;
```

Mit diesem Kommando werden die maximale Anzahl der Cache-Elemente je Wählmuster-Pool festgelegt, in unserem Fall:

- 5.000 Wählmuster im Wählmuster-Pool 1

- 120 Wählmuster im Wählmuster-Pool 2
- 100 Wählmuster im Wählmuster-Pool 4

Abfragen:

	`ABFRAGEN-DIMSU:TYP=NETZ;`

Mit diesem Kommando werden alle Parameter von netzweiten Leistungsmerkmalen, darunter die Anzahl der Cache-Elemente in den Cache-Pools 1 bis 8, ausgegeben.

	`ABFRAGEN-DIMSU:TYP=ALL,PARAM=LWMC1;`

Mit diesem Kommando wird nur die Anzahl der Cache-Elemente im Cache-Pool 1ausgegeben.

7.3.5 Einrichten einer HG 3500 am LAN Segment

Die HG 3500 Baugruppe (STMI2/4) stellt eine Payload Verbindungen zwischen dem zentralen OpenScape 4000 System und dem OpenScape 4000 LAN Segment her.

- HG 3500 Baugruppen dürfen sowohl den Peripherie-Rahmen (LTU 1-15) des zentralen Systems wie auch in den Access Points (LTU 17-99) eingesetzt werden. Es können so viele HG 3500 Gateways eingesetzt werden, wie mit dem AMO DIMSU (siehe Abschnitt 3.4.2, „Anzahl der internen HG 3500 Gateways eines Systems“, auf Seite 566) eingerichtet wurden.
- Es können mehrere HG 3500 Baugruppen in einem OpenScape 4000 System eingesetzt werden.
- Alle HG 3500 Baugruppen müssen am OpenScape 4000 LAN Segment angeschlossen sein.
- Die Hardware der HG 3500 ist die STMI2-/4-Baugruppe. Es handelt sich dabei um eine Baugruppe, die gleichzeitig über IP-Trunking, einen WAML-Satz, IPDA-Funktion, HFA-Funktion und SIP Subscriber Funktion verfügen kann. Die Art sowie Anzahl der jeweils zur Verfügung stehenden Sätze bzw. B-Kanäle wird mit dem AMO BFDAT festgelegt.

Anmerkung: Es ist nicht möglich, WAML auf STMIX zu konfigurieren.

Ein OpenScape 4000 LAN-Segment ist der Teil des Kundennetzwerks, in dem die IP-Komponenten des Zentralsystems und direkt (d. h. nicht über einen Router) verbundene Access Points installiert sind.

7.3.5.1 Einrichten des HG 3500 Gateways

Voraussetzung ist, dass das lokale LAN Segment erfolgreich eingerichtet worden ist. Als nächsten Schritt muss jedes HG 3500 Gateway installiert werden.

7.3.5.1.1 Einrichten der HG 3500 Baugruppe

Das Einrichtebeispiel ist für das linke OpenScape 4000 System „N 1“ mit Gatekeeper gültig. Die zu administrierende HG 3500 mit den entsprechenden Konfigurationsdaten ist gelb hinterlegt. Der Gatekeeper (IPADR=192.168.2.11) im Partnersystem „N 2“ ist farblich heller dargestellt und wird nur später bei den AMOs GKREG und GKTOP näher betrachtet.

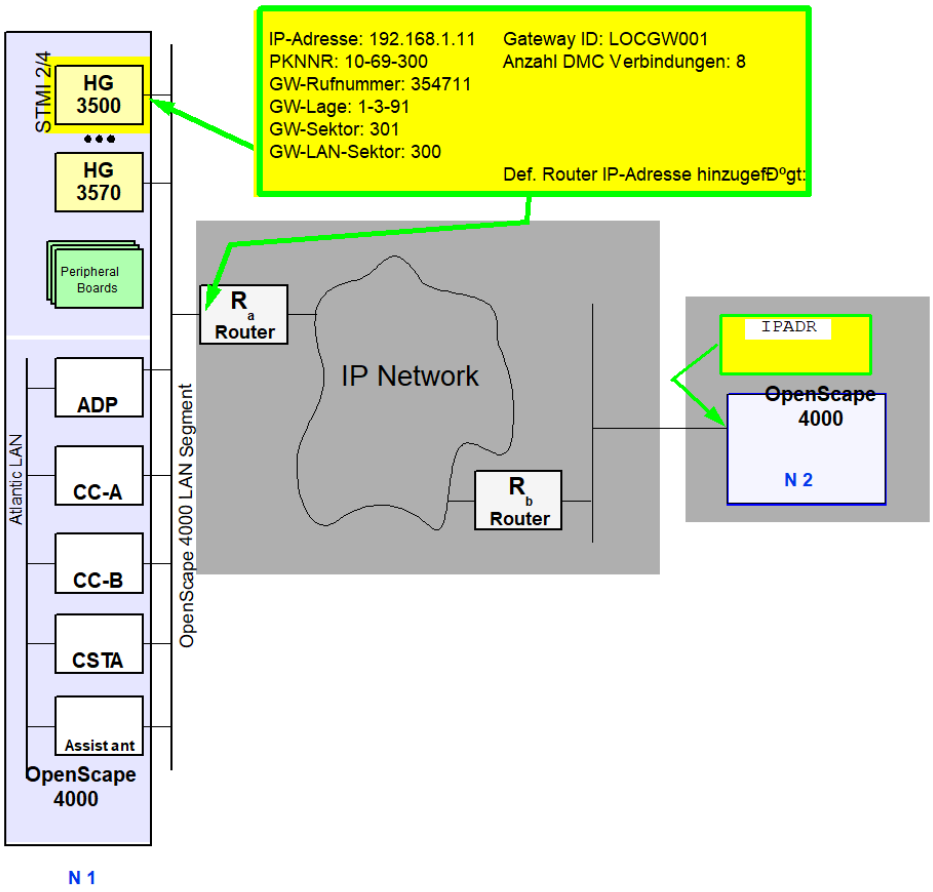


Abbildung 151: Einrichten eines HG 3500 Gateway

EINRICHTEN-BFDAT:	FCTBLK=1,	FUNCTION=HG3550,
	BGBKAN=BKAN60&BKAN120;	
AENDERN-BFDAT:	CONFIG=WEITER,	FCTBLK=1,
	FUNCTION=HG3550,	ANZSATZ=1,
	ANZEINH=3;	
AENDERN-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANTW=JA;	
EINRICHTEN-BCSU:	TYP=IPGW,	LTG=1,
	LTU=3,	EBT=91,
	SACHNR=Q2316-X10,	FCTID=1,
	FCTBLK=1,	BKAN3550=30;
EINRICHTEN-CGWB:	MTYP=CGWB,	LTU=3,
	EBT=91,	IPADR=192.168.1.11,
		NETMASK=255.255.255.0;
AENDERN-CGWB:	MTYP=CGWB,	LTU=3,
	EBT=91,	TYP=GWDATA,

Generierung

Eine HG 3500 Baugruppe wird durch 3 AMOs konfiguriert: BFDAT, BCSU und CGWB.

AMO BFDAT

Mit dem AMO BFDAT werden die Funktionsblöcke für die HG 3500 definiert.

	**Configuration Management > Alagendaten > Baugruppe > CGW-Funktionsblock** **NEU** klicken, Daten eingeben und **Sichern**.

	`EINRICHTEN-BFDAT:FCTBLK=1, FUNCTION=HG3550, BKANANZ=BKAN60&BKAN120;`
	`AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=1, FUNCTION=HG3550, ANZSATZ=1, ANZEINH=3;`
	`AENDERN-BFDAT=CONFIG=OK,FCTBLK=1,ANTW=JA;`

Tabelle 19: Parameter des AMO BFDAT

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BFDAT	ANTW	d	ANTW=JA Block-Konfiguration abschließen
	ANSW	e	ANSW=YES Finish block configuration
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze.
	LINECNT	e	Defines the number of lines related to the selected function.
	BKANANZ	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanälen
	BRDBCHL	e	Dedicates the block for boards with 60 and/ or 120 b-channels
	CONFIG	d	CONFIG=WEITER Weitere Block-Konfiguration möglich CONFIG=OK Block-Konfiguration abschließen

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CONFIG	e	CONFIG=CONT Continue block configuration CONFIG=OK Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des CGW fest. Dabei muss die evtl. benötigte HG3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG3530, HG3540 oder HG3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function.

AMO BCSU

Mit dem AMO BCSU wird die Baugruppe im System eingerichtet und eingeschaltet.

	**C**onfiguration Management > Anlagendaten > Baugruppe > Baugruppe **NEU** klicken, Daten eingeben und **Sichern**.
	EINRICHTEN- BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=91,SACHNR=Q2316-X10,FC- TID=1,FCTBLK=1,BKAN3550=30; AENDERN- BCSU:TYPE=HWYBDL,LTU=3,SLOT=81,PARTNO=Q2316-X10,HWYBDL=A;

Tabelle 20: Parameter des AMO BCSU

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	TYP	d	TYP=IPGW Common Gateway Baugruppe
	MTYPE	e	MTYPE=IPGW Common gateway board
	LTG	d	LTG-Nummer Parameter kann entfallen - oder muss auf 1 gesetzt werden.
	LTG	e	Line/Trunk Group Number Parameter can be omitted - or must be set to 1.
	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 eingesetzt wird. Die HG 3500 darf nur in den Rahmen des OpenScape 4000 Zentralsystems (LTU 1..15) eingesetzt werden. Der Rahmen muss mit einer LTUCX Baugruppe ausgestattet sein.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged. An HG 3500 may only be used in a shelf of the OpenScape 4000 central system (LTU 1..15). The shelf must be equipped with a LTUCX board.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	SACHNR	d	Sachnummer der HG 3500-Baugruppe

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	PARTNO	e	Part Number of the HG 3500 Board
	FCTID	d	Function ID
	FCTID	e	Function ID
	FCTBLK	d	Function Block Index
	FCTBLK	e	Function block index
	BKAN3550	d	Anzahl der B-Kanäle für die HG3550 Funktion
	BCHL3550	e	Amount of b-channels for HG3550 function
	HWYBDL	d	Highway Bündel Die HG 3500 / STMI2/4 und STMIX Baugruppe unterstützt die Wideband Technologie. Deshalb muss der Baugruppe entweder das Highway Bündel A (default) oder F zugewiesen werden.
	HWYBDL	e	Highway bundle The HG 3500 / STMI2/4 and STMIX board supports wideband technology. Thus either highway bundle A (default) or F must be assigned to this board.

AMO CGWB

Mit dem Zweig EINRICHTEN werden die für den Betrieb notwendigen individuellen Einstellungen der HG 3500 Baugruppe getätigt. Es werden globale und Ethernet spezifische Baugruppen-Daten konfiguriert. Diese werden erst beim Einschalten bzw. Aus- und wieder Einschalten der Baugruppe (RESTART-BSSU) auf die Baugruppe geladen.

Der AENDERN Zweig MTYP=CGW erlaubt die Einstellung einer Vielzahl von Parametern, die in unterschiedlichen Zweigen untergebracht sind. Zur Inbetriebnahme sind mindestens noch Daten der Zweige TYP=GWDATA, TYP=DMCDATA sowie TYP=LEGKDATA erforderlich.

Die Angabe einer GWNR ist vom eingestellten Betriebsszenario (siehe AMO ZANDE)

- PBX mit LEGK
- PBX ohne LEGK

abhängig. Ein Mischbetrieb ist nicht möglich.

Eine Gatewaynummer ist grundsätzlich erforderlich, wenn der Gatekeeper an der lokalen PBX eingerichtet und das Gateway hier registriert werden soll.

Soll sich ein Gateway am Gatekeeper einer fremden PBX registrieren, so ist keine Gateway Nummer erforderlich. Wurde die Gateway Nummer angegeben, so wird sie ignoriert.

Einrichten Ethernet spezifische Baugruppendaten

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** **Suchen** klicken und **BG-Name=STMI2** oder **BG-Name=STMI4 oder BG-Name=STMIX**auswählen. Geben Sie die Daten in der Lasche **STMI-Baugruppendaten** ein und **Sichern**. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.
	`EINRICHTEN-CGWB:LTU=3,SLOT=91,IPADDR=192.168.1.11,NET▶MASK=255.255.255.0;` Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung `RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91; neu geladen werden.`

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 21: Parameter des AMO CGWB

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	IPADR	d	IP-Adresse der HG 3500 im Kunden LAN Legt die IP-Adresse fest, über die ein HG 3500 Gateway am OpenScape 4000 LAN-Segment erreicht werden soll.
	IPADR	e	IP-Address of HG 3500 on customer LAN Assigns the address with which a HG 3500 gateway can be reached on the OpenScape 4000 LAN-segment.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	NETMASK	d	Netzmaske des LAN-Segmentes
	NETMASK	e	Netmask of LAN-segment
	MUSTER	d	Ruhebitmuster Der Default-Wert ist 213 (dezimal)
	PATTERN	e	Idle Pattern Default value is 213 (decimal)

Wichtig: Prüfen Sie vor dem `EINRICHTEN-CGWB` die Gateway IP-Adresse, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. *IPADR* darf nicht erreichbar sein - sonst wird die entsprechende Adresse bereits benutzt. *IPADR* muss für jede HG 3500 unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.

TYP=GWDATA - Ändern Gateway Identifikation

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Suchen klicken und BG-Name=STMI2 oder BG-Name=STMI4 oder BG=STMIX auswählen. Geben Sie die Daten in der Lasche **STMI2-IGW-Baugruppendaten** ein und **Sichern**. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`AENDERN-CGWB:MTYP=CGWB,TYP=GWDATA,LTU=3,EBT=91,GWID1=INTGW001;`
	Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung
	`RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91;`
	neu geladen werden.

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 22: Parameter des AMO CGWB im AENDERN-Zweig unter MTYP=CGW, TYP=GWDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	GWID1	d	Gateway Identifikation 1. Teil Die Gateway Identifikation ist der 1. Teil einer beliebigen 64 Zeichen langen Zeichenkette. Die Eingabe ist CASE-sensitiv.
	GWID1	e	Gateway Identifikation 1. part A gateway identification is the 1. part of an idividual 64 character long characterstring. The input is CASE-sensitive.
STMIB	GWID2	d	Gateway Identifikation 2. Teil Die Gateway Identifikation ist der 2. Teil einer beliebigen 64 Zeichen langen Zeichenkette. Die Eingabe ist CASE-sensitiv.
STMIB	GWID2	e	Gateway Identifikation 2. part A gateway identification is the 2. part of an idividual 64 character long characterstring. The input is CASE-sensitive.

Rücksetzen der Parameter auf Default-Werte

Das Rücksetzen auf die Grundinitialisierung ist mit dem Kommando `AENDERN-CGWB:MTYP=INITCGW,TYP=GWDATA; möglich.`

TYP LEGKDATA - Ändern der Gateway Rufnummer

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** **Suchen** klicken und **BG-Name=STMI2** oder **BG-Name=STMI4** auswählen. Geben Sie die Daten in der Lasche **STMI2-IGW-Baugruppendaten** ein und **Sichern**. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`AENDERN-CGWB:MTYP=CGW,TYP=LEGKDA▶`
	`TA,LTU=3,EBT=91,GWNR=3,GWRNR=354711;`
	Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung
	`RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91;`
	neu geladen werden.

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 23: Parameter des AMO CGWB im AENDERN-Zweig unter MTYP=CGW, TYP=LEGKDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	GWNR	d	Gateway Nummer Die Gateway Nummer dient zur Identifikaiton der HG 3500 und ist immer erforderlich, wenn ein Gatekeeper an der lokalen PBX betrieben wird. Verfügt die lokale PBX über keinen Gatekeeper so wird auch keine Gateway Nummer benötigt Der Default-Wert ist 0 (dezimal)

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	GWNO	e	Gateway number A gateway number is used to identify a HG 3500 and it necessary, when a gatekeeper is operating on the lokal PBX. Is there no gatekeeper working on the lokal PBX then no gateway number is needed Default value is 0 (decimal)
	GWRNR	d	Gateway Rufnummer Legt eine Rufnummer fest, mit der das Gateway an der lokalen PBX erreichbar ist. Die Rufnummer muß eigens mit dem AMO WABE und Kennzahlpunkt QUER eingerichtet werden.
	GWSTNO	e	Gateway station number Assigns an access code, with which a gateway can be reached on the local PBX. The access code must be specially configured with AMO WABE and DAR = QUER.
	REGEXTGK	d	Gateway Registrierung an einem remote Gatekeeper Damit wird gesteuert, ob sich ein Gateway an einem remote Gatekeeper registrieren darf.
	REGEXTGK	e	Gateway registration at remote gatekeeper Controls, if a gateway is permitted to register at a remote gatekeeper.

Rücksetzen der Parameter auf Default-Werte

Ein Rücksetzen der CGWB-Parameter für den LEGKDATA ist nicht sinnvoll bzw. vorgesehen. Eine Änderung auf andere Werte ist nur mit dem Kommando `AENDERN-CGWB: MTYP=STMI2IGW,TYP=LEGKDATA, ..... ;`

TYP DMCDATA - Ändern Anzahl der DMC Verbindungen

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und die Baugruppe auswählen. Geben Sie die Daten in der Lasche **STMI-Baugruppendaten** ein und **Sichern**. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`AENDERN-CGWB:MTYP=CGWB,TYP=DMCDATA,LTU=3,EBT=91,DMCCONN=8;`
	Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung
	`RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91;`
	neu geladen werden.

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 24: Parameter des AMO CGWB im AENDERN-Zweig unter MTYP=CGW, TYP=DMCDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	DMCCONN	d	Anzahl der möglichen DMC Verbindungen Legt den Maximalwert der möglichen DMC Verbindungen für die HG 3500 fest.
	DMCCONN	e	Number of possible DMC connections Assigns the maximum number of possible DMC connections for the HG 3500.

Rücksetzen der Parameter auf Default-Werte

Das Rücksetzen auf die Grundinitialisierung ist mit dem Kommando:
`AENDERN-CGWB:MTYP=INITCGW,TYP=DMCDATA; möglich.`

TYP GLOBIF - Ändern der Default Router IP-Adresse

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und die Baugruppe auswählen. Die Daten in der Lasche **STMI2-IGW-Baugruppendaten** eingeben und **Sichern**. **Configuration Management > Anlagendaten > Wartung > BG-Wartung** **Suchen** klicken und **STMI** auswählen. Im Pulldownmenü **Aktion Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`AENDERN-CGWB:MTYP=CGW,TYP=GLOBIF,LTU=3,EBT=91,DEFRT=192.168.1.254`
	Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung
	`RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91;`
	neu geladen werden.

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 25: Parameter des AMO CGWB im AENDERN-Zweig unter MTYP=CGW, TYP=GLOBIF

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	DEFRT	d	IP-Adresse der Default Routers Der Default-Wert ist 0.0.0.0
	DEFRT	e	Default router IP-address Default value is 0.0.0.0

Rücksetzen der Parameter auf Default-Werte

Das Rücksetzen auf die Grundinitialisierung ist mit dem Kommando:
`AENDERN-CGWB:MTYP=INITCGW,TYP=GLOBIF; möglich.`

TYP GKDATA - Ändern IP-Adressen für primäre und sekundäre Gateways

Dieser Schritt ist an nur dann notwendig, wenn am lokalen OpenScape 4000 System kein Gatekeeper konfiguriert ist und ein Gateway sich am Gatekeeper einer fremden PBX registrieren soll. Mit diesem Kommando werden die IP-Adressen der entsprechenden Gateways eingetragen.

	Configuration Management > Anlagendaten > IPDA > IPDA Access Point **Suchen** klicken und Access Point auswählen, Daten ändern und **Sichern**.
	`AENDERN-CGWB:MTYP=CGW,TYP=GKDATA,LTU=3,EBT=91,PRIGK▶IP=192.168.1.90,PRIGKPN=1719,PRIGKID1=PRIMARYRASMANAGERID;` In diesem Fall wird nur ein Primary-Gatekeeper zugewiesen. Damit diese Änderung auf der HG 3500 wirksam wird, muss diese mit Verwendung `RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=91;`

Wichtig: Bestehende **Verbindungen werden dadurch getrennt!**

Tabelle 26: Parameter des AMO CGWB im AENDERN-Zweig unter MTYP=CGW, TYP=GKDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 gesteckt ist.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	PRIGKIP	d	IP Adresse der HG 3500 des primär anzusprechenden Gatekeeper Jeder Gatekeeper wird durch eine IP-Adresse adressiert.
	PRIGKIP	e	IP address of the HG 3500 for the primary addressed gatekeeper Every gatekeeper is addressed by itâs own IP address
	PRIGKPN	d	Portnummer der HG 3500 Die Portnummer für HG 3500 ist standardmäßig 1719.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	PRIGKPN	e	Portnumber of HG 3500 The default portnumber for a HG 3500 is .1719.
	PRIGKID1	d	ID des primär anzusprechenden Gatekeeper - 1. Teil Der Default-Wert ist “PrimaryRASManagerID“. Die Eingabe ist CASE-sensitiv.
	PRIGKID1	e	ID of the primary addressed gatekeeper - 1. part Default value is “PrimaryRASManagerID“. The input is CASE-sensitive.
	PRIGKID2	d	ID des primär anzusprechenden Gatekeeper - 2. Teil Die Eingabe ist CASE-sensitiv.
	PRIGKID2	e	ID of the primary addressed gatekeeper - 2. part The input is CASE-sensitive.
	SECGKIP	d	IP Adresse der HG 3500 des sekundär anzusprechenden Gatekeeper Jeder Gatekeeper wird durch eine IP-Adresse adressiert.
	SECGKIP	e	IP address of the HG 3500 for the secondary addressed gatekeeper Every gatekeeper is addressed by itâs own IP address

Rücksetzen der Parameter auf Default-Werte

Das Rücksetzen auf die Grundinitialisierung ist mit dem Kommando:
`AENDERN-CGWB: MTYP=INITCGW,TYP=GKDATA; möglich.`

Abfragen:

AMO BCSU

Beim Einrichten einer HG 3500 wird die Verteilung sowie nutzbare Zahl der IP-Verbindungen (b-Kanäle) über die FCTID der HG 3500 im AMOs BCSU definiert.

Im Gegensatz zu NCUI4 und STMI2/4 wird für ein HG 3500 Gateway keine Zusatzinformation wie z.B. IP-Adresse, b-Kanäle, etc. ausgegeben.

	Die Abfrage kann mit dem OpenScape 4000 Assistant, Fenster Baugrupen durchgeführt werden.
	`ABFRAGEN-BCSU:TAB,1,LTU-Nummer,Einbauteilung;` Der AMO gibt die üblichen Baugruppendaten für das Common Gateway aus.

```
AB-BCSU:TAB,1,3,91;
H500:  AMO BCSU GESTARTET
 ADDRESSE :  LTG  1   LTU 3    SOURCE GROUP 1
-----+----------+--------+---+-+-+---+-+-----------
+-----------+----------|
     |           |        |   |S|H|AL-| |           |
       |           |
     | SOLL      | BG     |FCT|E|W|ARM| | IST       |
 HW-     | BG        |
 EBT | BG        | TYP    |ID |C|Y|NR | | BG        |STAND
 INFO  | ZUSTAND   |
-----+----------+--------+---+-+-+---+-+-----------
+-----------+----------|
  91 | Q2316-X10  STMI2      1   A   0|*| Q2316-X10  | -05
 -      | READY     |
     +-------------------------------+-+-----------
+-----------+----------|
     | IP ADRESSE : 192.168.  1. 11         B-KANAELE : 120
     ANZBKAN : 120 |
     | BLOCK-NR   :   1                     RERESERV. LINES
 UMGEWANDELT: NEIN |
     |  1. FUNKT  : STMI2-IPGW    1 LINES   B-KANAELE :  30
     ANZBKAN :  30 |
     +-------------------------------+-+-----------
+-----------+----------|
```

AMO CGWB

	Die Abfrage mit dem AMO CGWB kann nur über den Expertenmodus durchgeführt werden. Expertenmodus > Expertenzugang > Open ... <IP> mittels AMO (siehe AMO Kommando)
	`ABFRAGEN-STMIB:CGW,LTU-Nummer,Einbauteilung;` Der AMO gibt alle HG 3500 spezifischen Daten aus.

Für die folgenden Daten müssen Werte konfiguriert werden, um einen korrekten Betrieb zu gewährleisten:

- Ethernet-Schnittstelle
- Gateway Daten
- Gatekeeper spezifische Daten

Löschen:

AMO BCSU

	Das Löschen mit dem AMO BCSU kann nur über den Expertenmodus durchgeführt werden. Expertenmodus > Expertenzugang > Open ...<IP> mittels AMO (siehe AMO Kommando)
	`LOESCHEN-BCSU:PER,,LTU-Nummer,Einbauteilung,Sachnummer;` Der AMO löscht die angegebene Baugruppe aus dem OpenScape 4000 System.

AMO CGWB

Der AMO besitzt keinen Löschen-Zweig. Die mit AMO CGWB (TYP=LEGKDATA) geänderten Konfigurationsdaten für ein lokales Gateway werden beim Löschen vom AMO GKREG mit gelöscht.

Wiedereinrichten ist danach mit dem AMO CGWB sowie GKREG jederzeit möglich.

Rücksetzen der Parameter auf Default-Werte:

- Ein Rücksetzen der CGWB-Parameter für den LEGKDATA ist nicht sinnvoll bzw. vorgesehen.
- Das Rücksetzen einzelner Datentypen auf die Grundinitialisierung ist mit dem Kommando:
  `AENDERN-CGWB:MTYP=INITCGW,TYP= <param>; möglich.`
- Das Rücksetzen aller Datentypen auf die Grundinitialisierung ist mit dem Kommando:
  `AENDERN-CGWB:MTYP=INITCGW,TYP=ALL; möglich.`

7.3.5.1.2 Einrichten der HG 3500 Sätze

Für jede Common Gateway Baugruppe muss, basierend auf ihrer Konfiguration (siehe AMO BFDAT: Parameter FCTBLK), die entsprechende Anzahl von Sätzen eingerichtet werden. Dazu wird, wie bei allen anderen Sätzen üblich, der AMO TDCSU verwendet.

Zu beachten ist, das einige HG 3500 spezifische Parameter benötigt werden, die für alle AMO Kommandos im Zweig GER=HG3550IP zusammengefasst sind.

Mit dem Parameter **DMCERL** wird festgelegt, ob dieser Satz in einer Direct Media Connection verwendet werden kann.

Es ist zu beachten, das gegebenenfalls benötigte Satzdaten wie z.B. besondere Satz- und Leitungsparameter, Bündel, u.s.w. zuvor mit den entsprechenden AMOs konfiguriert werden müssen.

Jeder Satz einer HG 3500 muss ein eigenes Bündel haben.

7.3.5.1.3 Ändern der HG 3500 Gateway Registrierung

Das OpenScape 4000 System unterstützt die direkte Änderung der Art der Gateway-Registrierung - von remote auf internen Gatekeeper und umgekehrt - nicht. Ebenso ist es nicht erlaubt im AMO ZANDE den Schalter **GATEKPR** zu ändern, solange noch ein Gateway konfiguriert ist. Dies kann zu schwerwiegenden Betriebsstörungen führen!

Da der AMO CGWB keinen Löschen-Zweig hat ist es Aufgabe des AMO BCSU interne HG 3500 Konfigurationsdaten sowie die erweiterten Baugruppendaten zu löschen.

- In einer PBX **mit/ohne** Gatekeeper müssen die HG 3500 Gateways zuerst in jedem Fall gelöscht und anschließend neu konfiguriert werden. Beachten Sie, in diesem Fall sind alle Gateways entweder intern (PBX mit Gatekeeper) oder remote (PBX ohne Gatekeeper) registriert.

  – Ändern der Gateway-Registrierung von intern auf remote:

  Löschen des Gateway's mit AMO GKREG und AMO BCSU, ändern des **GATEKPR** Schalters auf **NEIN** und neuerliches konfigurieren des Gateway's mit AMO BFDAT, AMO BCSU und AMO CGWB.

  – Ändern der Gateway-Registrierung von remote auf intern:

  Löschen des Gateway's mit AMO BCSU, ändern des GATEKPR Schalters auf JA und neuerliches konfigurieren des Gateway's mit AMO BFDAT, AMO BCSU, AMO CGWB und AMO GKREG.
- In einer PBX **mit** Gatekeeper kann die Registrierung einiger spezieller loakler Gateways von intern auf remote geändert werden:

  Löschen der Gatewaydaten mit AMO GKREG und anschließender Neukonfigurierung des Gateways mit dem AMO CGWB - REGEXTGK=JA!
- In einer PBX **mit** Gatekeeper kann ein zusätzliches lokales Gateway für remote Registrierung konfiguriert werden:

  Konfigurieren des Gateways mit AMO BFDAT, AMO BCSU und AMO CGWB - **REGEXTGK=JA**!

7.3.6 Einrichten der HG 3500 Rufnummer

Jede HG 3500 benötigt eine Rufnummer, mit der sie am OpenScape 4000 System des Gatekeepers angesprochen werden kann. Die Rufnummer wird einer HG 3500 mit dem AMO CGWB bekanntgegeben (Kommando: `EINR-CGWB:MTYP=CGW,LTU=<nummer>, EBT=<nummer>,TYP=LEGKDATA,GWRNR=<GW-Rufnummer>;`).

Bei einer HG 3500 die sich an einem fremden OpenScape 4000 System mit Gatekeeper registrieren muss ist nicht zwingend ein Eintrag in der Wahlbewertung des eigenen OpenScape 4000 System erforderlich. Im System **mit** Gatekeeper muss jedoch die Rufnummer unter dem Kennzahlpunkt GATEWAY, oder bei mehr als 6 stelliger Rufnummer im LCR, eingerichtet werden.

Als Zusatzinformation benötigt der WABE-Eintrag einer remote HG 3500 am OpenScape 4000 System mit Gatekeeper die zugehörige Gateway Nummer. Diese wird mit dem AMO GKREG beim Einrichten oder Löschen administriert, d.h. in die entsprechenden WABE-Einträge eingetragen oder wieder gelöscht. Damit ist sichergestellt, das ein Betrieb erst aufgenommen werden kann, wenn das Gateway richtig in der LEGK Verwaltung eingerichtet ist.

Die eigene Rufnummer der HG 3500 muss aus dem Rufnummernplan der Teilnehmer stammen.

Bei einer HG 3500 die sich am lokalen OpenScape 4000 registrieren muss ist die Gateway Rufnummer unter Kennzahlpunkt QUER einzurichten (TSC - Verbindung). Eine Gateway Nummer als Zusatzinformation ist in diesem Fall nicht erforderlich.

Der WABE-Eintrag einer HG 3500 (Kennzahlpunkt GATEWAY) kann erst gelöscht werden, wenn zuvor die Gateway Nummer entfernt worden ist. Dazu

muss mit dem AMO GKREG das Gateway aus der LEGK Verwaltung gelöscht werden.

Generierung

AMO WABE

Einrichten der Rufnummer einer **remote** HG 3500 im lokalen System, d.h. das Gateway muss sich im lokalen LEGK registrieren. In diesem Fall muss das Gateway mit dem Kennzahlpunkt GATEWAY eingerichtet werden.

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster Rufnummer durchgeführt werden (Typ=GATEWAY).
	`EINRICHTEN-WABE:RNR=35101,KZP=GATEWAY;` Für die jeweils vordefinierten Verkehrssituationen wird die Rufnummer 35101 eines remote Gateway als KZP Gateway in der Wahlbewertung eingerichtet.

Einrichten der Rufnummer einer HG 3500 im System mit Gatekeeper, d.h. das Gateway kann sich im lokalen Gatekeeper registrieren. In diesem Fall muss das Gateway mit dem Kennzahlpunkt QUER eingerichtet werden.

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster Rufnummer durchgeführt werden (Typ=QUER).
	`EINRICHTEN-WABE:RNR=452001,KZP=QUER;` Für die jeweils vordefinierten Verkehrssituationen wird die Rufnummer 452001 eines lokalen Gateway als KZP Querverbindung in der Wahlbewertung eingerichtet.

Abfragen:

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster Rufnummer durchgeführt werden.
	`ABFRAGEN-WABE:ALLG,Rufnummer;` Der AMO gibt die Daten zur angegebenen Rufnummer aus.

Löschen:

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster Rufnummer durchgeführt werden.
	`LOESCHEN-WABE:RNR,Rufnummer,,Kennzahlpunkt;` Der AMO löscht für den angegebenen Kennzahlpunkt die gewünschte Rufnummer.

7.3.7 Einrichten des IP-Trunking im LCR

Bei der Adressauflösung für TDM-Verbindungen wird eine LCR-Richtung als Zieladressinformation adminstriert, woraus sich nachfolgend der LODEN eines abgehenden Satzes für AMT- oder QUER-Verbindungen ermitteln lässt.

Um den Anforderungen der IP-Adressauflösung gerecht zu werden mit dem AMO LDAT zusätzlich in den LCR-Daten neue Parameter für Ziel Gateways (GW1 bis GW5) administriert. Information über das Ziel Gateway 1...5, bestehend aus:

1) der Gateway Nummer

der Sektor-Pfad Nummer

Über die Gateway-Nummer ist die IP-Adresse des Zielgateways zu ermitteln und somit jedes gewünschte OpenScape 4000 System im IP-Netz des Kunden zu erreichen.

Unter der Sektor-Pfad Nummer sind alle Sektoren einzutragen, die durchlaufen werden, um den Sektor des Ziel-Gateways zu erreichen. Er enthält grundsätzlich nicht die Sekornummern von Ursprungs- und Ziel-Gateway.

Es gibt keine mehreren Pfade für diesen Pfadtyp. Mit anderen Worten, es gibt nur einen definierten Pfad. Damit aber nicht unnötig viele Sektor-Pfade eingerichtet werden müssen, kann ein Sektor-Pfad, der für DMC definiert wurde auch hier angegeben werden. Sollte es sich dabei um einen Mehrfach-Pfad handeln, wird auch hier der richtige Sektor-Pfadteil herausgesucht. Zur besseren Übersicht sollten allerdings getrennte Sektor-Pfade für IP-Trunking und DMC definiert werden.

Die Administration der IP-Adressauflösung ist vom Konzept in die bisherige LCR-Gerätesuche eingebettet und kann mit den selben AMOs (das sind AMO RICHT, LDAT und LDPLN) durchgeführt werden.

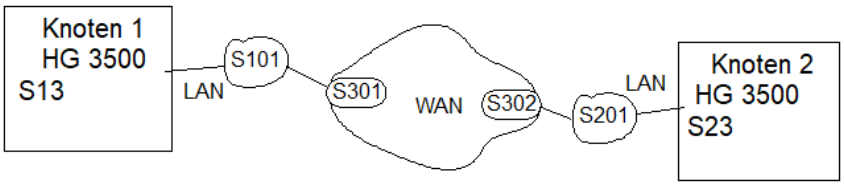


Abbildung 152: Beispiel für Sektor-Pfad Beschreibung

Eine gehende Belegung von Gateway S13 zum Gateways S23 gibt folgenden Sektor-Pfad:

2) **S13 > S23**: S101,S301,S302,S201

Generierung

AMO RICHT

Das Einrichten der LCR-Richtung für IP-Trunking erfolgt mit dem Zweig ART=LRTGNEU. Eine zusätzliche Möglichkeit ist, das beim Einrichten einer IP-Adressauflösung für ein remote Gateway (OpenScape 4000 System ohne Gatekeeper) auf die Bündelnummer verzichtet werden kann, da in diesem Fall keine b-Kanäle an der PBX des Gatekeepers belegt werden müssen.

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtung durchgeführt werden.
	EINRICHTEN-RICHT:ART=LRTGNEU, LRTG=35, LDIENST=ALLE, NAME="STMI2 3- 91", ZKNNR=1-69-300, REROUT=NEIN, ROUTATT=NEIN, EMCYRTT=NEIN, PZKN▶ NR=10-69-300, ZEICHUM=NEUTRAL, CONFTON=NEIN, RERINGRP=NEIN; Die Richtung 35 wird für HG 3500 auf Lage 3-91 für alle Dienste eingerichtet, Bündelnummer wurde keine eingegeben.

AMO LDAT

Mit diesem AMO richtet man für eine LCR-Richtung die erforderlichen LCR-Richtungselemente für IP-Trunking ein.

Jedes Richtungselement kann bis zu fünf Zielgateways von entfernten OpenScape 4000 Systemen enthalten. Die Parameter GW1 bis GW5 definieren die Reihenfolge mit der ein Verbindungsaufbau erfolgt, d.h. zuerst der Weg beschrieben in GW1 bis zuletzt der Weg in GW5.

Reichen fünf Ziel-Gateway nicht aus, so ist ein neues Richtungselement einzurichten, zusätzlich ist hier im Parameter LATTR der Wert LRTGCONT anzugeben. Damit werden weitere fünf Ziel-Gateways für das gleiche Richtungselement angelegt. Es werden dabei automatisch alle Daten des zuvor angelegten Richtungselements unabhängig von der aktuellen AMO-Eingabe übernommen.

Selbstverständlich können wie bisher auch mehrere Richtungselemente mit unterschiedlichen LCR-Parametern für eine LCR-Richtung konfiguriert werden. In diesem Fall darf im Parameter LATTR der Wert LRTGCONT nicht enthalten sein.

Die Angabe der Bündelnummer kann entfallen. Ist eine Bündelnummer angegeben so werden alle bündelspezifischen Daten ebenfalls übernommen.

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtungselement durchgeführt werden.
	EINRICHTEN-LDAT:LROUTE=35, LSVC=ALL, LVAL=1, ODR=2, LAUTH=1, CARRI▶ ER=1, ZONE=TIE01, LATTR=WCHREG, VCCYC=4, GW1=1-1; Für Richtung 35 wird ein Richtungselement mit Wegedaten für Zielgateway 1 angelegt. EINRICHTEN-LDAT:LRTG=35, LWERT=1, LWR=2, LBER=1, LATTR=LCRCONT, GW1=6- 16; Wenn bei Richtung 35 die Wegedaten für alle fünf Zielgateways in einem Richtungselement eingetragen sind, kann mit diesem Folge-Kommando ein weiteres Richtungselement mit den Wegedaten für z.B. das sechste Zielgateway angelegt werden.

AMO LDPLN

Mit diesem AMO richtet man die LCR-Wahlmuster für jedes Zielgateway in den OpenScape 4000 Systemen eines Kundennetzes ein.

Es können 2048 Wählpläne eingerichtet werden. Zuvor müssen jedoch die gewünschten Wählplan Nummern mit dem AMO LDPLN administriert werden. Eine Ausnahme bildet die Wahl der Plannummer 0. Dies konfiguriert Fixes und kann nicht im Zweig LCRCOS=LCRADM verwaltet werden. Hier können sofort beliebige Wählmuster eingerichtet werden.

Soll das LCR-Wahlmuster unter einer anderen Wählplan Nummer als 0 abgelegt werden, so muss diese vor dem ersten Eintrag konfiguriert werden. Dazu wird der Zweig LCRCONF=LCRVERW benützt. Der Benutzer arbeitet in den nachfolgenden AMOs ausschließlich mit der Wählplan Nummer (0-2047).

Eine Wählplan Nummer größer als der fix konfiguriere Plan 0 wird üblicher Weise nur dann benötigt, wenn ein Gatekeeper am lokalen System konfiguriert ist.

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.
	`EINRICHTEN-LDPLN:LCRCONF=LCRVERW, WAPLNUM=2, LWMPOOL=1;` Die Wählplan Nummer 2 wird im LCR-Wählmusterpool 1 auf den ersten nicht belegten Wählplan konfiguriert.

Mit dem folgenden Schritt kann das gewünschte Wählmuster eingerichtet werden

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.

	`EINRICHTEN-LD▶`
	`PLN:LCRCONF=LCRMUST, WAPLNUM=2,`
	`LWM="00891242390", LBER=1, PINP=NEIN;`
	Es wird das Wählmuster 00891242390 unter Wählplan Nummer 2 angelegt.

Einen Sonderfall stellt das Wählmuster dar, das auf ein Gateway führt.

Wenn eine Gateway Rufnummer nicht über die Wahlbewertung (WABE) aufgelöst werden kann, muss sie im LCR-Wählplan WAPLNUM=0 adminstriert werden. Dazu wird folgendes Kommando benötigt (siehe auch Abschnitt 3.6, „Einrichten der HG 3500 Rufnummer“, auf Seite 587).

	Das Einrichten kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.

	`EINRICHTEN-LD▶`
	`PLN:LCRCONF=LCRMUST,WAPLNUM=0,`
	`LWM="008973114711", GWNU=7, LBER=3;`
	Es wird der Gateway Rufnummer 008973114711 das Zielgateway 7 zugeordnet.

Abfragen:

AMO RICHT

	Das Abfragen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtung durchgeführt werden.
	`ABFRAGEN-RICHT:ART=LRTG, LRTG=35;` Der AMO gibt die LCR-Richtungdaten für LRTG 35 aus.

AMO LDAT

	Das Abfragen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtungselement durchgeführt werden.
	`ABFRAGEN-LDAT:ART=LCR, LRTG=35;` Der AMO gibt für LCR-Richtung 35 die konfigurierten Wegedaten aller konfigurieren Richtungselemente aus.

AMO LDPLN

Abfragen der internen Verwaltungs-Konfiguration für die Wählplan Nummer 2.

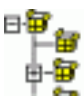
	Das Abfragen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.
	`ABFRAGEN-LDPLN:LCRCONF=LCRVERW, WAPLNUM=2;` Der AMO gibt die Verwaltungsdaten LWMPOOL, WAEHLPLN und INFO für die Wählplan Nummer 2 aus.

Abfragen der eingerichteten Wählmuster für Gateway 7.

	Das Abfragen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.
	`ABFRAGEN-LDPLN:LCRCONF=LWM, GWNU=7;` Der AMO gibt die eingerichteten Wählmuster-Daten für Gateway 7aus.

Löschen:

AMO RICHT

	Das Löschen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtung durchgeführt werden.
	`LOESCHEN-RICHT:ART=LRTG, LRTG=35;` Der AMO löscht die LCR-Richtung 35.

AMO LDAT

	Das Löschen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Richtungselement durchgeführt werden.

	`LOESCHEN-LDAT:ART=LRTG, LRTG=35;`
	Der AMO löscht alle Richtungselemente und Daten für LCR-Richtung 35.
	ODER
	`LOESCHEN-LDAT:ART=LRTGEL, LRTG=35, LRTGEL=1, GWIDX=2;`
	Der AMO löscht für die LCR-Richtung 35 im Richtungselement 1 selektiv nur den zweiten Gateway-Eintrag.

Das letzte Gateway eines LCR-Routelementes kann mittel GWIDX nicht gelöscht werden. In diesem Fall muss das ganze Routeelement (LRTGEL) gelöscht werden.

AMO LDPLN

Löschen der internen Verwaltungs-Konfiguration für die Wählplan Nummer 2.

Eine Wählplan Nummer kann nur gelöscht werden wenn zuvor alle Wählmuster gelöscht sind.

	Das Löschen kann mit OpenScape 4000 Assistant/Manager in dem Fenster LCR-Wählmuster durchgeführt werden.
	`LOESCHEN-LDPLN:LCRCONF=LCRVERW, WAPLNUM=2;` Der AMO löscht die Wählplan Nummer 2. Auf diese Wählpläne kann anschließend nicht mehr zugegriffen werden. Wenn die Wählplan Nummer 2 wieder benötigt wird ist sie neu einzurichten.

Löschen der eingerichteten Wählmuster für eine Wählplan Nummer.

	Das Löschen kann mit OpenScape 4000 Assistant/Manager in dem Fenster Rufnummer durchgeführt werden.
	`LOESCHEN-LDPLN:LCRCONF=LCRMUST, WAPLNUM=6, LWM="0307469412";` Der AMO löscht das eingerichtete Wählmuster 0307469412 für Gateway 6 aus.

7.3.8 Einrichten von Sätzen und Endgeräten

7.3.8.1 Einrichten von Sätzen

An der grundlegenden Konfiguration der analogen (AMO TACSU) und digitalen Leitungssätzen (AMO TDCSU) sowie bei Spezialsätzen (TSCSU) gibt es durch dieses Leistungsmerkmal keine Veränderung.

Parameter **CLASSMRK** muss auf „HG3550: Bandbreitenkontrolle für integriertes HG 3550 IP-Gateway“ gesetzt werden.

7.3.8.2 Einrichten von Endgeräten

An der grundlegenden Konfiguration der Endgerätedaten (AMO SDAT) und des Vermittlungsplatzes (AMO ACSU) gibt es durch dieses Leistungsmerkmal keine Veränderung.

Parameter **CLASSMRK** muss auf „HG3550: Bandbreitenkontrolle für HG 3550 IP-Satz gesetzt werden“.

Im AMO SBCSU ist noch zusätzlich der Parameter **IPCODEC** eingeführt worden. Damit kann der Codec Typ für IP-Endgeräte eingestellt werden. Als Standardwert für STMI2/4-HFA Endgeräte ist der Wert G711PREF vorgesehen.

7.3.9 Ändern der Systembandbreiten

Mit dem AMO SIPCO können unter TYP=BANDW die vorgegebenen Standardbandbreiten der IP-Verbindungen verändert werden.

In der vorhanden Tabelle wurde aufgrund der bisherigen Erfahrungen für jeden Codec Typ und die Sample Size eine standard Bandbreite in kBit fix eingestellt. Diese Werte können mit dem AMO SIPCO geändert werden.

Einrichten:

Beispiel: Ändern der Einstellung für Eintrag Nr. 3 auf 90 KBit

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** **Suchen** klicken, auf Registerkarte **Bandbreitedaten** im Bereich **Diensttyp** die Checkbox **Autom. Verhandlung aktivieren** deaktivieren, sowie **Geschwindigkeit** und **Modus** eingeben und **Sichern**.
	`AENDERN-SIPCO:TYP=BANDW,TBLIDX=3,BWRES=90;` Das Kommando ändet die Bandbreite für Index 3 auf 90 kBit.

Beispiel: Wiederherstellen der Standardwerte für die ganze Tabelle

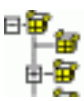
	
	`AENDERN-SIPCO:TYP=BANDW,TBLIDX=0,STANDBW=J;` Das Kommando setzt die gesamte Tabelle auf die definierten Systembandbreiten zurück.

Tabelle 27: Parameter des AMO SIPCO im Ändern-Zweig unter TYP=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table
	BWRES	d	neuer Wert für reservierte Bandbreite in kBit
	BWRES	e	new value for reserved bandwidth in kBit
	STANDBW	d	Rücksetzen auf Standardwerte Wird BWRES=0 angegeben so wird die gesamte Tabelle auf die Standardwerte zurückgesetzt sonsten nur der angegebene Index.
	STANDBW	e	reset to default values Is BWRES=0 entered then the whole table is reset to the default values, otherwise only the entered tableindex..

Löschen:

Beispiel: Löschen von Index 5 in der Systembandbreiten-Tabelle

	
	`LOESCHEN-SIPCO:TYP=BANDW,TBLIDX=5;` Das Kommando löscht die Bandbreite für den Tabellenindex 5.

Tabelle 28: Parameter des AMO SIPCO im Abfragen-Zweig unter TYP=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table

Abfragen:

Beispiel: Ausgeben der eingestellten Systembandbreiten-Tabelle

	
	`ABFRAGEN-SIPCO:TYP=BANDW;` Das Kommando gibt alle konfigurierten Einträge der Systembandbreiten-Tabelle aus.

Tabelle 29: Parameter des AMO SIPCO im Abfragen-Zweig unter TYP=BANDW

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TBLIDX	d	Index eines Eintrages in der Bandbreitentabelle
	TBLIDX	e	Index of an entry in the bandwidth encoding time table

8 HiPath Feature Access (HFA)

8.1 Überblick

Das Gateway HG 3500 bietet IP-Telefonen und analogen Geräten über CorNet IP Zugang zu sämtlichen OpenScape 4000-Leistungsmerkmalen.

HG 3500 bietet folgende Leistungsmerkmale und Vorteile:

- Zugriff auf sämtliche OpenScape 4000-Leistungsmerkmale für folgende IP-Telefone
  - optiPoint 4x0 CorNet IP
  - OpenStage Familie,
  - AP 1120 Analog-Adapter (Mehr Details zum AP 1120 finden Sie im E-Doku-Angebot im Intranet (http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=AP%201120&product_version_main=&product_version_sub=&search_term_type=all&term=result=title&docclass=&language=&checkdate=&lang=de).)
- Das Gateway HG 3500 unterstützt DMCs (Direct Media Connections) zwischen IP-Clients und sorgt so für optimale Sprachqualität bei minimalen Verzögerungen.
- Hohe Sprachqualität. Wegen der systembedingt höheren Verzögerung des Sprachsignals in IP-Netzen beeinflusst Echo die Sprachqualität negativ, wenn es nicht vor der Übertragung entfernt wird. Deshalb haben die HG 3500-Baugruppen integrierte Echo-Canceller.
- HG 3500 bietet eine 10BT/100BT-Schnittstelle zum IP-Netzwerk und unterstützt bis zu 240 IP-Telefone an einem einzelnen Gateway.
- Niedriger Bedarf an Bandbreite.
- HG 3500 unterstützt sämtliche Telefon-Adapter, die keinen eigenen B-Kanal benötigen (Phone-Adapter, a/b-Adapter, S0-Adapter und V.24-Adapter werden nicht unterstützt).
- HG 3500 unterstützt Reserve-Gateways zur Absicherung gegen Ausfälle mehrerer Gateways.
- HG 3500 unterstützt Mobility-Features (einschließlich Unterstützung von E911).
- Die zentrale Verwaltung über OpenScape 4000 Management wird in derselben Weise wie für herkömmliche Teilnehmer unterstützt.
- Die Unterstützung von IP-Telefonen sorgt für Mobilität und stark vereinfachte MAC.
- Es wird die bestehende IP-Infrastruktur genutzt.
- Unterstützt bis zu 12.000 Teilnehmer an einer einzelnen OpenScape 4000, einschließlich der IP-Benutzer an IP Access Points.
- Unterstützung von Quality of Service im IP-Netz durch Priorisierung. HG 3500 unterstützt die Priorisierung im IP-Netz auf Basis folgender Standards:
  - IEEE 802.1 p/q (VLAN-Tagging) auf Schicht 2
  - IETF RFC 2474 (DiffServ) auf der IP Schicht
- Unterstützung von Networkmanagement auf Basis von SNMP. HG 3500 unterstützt Networkmanagement auf Basis des SNMP-Protokolls. Statistische Daten aus den anwendbaren Standard-MIBs sowie zusätzlich Daten aus proprietären MIBs lassen sich abfragen.

8.2 Anwendungsbeispiel

8.2.1 Leistungsmerkmalbeschreibung

Das Leistungsmerkmal HiPath Feature Access (HFA) ermöglicht die stufenlose Migration der Kommunikationsplattform von leitungsgebundener zu IP-basierter Infrastruktur. Damit ist es für den Kunden ausreichend nur mehr ein leistungsfähiges und Quality of Service (QoS) unterstützendes Local Area Network (LAN) zu installieren und zu betreiben. Daten und Sprachkommunikation teilen sich die verfügbare Netzbandbreite, wobei für den Datenverkehr die Durchsatzrate und für die Telefonie die Echtzeitfähigkeit von Bedeutung sind. Folglich ist vor der Installation eines HFA Systems die Untersuchung und Aktualisierung der IP Infrastruktur betreffend Bandbreite und QoS unterstützender LAN Komponenten (Router, Switch, Gateway) entscheidend für die spätere Qualität der Sprachverbindungen.

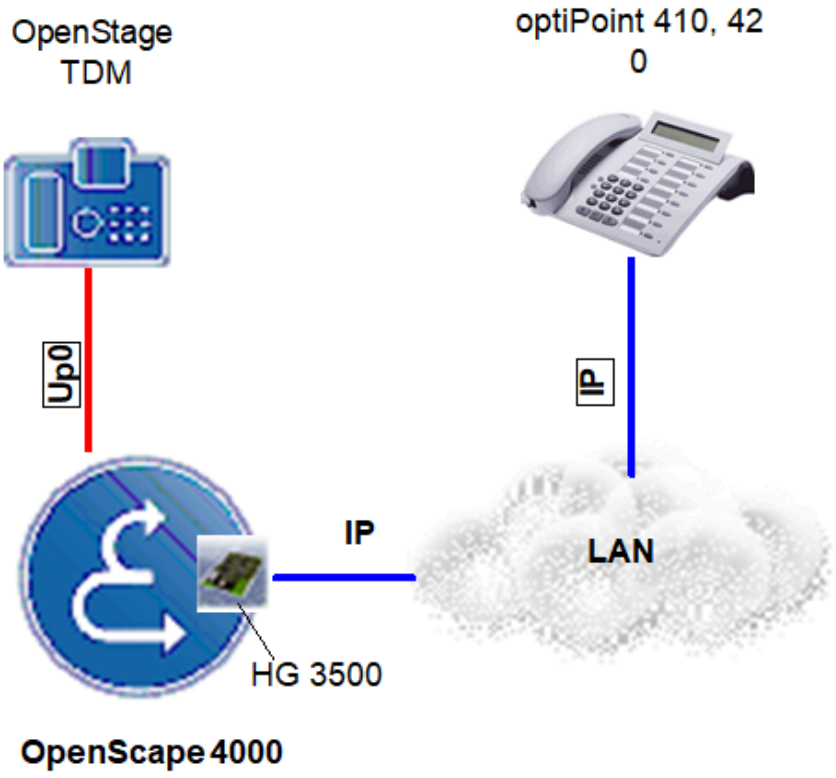


Abbildung 153: HFA Infrastruktur

Das verwendete LAN Segment muss um eine einwandfreie Sprachqualität auch bei hoher Netzbelastung zu gewährleisten, aus QoS unterstützenden LAN Komponenten bestehen. Es wird auch empfohlen ein 100Mbit Ethernet zu verwenden.

Unterstützung von Quality of Service im IP Netzwerk durch Priorisierung

- IEEE 802.1 p/q (VLAN-Tagging) auf Schicht 2
- IETF RFC 2474 (DiffServ) auf Schicht 3.

Für den Teilnehmer gibt es keine wesentlichen Einschränkungen, nur Autoset-Relocate und Teleworking werden nicht unterstützt. Die IP-Endgeräte bieten ansonsten die gleiche Funktionalität wie die UP0e basierten Endgeräte. Es werden aber keine S0 oder a/b Adapter unterstützt.

Mit der HG 3500 werden G.711, G.723 und G.729 unterstützt. Die optiPoint-Endgeräte 410/420 beherrschen bei Direct Media Connection (DMC) auch G.722 mit CD-Qualität.

8.2.1.1 Technischer Hintergrund

Bei UP0e basierenden Teilnehmeranschlüssen wird die Signalisierungsverbindung (D-Kanal) von der Sprachverbindung (B-Kanal) getrennt, indem das physikalische Medium in Zeitschlitze unterteilt wird und den beiden Verbindungen unterschiedliche Zeitschlitze zugeordnet werden. Bei HFA wird die Zweidrahtleitung als physikalisches Medium des digitalen Teilnehmeranschlusses durch ein IP basierendes LAN ersetzt. Die Signalisierungsverbindung zwischen Endgerät und HFA (Common) Gateway benutzt eine gesicherte TCP Verbindung und die Sprachdaten werden über eine H.323 Verbindung mit dem Protokoll RTP/RTCP übertragen. Die beiden Verbindungen können nun in einem LAN unterschiedlich geroutet werden. Es ist deshalb möglich, dass eine Signalisierung besteht, jedoch die Sprachverbindung temporär unterbrochen ist.

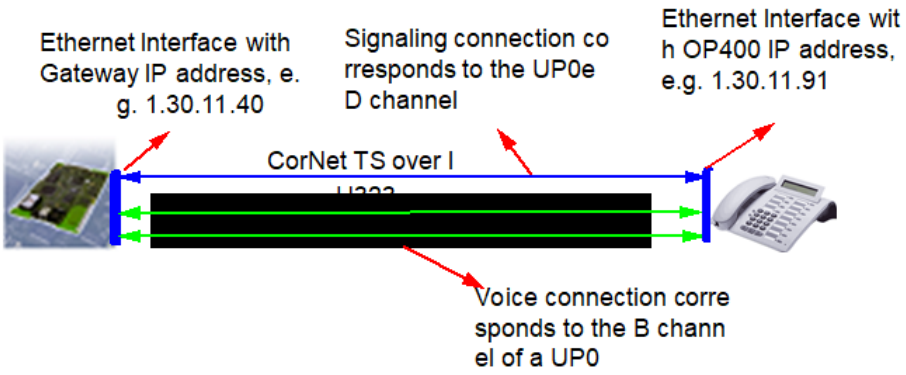


Abbildung 154: Technischer Zusammenhang zwischen UP0e und HFA Teilnehmeranschluss

Um einen HFA-Teilnehmer zu konfigurieren sind daher primär folgende Punkte vorab zu klären:

- IP Adresse, Subnetz-Maske, Subnetz-Gateway IP Adresse des Common-Gateways
- IP Adresse, Subnetz-Maske und Subnetz-Gateway IP Adresse des HFA-Endgerätes

8.2.1.2 HFA Teilnehmerregistrierung

Teilnehmer werden an einer bestimmten Baugruppen-Lage konfiguriert (AMO SBCSU). Während aber ein digitales (oder analoges) Endgerät nach

Anschaltung an seine Baugruppe direkt in Betrieb gehen kann, müssen bei einem IP-Telefon zuerst noch Einstellungen am Endgerät gemacht werden.

Zuerst braucht ein HFA-Teilnehmer eine eigene IP-Adresse, eine Subnetzmaske und optional die Angabe eines Default- (Kundennetz-) Routers. Bei einem Soft-Client hat man natürlich den Vorteil, dass dieser die Netzwerkkarte des PCs benutzt und man daher hier keine Einstellungen vornehmen braucht.

Bei einem HFA-Festgerät müssen die IP-Einstellungen aber geleistet werden. Entweder geschieht dieses „automatisch“ über DHCP (Standardeinstellung der HFA-Festgeräte) oder manuell.

Ein HFA-Teilnehmer mit IP-Einstellungen versucht sich nun bei seinem zuständigen Gatekeeper zu registrieren. Sein Gatekeeper ist die HG 3500, auf deren Lage er eingerichtet ist. Um seine „Heimat“- HG 3500 finden zu können, muss deren IP-Adresse am Endgerät eingestellt werden.

Allein dieses reicht aber noch nicht aus. Die HG 3500 muss noch kontrollieren, ob der Teilnehmer, der ihr einen „Registration Request“ sendet, überhaupt berechtigt ist, sich bei ihr einzubuchen. Zur Identitätsprüfung muss ihr das Endgerät die Teilnehmernummer mitschicken. Die HG 3500 fragt dann in der OpenScape 4000 nach, ob auf ihrer Lage diese Teilnehmernummer eingerichtet ist. Wenn ja, wird der HFA-Teilnehmer registriert - wenn nicht, dann wird der HFA-Teilnehmer abgewiesen. Am Endgerät muss also zwingend die Teilnehmernummer voreingestellt werden.

Um zu verhindern, dass ein User sich einfach mit der Teilnehmernummer eines anderen Mitarbeiters anmeldet, kann man im AMO SBCSU noch ein sogenanntes IP-Passwort (IPPASSW) einrichten. Dieses kann nur über den Administrator verändert werden, aber nicht vom User am Endgerät. Ist im AMO SBCSU ein IP-Passwort eingestellt, so muss es auch am Endgerät konfiguriert sein, sonst wird der Teilnehmer nicht registriert.

Fazit:

IP-Adresse der HG 3500, Teilnehmerrufnummer aus dem AMO SBCSU und optional das IP-Passwort aus dem AMO SBCSU müssen am Endgerät konfiguriert werden, sonst wird das HFA-Endgerät nicht registriert und bleibt somit außer Betrieb. Die Konfiguration dieser Daten kann am Endgerät selbst, über das WBM oder über das DLS erfolgen.

Beim Soft-Client wird die entsprechende Konfiguration nach dem Programmaufruf vorgenommen:

Anmerkung:

In einigen Kundennetzen kann es unter Umständen nötig sein, darüber hinaus die L2-Priorisierung und die VLAN-ID am HFA-Endgerät voreinzustellen. Hier ist aber auch ein Automatismus über DHCP möglich.

Die HG 3500 übergibt nach erfolgreicher Registrierung Daten über den HFA-Teilnehmer an den AMO SBCSU wie zum Beispiel Gerätetyp, IP-Adresse etc. (AB-SBCSU / Zweig TYP=OPTIDAT). Diese Daten können auch im UW7 über das Configuration Menu in der Teilnehmerübersicht eingesehen werden!

In folgender Abbildung ist die Registrierung für den Teilnehmer 4711 schon erfolgt. Das andere Telefon hat zwar alle IP- Einstellungen, ist aber noch nicht registriert.

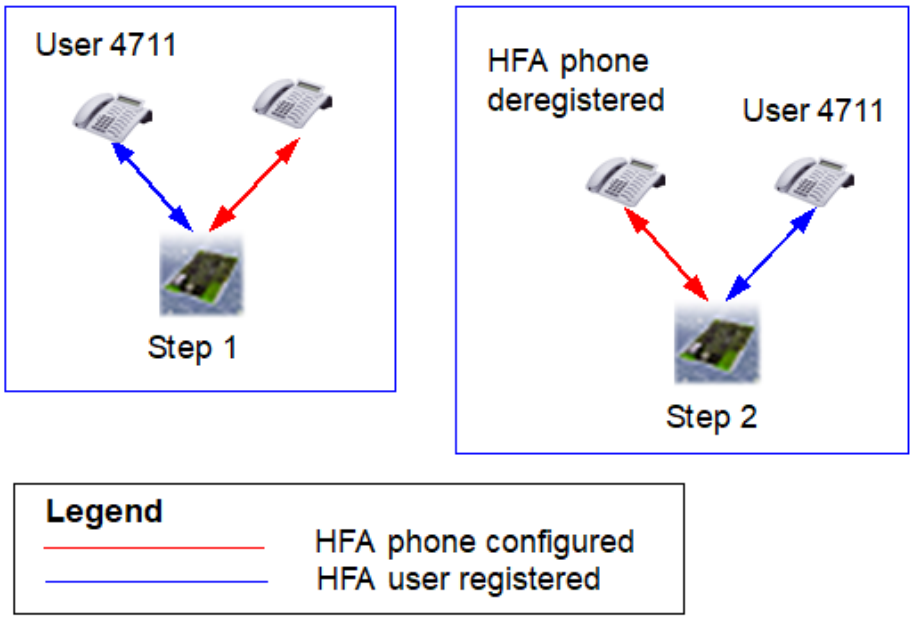


Abbildung 155: Ein Teilnehmer meldet sich bei einem anderen HFA-Endgerät an

Ist ein HFA-Teilnehmer schon angemeldet, kann er zu einem anderen HFA-Endgerät wechseln, indem er sich dort durch Angabe der IP-Adresse seiner „Heimat“-HG 3500, seiner Teilnehmernummer und seines optionalen IP-Passworts anmeldet. Durch die Neuanmeldung wird das ursprüngliche Endgerät automatisch abgemeldet. Dies ist nur dann nicht möglich, wenn eine Gesprächsverbindung zum ursprünglichen Endgerät besteht. Es gibt für HFA-Teilnehmer die Möglichkeit über einen Kennzahlpunkt in der WABE die Umbuchung auf ein anderes Endgerät vorzunehmen. Dadurch muss der Teilnehmer am Endgerät nicht mehr das versteckte Konfigurationsmenu für einen Umzug aufrufen. Die Einrichtung des Leistungsmerkmals „Mobile HFA“ finden Sie in den „IP Lösungen“, „Mobile HFA Logon“.

8.2.2 Benutzeroberfläche

Die Benutzeroberfläche für die Administration der IP-HFA-Endgeräte ist spezifisch für jedes Endgerät und daher nicht Teil dieses Dokuments (siehe dazu Administrationshandbücher für die relevanten Endgeräte).

Zum Einrichten eines HFA-Endgeräts können Sie die folgenden Optionen verwenden:

- Direkte Administration über das Endgerät oder über das WBM des Endgeräts.

  Siehe hierzu die Dokumentation zu Ihrem HFA-Endgerät (http://apps.g-dms.com:8081/techdoc/search_de.htm).
- OpenScape Deployment Service (DLS):

  DLS (http://apps.g-dms.com:8081/techdoc/de/P31003S2330M1000100A9/index.htm).

  Die folgenden Pflicht-Parameter müssen versorgt werden, damit das Endgerät betriebsfähig ist:

- Vollqualifizierte Telefonnummer (E.164)
- Adresse und Port des Gateways (HG3500)
- Kennwort des Teilnehmers

Wenn sich ein Teilnehmer erfolgreich registriert hat, steht ihm die gleiche Benutzeroberfläche wie bei Standard digitalen Endgeräten zur Verfügung.

8.2.3 Einschränkungen

Es bestehen die folgenden funktionalen Einschränkungen:

- Autoset-Relocate ist für den HFA-Teilnehmer nicht nutzbar
- Teleworking TW2.6 ist für den HFA-Teilnehmer nicht erlaubt
- Es werden keine S0 oder a/b Adapter unterstützt

8.2.4 Generierung

Wichtig: Wenn T.38 mit AP 1120 verwendet werden soll, muss G.711 als Sprachcodec konfiguriert werden, d.h. immer wenn ein Modem oder Fax an einem AP 1120 angeschlossen wird, muss im AP 1120 als Sprachcodec G.711 eingestellt werden (keine Kompression möglich).

Vor der Erstkonfiguration eines HFA-Teilnehmers muss die Speicherkonfiguration mit dem AMO-DIMSU geprüft werden:
`PRUEFEN-DIMSU:LIST=JA;`

Um nun zum Beispiel 4 Baugruppen zu konfigurieren, muss folgende Konfiguration durchgeführt werden:
`EINRICHTEN-DIMSU:TYP=SYSTEM,CGW=4;`

Die Einstellung G.711-Codierungsart (a-law oder µ-law) der IP-Sprachdaten erfolgt über die zentralen Anlagendaten (in der Regel schon richtig gesetzt):
`AENDERN-ZAND:TYP=CONFC,KENNL=<ALAW/ULAW>;`

Jetzt kann die Konfiguration der HG 3500-Baugruppe beginnen.

8.2.4.1 Konfiguration der HG 3500-Baugruppe

Konfiguration der HG 3500 Baugruppe mit dem AMO-BFDAT werden die Funktionsblöcke der HG 3500 konfiguriert. Im Beispiel wird eine STMI4 (Q2324-X510) mit 120 möglichen B-Kanälen nur mit HFA eingerichtet.
`EINRICHTEN-BFDAT:FCTBLK=6,FUNCTION=HG3530,BGBKAN=BKAN120;`

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=6,FUNCTION=HG3530,ANZSATZ=60,ANZBKAN=6
/*Es werden 60 HG 3530-B-Kanäle konfiguriert
```

Die Konfiguration der Baugruppe wird mit dem folgenden Kommando abgeschlossen:
`AENDERN-BFDAT:CONFIG=OK,FCTBLK=6,ANTW=JA;`

Mit dem AMO-BCSU werden die LTU-Baugruppen konfiguriert:
`EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=14,SACHNR="Q2324-`

```
X510",FCTID=1,LWVAR="0",FCTBLK=6,BKAN3530=60,ALARMNR=0;
```

Die Konfiguration der IP-Adressen, Subnetz-Masken etc. der Loadware erfolgt über den AMO-CGWB.

```
EINR-
CGWB:LTU=3,EBT=14,SMODE=NORMAL,IPADR=172.28.145.240,NETMASK=2
55.255.255.0;
```

Jetzt müssen die Baugruppendaten und die Satzdaten noch auf die Baugruppe geladen werden. Dies geschieht entweder durch das Stecken der STMI-Baugruppe nach der Generierung mit dem AMO CGWB oder durch das Kommando:

```
RESTART-
BSSU:ADRART=LAGE,LTG=1,LTU=3,EBT=14>,WTIME=<wartezeit
zwischen ein- und ausschalten in sekunden>;
```

8.2.4.2 Einrichten der HFA-Teilnehmer

Danach können die HFA-Teilnehmer (IP Phones) konfiguriert werden.

```
EINR-
SBCSU:TLNNU=<Nummer>,ART=OPTI,ANSCHL=IP2,GERKON=OPTIIP,COS1=3
3,COS2=30,LCOSS1=5,LCOSS2=1,LCOSD1=5,LCOSD2=1,
[IPPASSW=<Passw
ort>];
```

Wenn Ein Soft-Client als Besonderheit hat, dass er als Leistungsmerkmal TAPI 1st party besitzt, benötigt er aus diesem Grunde einen andere SBCSU-Konfiguration:

```
EINRICHTEN-
SBCSU:TLNNU=<number>,ART=OPTI,ANSCHL=IP2,GERKON=OPTIIP&API,
COS1=33,
COS2=30,LCOSS1=5,LCOSS2=1,LCOSD1=5,LCOSD2=1,APICLASS=TSX,
[IPPASSW=<Passwort>];
```

Jedem HFA-Teilnehmer kann für die Anmeldung ein eigenes Passwort vergeben werden, welches durch den Administrator festgelegt wird und ähnlich der PIN vom Teilnehmer selbst nicht administriert werden kann. Wird kein Passwort angegeben, dann genügt bei der Anmeldung die Teilnehmerrufnummer.

8.2.5 Generierung über OpenScape 4000 Assistant

8.2.5.1 Einrichtung der HG 3500 über den OpenScape 4000 Assistant

HG 3500 lässt sich über das Configuration Management des OpenScape 4000 Assistant einrichten und verwalten.

Zunächst müssen die Funktionsblöcke eingestellt werden (entsprechender AMO: AMO BFDAT).

Start **Configuration Management > Anlagendaten > Baugruppe > CGW-Funktionsblock**.

Klicken Sie auf die Schaltfläche **Suchen**, um zu ermitteln, welche Funktionsblöcke bereits konfiguriert wurden. Bei dem Beispiel im folgenden Fenster wurden fünf Funktionsblöcke konfiguriert. Zum Anzeigen der Funktionsblöcke klicken Sie sich durch die Objektliste.

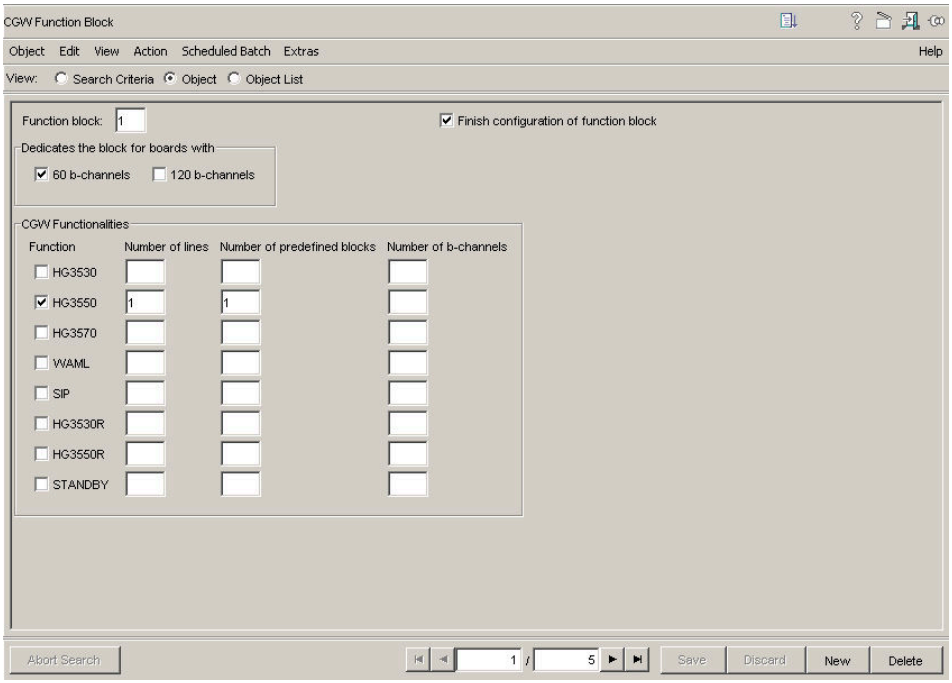


Abbildung 156: Configuration Management - CGW-Funktionsblock - Ansicht: Objekt

Es besteht auch die Möglichkeiten, sämtliche Funktionsblöcke in einer Tabelle anzuzeigen. Markieren Sie hierzu die Option **Objektliste**.

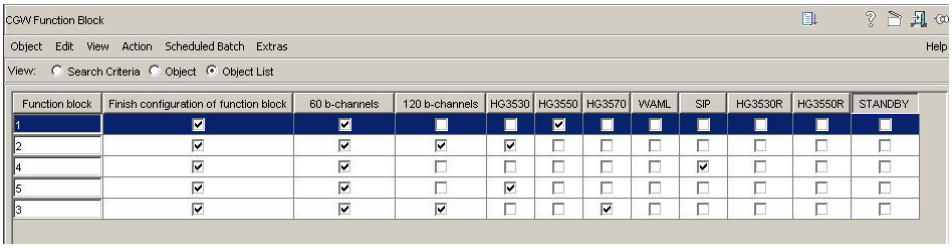


Abbildung 157: Configuration Management - CGW-Funktionsblock - Ansicht: Objektliste

Zum Konfigurieren eines neuen Funktionsblocks klicken Sie auf **Neu**. Geben Sie bei **Funktionsblock** eine freie Nummer ein. Stellen Sie die maximale Anzahl von B-Kanälen der Common Gateway-Baugruppe ein. Wählen Sie die gewünschte(n) Funktion(en) für den Funktionsblock. Klicken Sie auf **Sichern**. Anschließend müssen Sie für die ausgewählten Funktionen die erforderliche **Anzahl der Leitungen**, die **Anzahl vordefinierter Blöcke** und/oder die **Anzahl der B-Kanäle** eingeben. Klicken Sie danach erneut auf **Sichern**. Wenn Sie mit der Konfiguration des aktuellen Funktionsblocks fertig sind, wählen Sie **Konfiguration des Funktionsblocks abschließen** und klicken Sie auf **Sichern**.

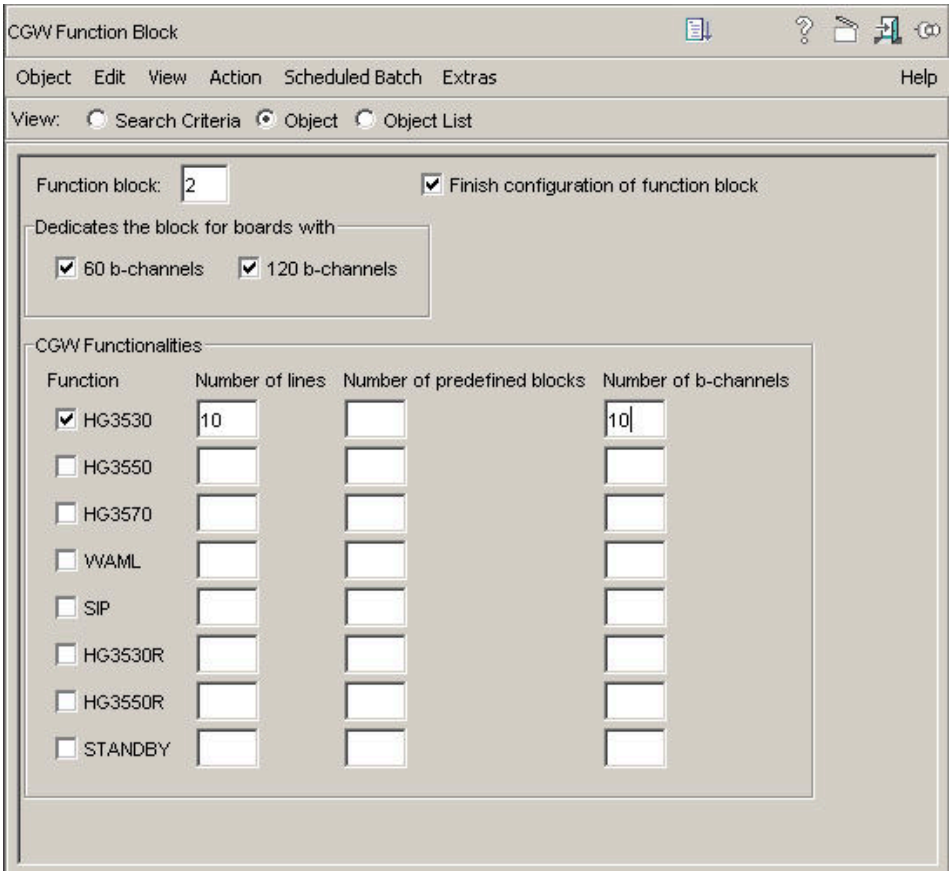


Abbildung 158: Configuration Management - Neuen CGW-Funktionsblock konfigurieren

Nun müssen Sie dem Funktionsblock eine Common Gateway-Baugruppe zuweisen (entsprechender AMO: AMO BCSU). Start **Configuration Management > Systemdaten > Baugruppe > Baugruppe**. Klicken Sie auf **Suchen**, um nach allen im System konfigurierten Baugruppen zu suchen.

Zum Konfigurieren einer neuen Common Gateway-Baugruppe wählen Sie die gewünschte Baugruppe aus (**Sachnummer**) und klicken Sie auf **Neu**. Die folgenden Daten sind einzugeben:

- LTU
- EBT
- Sachnummer
- Function ID (ist grundsätzlich auf 1 eingestellt)
- Baugruppenname
- CGW-Funktionsblock

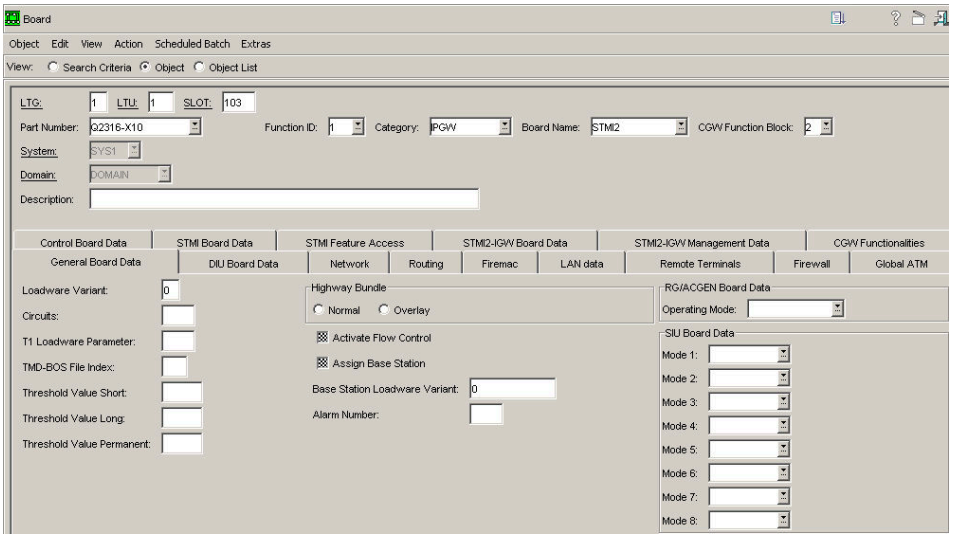


Abbildung 159: Configuration Management - Baugruppe

Wählen Sie die Registerkarte **STMI2-IGW Baugruppendaten** (entsprechende AMOs: AMO BCSU und AMO CGWB). Hier müssen die folgenden Eingaben gemacht werden:

- Ethernet-Schnittstelle
  - IP-Adresse des Kunden-LAN
  - Subnetzmaske
  - Standard Gateway IP-Adresse
- Daten für Large Enterprise Gatekeeper
- Amtsprotokoll (im vorliegenden Beispiel nicht verwendet)
- Primärer und sekundärer Gatekeeper
- Gateway-Daten
- H.235-Sicherheitsdaten
- Dienstschnittstelle

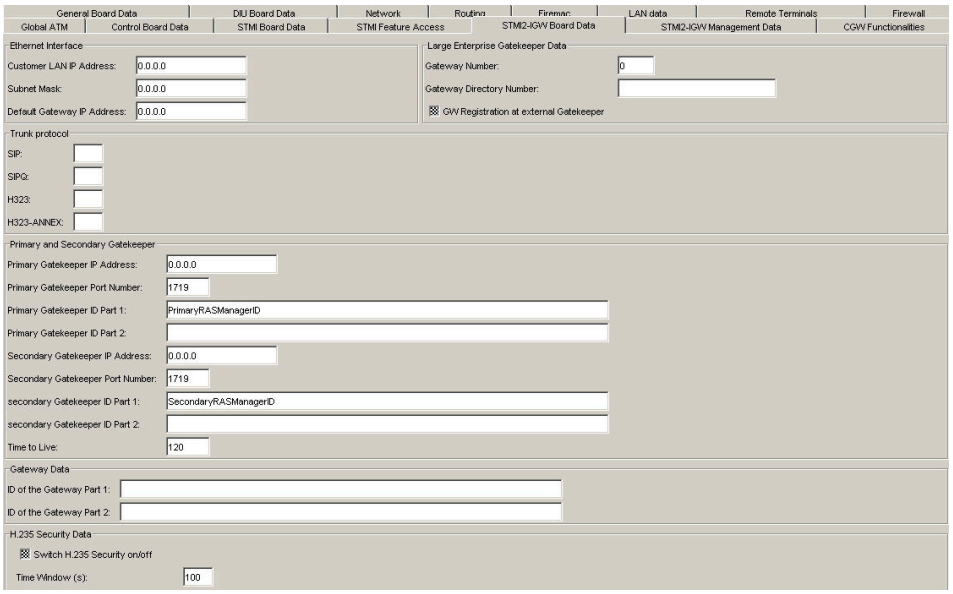


Abbildung 160: Configuration Management - Baugruppe - Registerkarte STMI2-IGW Baugruppendaten

Die nächste Bildschirmabbildung zeigt die Registerkarte **STMI Baugruppendaten**. Hier können Sie u.a. Einstellungen für **Ruhemuster**, **IP- Adresse** und **Anzahl DMC-Verbindungen** vornehmen(entsprechender AMO: AMO CGWB).

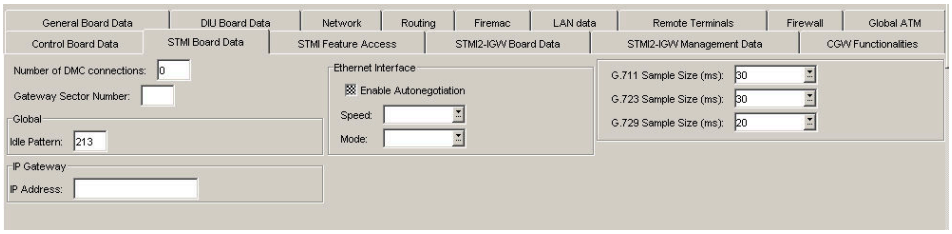


Abbildung 161: Configuration Management - Baugruppe - Registerkarte STMI Baugruppendaten

Speichern Sie nun die gemachten Einstellungen mit der Schaltfläche **Sichern**.

Gehen Sie über die Schaltfläche **Suchen** auf die von Ihnen bereits konfigurierte Baugruppe. Auf der Registerkarte **STMI-Leistungsmerkmalzugriff** (entsprechender AMO: AMO CGWB) können Sie die gewünschte Betriebsart für das Common Gateway konfigurieren (**Normal**, **Standby bereit** oder **Standby defekt**) und Einstellungen zur **Ethernet-Schnittstelle** und zu den **Audio-Stream-Steuerdaten** vornehmen.

Wichtig: Hierbei sollte darauf geachtet werden, dass die Anzahl der UDP-Ports mindestens doppelt so groß ist wie die Anzahl der B-Kanäle der Common Gateway-Baugruppe.

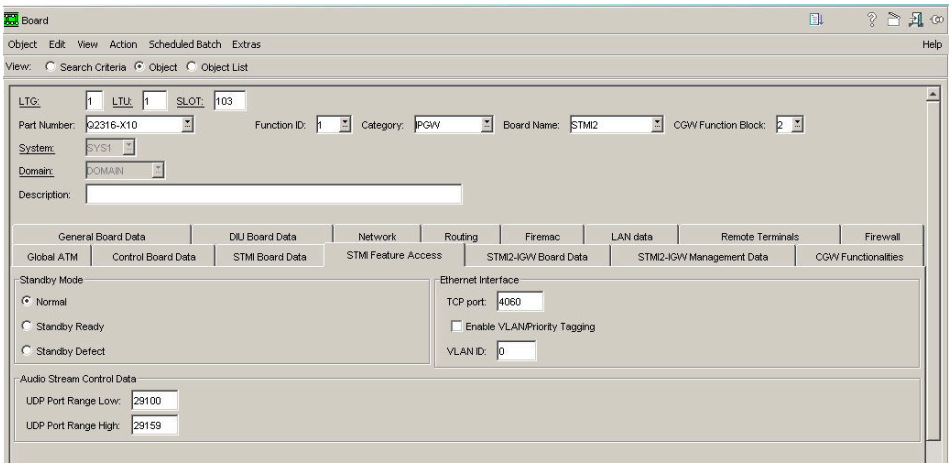


Abbildung 162: Configuration Management - Baugruppe - Registerkarte STMI-Leistungsmerkmalzugriff

8.2.5.2 Einrichten eines HFA-Teilnehmers über den OpenScape 4000 Assistant

HFA-Teilnehmer werden wie Up0/E-Teilnehmern eingerichtet.

Start **Configuration Management > Anschluss > Teilnehmeranschluss**

Im Kopf des Eingabefensters kann man **Rufnummer**, **Lage**, **Gerätekombination**, **Anschlussart** etc. konfigurieren.

Unter der Registerkarte **Basis 1** finden sich die Standardeinstellungen und andere Benutzerdaten aus AMO SBCSU.

Nicht abgebildet ist die Registerkarte **Basis 2**, auf der das IPPASSW aus AMO SBCSU eingegeben wird. Dort sieht man auch die IP-Adresse eines eingerichteten Teilnehmers.

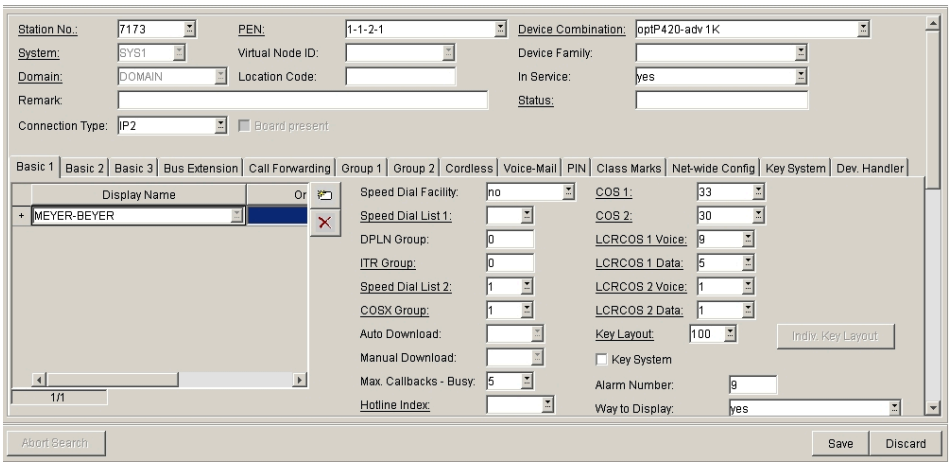


Abbildung 163: Configuration Management - Baugruppe - Registerkarte Basis 1

8.2.6 Löschen

Das Löschen von HFA-Komponenten ist nicht symmetrisch zur Generierung: Der AMO CGWB hat keinen Löschzweig, da einmal eingerichtete Baugruppendaten immer bis zum Löschen der Baugruppe mit dem AMO BCSU gültig sind.

Beispiel: Es sollen die im vorherigem Abschnitt generierten HFA-Komponenten gelöscht werden.

Zuerst werden die HFA-Teilnehmer gelöscht:
`LOESCHEN-SBCSU:TLNNU=<number>,DIENST=ALLE;`

Danach kann sofort die Common Gateway Baugruppe gelöscht werden. Damit sind auch die Baugruppendaten automatisch gelöscht, so dass kein AMO CGWB Kommando nötig ist.
`LOESCHEN-BCSU:TYP=IPGW,LTG=<LTGNR>,LTU=<LTUNR>,EBT=<EBTNR>;`

Anschließend können Sie die Baugruppe mit anderen Funktionen neu konfigurieren.

8.2.7 Tuning der Sprachqualität

In Abhängigkeit von der vorhandenen Infrastruktur stehen im AMO CGWB, Zweig DSP verschiedene Konfigurationsparameter zur Verfügung:

- Rauschunterdrückung durch Voice Activity Detection
- Behebung von Problemen mit Paketverzögerung und Paketreihenfolge
- Echounterdrückung
- Samplelänge

Die Steuerung dieser Leistungsmerkmale erfolgt durch den AMO CGWB. Bei der Verwendung im laufenden Betrieb ist hier kein explizites Nachladen der Baugruppen-Daten notwendig. Die Daten werden sofort auf der Baugruppe wirksam.

HG 35XX beherrscht unterschiedliche Moden des Jitter Buffers. Bei HG 3500 gibt es zwei unterschiedliche Einstellungsvarianten:

1) Der **statische Jitter Buffer mit Drift-Korrektur**. Die Länge des Jitter Buffers bleibt immer konstant (er wird fest eingestellt wie im „legacy mode“, aber es findet eine Anpassung an die Laufzeit des ankommenden Signals statt.
`AENDERN-`
`CGWB:MTYP=CGW,LTU=<ltunr>,EBT=<ebtnr>,TYP=JB,JBMODE=1;`

WBM > Explorer > Payload > HW-Module > DSP Jitter Buffer-Einstellungen ändern > Jitter-Buffer-Typ > Statisch

2) Der **adaptive Jitterbuffer** (Standardeinstellung). Dieser Modus kann sowohl die Drift korrigieren als auch sich in seiner Größe dynamisch anpassen. Der im Parameter JITBUFD eingestellte Wert wird bei dieser Methode nicht ausgewertet. Aktiviert wird der adaptive Jitter Buffer über
`AENDERN-`
`CGWB:MTYP=CGW,LTU=<ltunr>,EBT=<ebtnr>,TYP=JB,JBMODE=2;`

WBM > Explorer > Payload > HW-Module > DSP Jitter Buffer-Einstellungen ändern > Jitter-Buffer-Typ > Adaptiv

Der Jitter Buffer kann durch Festlegen von Werten für die folgenden Parameter noch optimiert werden:

- **Durchschnittliche Verzögerung für Sprache (ms) - AVGDLYV**

Legt den Normalwert (Anfangswert) des Jitter Buffers fest.

- **Maximale Verzögerung für Sprache (ms) - MAXDLYV**

Legt die größtmögliche Länge des Jitter Buffers fest.

- **Minimale Verzögerung für Sprache (ms) - MINDLYV**

Legt die geringstmögliche Länge des Jitter Buffers fest.

- **Paket-Verlust / Delay-Präferenz - PACKLOSS**

Optimiert werden kann der Jitter Buffer durch den Parameter PACKLOSS. Der Standardwert 4 sollte zunächst immer voreingestellt werden. Setzt man den Wert auf 0, 1, 2oder 3, so versucht der Algorithmus Paketverlust zu vermeiden und vergrößert den Jitter Buffer bei auftretenden Problemen. Umgekehrt versucht der Algorithmus bei PACKLOSS= 5, 6, 7 oder 8

zunehmend immer mit einem möglichst kleinen Jitter Buffer zu arbeiten und nimmt dabei auch einen gewissen Paketverlust in Kauf.

- **Durchschnittliche Verzögerung für Daten (ms) - AVGDLYD**

Legt den Normalwert (Anfangswert) des Jitter Buffers für den Dienst Daten fest

- **Minimale Verzögerung für Daten (ms) - MINDLYD**

Legt die größtmögliche Länge des Jitter Buffers für den Dienst Daten fest

Bei HG 3500 wird empfohlen, den **adaptiven Jitter Buffer** zu verwenden. Falls jedoch ältere Faxgeräte vorhanden sind, ist unter Umständen ein statischer Jitter Buffer die bessere Wahl.

Weitere wichtige Parameter:

- **Voice Activity Detection**: **WBM > Explorers > Voice Gateway > Codec-Parameter**
- **Echo Canceller**: **WBM > Explorers > Payload > HW-Baugruppen > DSP-Einstellungen bearbeiten**

Weitere Parameter im AMO CGWB, TYP=ASC:

Parameter	Beschreibung
VAD	Erkennung von Stille durch Voice Activity Detection (AMO CGWB:TYP=ASC, VAD=<ja,nein>)
RTP	Samplelänge der RTP-Paket in Abhängigkeit der Codecs.

8.2.8 Einschalten der Sprachkomprimierung

Das Einschalten der Sprachkompression vollzieht sich in der HG 3500 im AMO CGWB über den Zweig ASC. Für die Einstellung ist der Parameter CODECLST relevant. Wichtig ist es dabei auf die Reihenfolge der Codecs zu achten. Im nachfolgenden Beispiel verwendet die HG 3500 als erste Wahl G.729, als zweite Wahl G.711A und als dritte Wahl G.723. Welcher dieser Codecs letztlich genommen wird, hängt von den Einstellungen an der Gegenstelle (Teilnehmer) ab.

```
AENDERN-
CGWB:MTYP=CGW,LTU=<ltunr>,EBT=<ebtnr>,TYP=ASC,PRIO=PRIO1,CODEC=G729;
AENDERN-
CGWB:MTYP=CGW,LTU=<ltunr>,EBT=<ebtnr>,TYP=ASC,PRIO=PRIO2,CODEC=G711A;
AENDERN-
CGWB:MTYP=CGW,LTU=<ltunr>,EBT=<ebtnr>,TYP=ASC,PRIO=PRIO3,CODEC=G723;
```

8.2.9 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BSSU	ADRART=LAGE	d	Adressierung ueber physikalische Lage

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ADDRTYPE=PEN	e	Physical board/module address
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanäle für die HG3530 Funktion
	BCHL3530	e	Amount of b-channels for HG3530 function
	FCTID	d	Function Id (muss immer 1 sein)
	FCTID	e	Function id (mustbe set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Index to loadware block for the t1 board
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part number (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	SACHNR1	d	Sachnummer der zu ersetzenden Baugruppe (2. und 3. Block)
	PARTNO1	e	Part number of module that has to be replaced (2nd and 3rd bloc)
	SACHNR2	d	Sachnummer der neuen Baugruppe (2. und 3. Block)
	PARTNO2	e	Part number of new module (2nd and 3rd bloc)
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/ oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	ontinue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	3	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden.
	FUNCTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function.
BSSU	WTIME	d	Bei RESTART-Kommando: Wartezeit zwischen Aus- und Wiedereinschalten in Sekunden. Mögliche Werte: 0-20
	WTIME	e	For RESTART command: Wait time between switching off and switching on in seconds. Possible values: 0-20

AMO	Parameter	Sprache/ Language	Beschreibung/Description
CGWB	SMODE=NORMAL	d	Standby Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Standby Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Standby Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Standby Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Standby Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Standby Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board
	MTYP=INITCGWB	d	Zurücksetzen der Konfigurationsdaten der Common Gateway Baugruppe auf die Standardwerte
	MTYPE=INITCGWB	e	Reset configuration data of common gateway board to default values

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network addresss part but different host address parts (also the Default Router must fulfill this requirement)
DIMSU	CGW	d	Anzahl der Common Gateway-Baugruppen
	CGW	e	Number of common gateway boards
	TYP=APPLIKAT	d	DIMSU-Option: Applikation
	TYPE=APPLICAT	e	DIMSU options: application
	WSPROT	d	Sprach/Daten Applikation mit Workstation Protokoll
	WSPROT	e	integrated voice/data application using workstation prot.
SBCSU	ANSCHL=IP2	d	Anschluss-Art der Geräte IP2=Anschluss ueber IP (HFA Gateway Version 2)
	CONN=IP2	e	Device Connection Type IP2=Connection via IP (HFA gateway version 2)
	ART=OPTI	d	Hauptrufnummer des IP-Telefonan-schluss einrichten
	OPT=OPTI	e	Specification of bus type or unit to be expanded
	GERKON=OPTIIP	d	Geräte-Konstellation eines Teilnehmers OPTIIP=IP Sprachterminal

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DVCFIG=OPTIIP	e	Device Configuration OPTIIP=Digital IP voice terminal
	IPPASSW	d	passwort fuer ip login prozedur
	IPPASSW	e	Password for IP logon procedure
	SNU	d	Standard Tastaturbelegung
	STD	e	Standard Key Layout
ZAND	APIMAX	d	Maximale Anzahl der gleichzeitig aktiven API Sessions. DB-Initialisierung: 10
	APIMAX	e	Maximum number of allowable active API sessions. DB initialization: 10
	KENNL	d	Linearisierungs- und Kompandierungskennlinien bei der PCM-Kodierung/Dekodierung. Der eingegebene Wert wird zum einen in die zentralen Anlagendaten übernommen, zum anderen bei eingerichteter LTG auch in die entsprechenden COFI-Daten. Der Wert in den zentralen Anlagendaten ist auch gültig bei der Konfiguration von NCUI-Baugruppen in NBCS-Shelfs.Es sollte daher nach Konfiguration von NBCS-Shelfs dieser Wert nicht mehr geändert werden!
	CODE	e	Speech coding.The entered value will be issued once to central system data and once for assigned LTG in the according COFI-data. The value in central system data is also valid for configuration of NCUI-boards in NBCS shelfs. Therefore this value should not be changed after configuration of NBCS-shelfs!
	TYP=CIT	d	Konfigurieren von fiktiven Geräten, Einstellungen für API Schnittstelle
	TYPE=CIT	e	Configure virtual stations, settings for API interface

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	TYP=CONFC	d	Länderspezifische Einstellung für KENNL, K- oder TDAEMPF. Dieser Zweig gilt nur für kompakte Hardware.
	TYPE=CONFC	e	Selection of country-specific settings for CODE, CONFAT STNAT. This branch is only for compact hardware.

8.3 FAQs (häufig gestellte Fragen)

1) **Frage**: Wie weit kann ein IP-Telefon maximal vom Host entfernt sein?

Antwort: Es gibt bezüglich der Entfernung keine feste Einschränkung. In der Praxis ergeben sich jedoch durch die Verzögerungen bei der Übertragung Einschränkungen der Reichweite. Mit zunehmendem Abstand zwischen Host und IP-Workpoint werden auch die durch das zugrundeliegende Netzwerk erzeugten Verzögerungen größer. Nach Möglichkeit sollten die Verzögerung in einer Richtung weniger als 200 ms betragen.

2) **Frage**: Wie viele IP-Telefone werden pro OpenScape 4000 unterstützt?

Antwort: Pro OpenScape 4000 werden bis zu 12.000 IP-Telefone unterstützt. HG 3500 wird dabei auf sämtlichen IP Access Points unterstützt.

3) **Frage**: Wie viele IP-Telefone werden pro HG 3500 maximal unterstützt?

Antwort: Pro HG 3500 werden maximal 240 IP-Telefone unterstützt. In Abhängigkeit von den Anforderungen der Teilnehmer wird ein GW für 60 oder für 120 Verbindungen benötigt.

4) **Frage**: Werden Gesprächsverbindungen zwischen IP-Telefonen im IP-Netzwerk vermittelt?

Antwort: Ja. HG 3500 Gateways unterstützen Peer-to-Peer-Verbindungen (IP-Switching).

5) **Frage**: Unterstützen an HG 3500-Gateways angeschaltete IP-Telefone Mobility-Funktionen?

Antwort: Ja. Es stehen folgende Optionen zur Verfügung:

- Der Benutzer kann sein IP-Telefon in ein anderes Büro oder an einen anderen Standort mitnehmen, wobei die entsprechenden Daten automatisch, d.h. ohne Zutun des Benutzers, übernommen werden.
- Der Benutzer kann sich von jedem beliebigen Standort über einen Soft-Client an seinem Workpoint anmelden. Letzterer wird dabei automatisch vom OpenScape 4000-Gateway getrennt. Am Soft-Client stehen dem Benutzer die selben Leistungsmerkmale und Berechtigungen zur Verfügung wie am Standard-Workpoint.
- Der Benutzer kann sich an einem beliebigen IP-Telefon innerhalb des Systems oder CorNet-Netzwerks anmelden und das Telefon vorübergehend zu seinem Stammapparat machen. Das ursprüngliche Stammgerät wird hierbei automatisch abgemeldet. Anrufe auf dieses Telefon werden entsprechend den CFNR (Call Forwarding No Reply,

Rufweiterschaltung)-Einstellungen umgeleitet. Am „Gast-Telefon“ stehen dem Benutzer die selben Leistungsmerkmale und Berechtigungen zur Verfügung wie am Standard-Workpoint.

6) **Frage**: Müssen die Telefone statische IP-Adressen haben?

   Antwort: Nein, die aktuelle Version des HG 3500-Gateways unterstützt für DHCP konfigurierte Clients. Dabei muss im IP-Netzwerk ein DHCP-Server eingerichtet sein. Andernfalls müssen sämtliche Clients eine statische IP-Adresse haben.

7) **Frage**: Können Benutzer über eine Wireless-Verbindung angeschaltet werden?

   Antwort: Ja. Nachdem IP-Gateways das Standard-TCP/IP-Protokoll unterstützen und für Verbindungen über WAN-Links ausgelegt sind, gibt es bestenfalls Probleme mit übermäßigen Verzögerungen. Um Verzögerungen zu minimieren, muss sichergestellt werden, dass die Wireless-Transceiver wie Ethernet-Bridges funktionieren.

8) **Frage**: Werden IP-Payload- bzw. -Signalisierungspakete automatisch in die richtige Reihenfolge gebracht, falls sie in der falschen Reihenfolge ankommen?

   Antwort: Solange sich die jeweiligen IP-Payload-Pakete noch im Jitter-Buffer befinden, werden in der falschen Reihenfolge eingegangene IP-Pakete automatisch neu geordnet. Nachdem bei der Signalisierung mit TCP/IP gearbeitet wird, werden Pakete mit einer falschen Reihenfolge vom Protokoll richtig verarbeitet.

9) **Frage**: Welche Protokolle werden für die Signalisierung und für QoS verwendet?

   Antwort: Signalisierung: TCP/IP QoS: LAN-Tagging gemäß IEEE 802.1p/q, DiffServ gemäß RFC 2474

10) **Frage**: Ist die H.323 Fast Connect-Prozedur bei der HG 3500 implementiert?

    Antwort: Ja, zur Verkürzung der Verbindungsaufbauzeit wird die H.323 Fast Connect-Prozedur verwendet, um Daten zum logischen H.245-Kanal auszutauschen.

11) **Frage**: Was passiert beim Anrufer, wenn das IP-Netzwerk ausgefallen ist und die OpenScape 4000 die IP-Telefone nicht erkennt?

    Antwort: Wenn keine Konnektivität zum IP-Telefon mehr besteht, befindet sich das Telefon in einem Reset-Zustand und versucht, wieder eine Verbindung zum Gatekeeper herzustellen. Es gibt keine Displaymeldung zu diesem Zustand. Außerdem ertönt kein Wählton. Ankommende Anrufe können mit Hilfe des Leistungsmerkmals „Alternate Routing on Error“ und LCR-Regeln auf ein beliebiges anderes Ziel umgeleitet werden, z.B. auf eine PhoneMail.

12) **Frage**: Findet bei einer DMC-Verbindung eine QoS/Payload-Überwachung statt?

    Antwort: Nein, HG 3500 bemerkt DMC-Verbindungen nicht.

13) **Frage**: Wie lange dauert die Neuanmeldung von IP-Telefonen an einem Reserve-GW?

    Antwort: Laut Leistungstests mit HG 3500 Reserve-Gateways dauert es ca. 2-3 Minuten, um 240 Telefone an der Reserve-Baugruppe neu anzumelden.

14) **Frage**: Warum werden auf der Baugruppenvariante für 120 Verbindungen nicht mehr als 240 Teilnehmer unterstützt?

    Antwort: Auf der Grundlage der Verkehrswerte ließen sich 600 Benutzer bei 6 CCS und einer Blockierungsrate von 1% unterstützen. Allerdings würde bei einer solchen Benutzerzahl der Signalisierungsverkehr nicht mehr hinreichend unterstützt werden. Außerdem ist es aus Reliability-Gründen nicht ratsam, so viele Benutzer auf einer einzelnen Baugruppe zu konfigurieren.

15) **Frage:** Die für HFA dokumentierten Default-Werte für das TOS-Byte, d.h. die vorgegebenen DiffServ CodePoints (DSCP) bewirken zusammen mit der Standardeinstellung populärer Router-Hersteller genau das Gegenteil dessen, was beabsichtigt ist. Die von uns als hochprior gekennzeichneten Pakete werden vom Router bevorzugt weggeworfen. Was soll der Unsinn?

    Anwort: Die für HFA verwendeten Default-Werte stammen aus einem Firmen-internen Standard der in allen HG 35xx Gateways umgesetzt wurde. Das Interoperabilitätsproblem ist mittlerweile bekannt - und der Hausstandard soll demnächst geändert werden. Die Default-Werte können aber jederzeit verändert und an die tatsächlichen Gegebenheiten im Kundennetz angepasst werden.

16) **Frage:** Unterstützt HFA VLANs?

    Anwort: Ja, aber nur zusammen mit Priority-Tagging. Tagging nach IEEE 802.1 p/q wurde für HFA eingeführt um Priority-Tagging zu unterstützen. Wird Tagging eingeschaltet, so werden immer die fest vorgegebenen Priority-Bits der unterschiedlichen Verkehrsarten gesetzt. Ist Tagging aktiv, kann zusätzlich die VLAN-ID eingestellt werden (Default-Wert ist Null). Was nicht unterstützt wird ist VLAN-ID ohne gesetzte Priority-Bits.

17) **Frage:** Unterstützt HFA Subnetting (RFC 950)?

    Anwort: Ja. Bei der Eingabe der Netzmaske wird überprüft, ob der Block der gesetzten Einsen mindestens so lange ist, wie es für die Klasse der Adresse erforderlich ist, d.h. 8 Einsen für Klasse A, 16 für B sowie 24 für C. Ist die Zahl der Einsen größer als für die Klasse erforderlich, ist Subnetting aktiviert.

18) **Frage:** Unterstützt das HG3500 Gateway (STMI2/STM4) ClassLessInterDomainRouting (CIDR), d.h. Subnetting/Supernetting?

    Antwort: Ja.

19) **Frage:** Unterstützt das vHG3500 Gateway (OpenScape 4000 SoftGate) ClassLessInterDomainRouting (CIDR), d.h. Subnetting/Supernetting?

    Antwort: Ja.

9 Mobile HFA Logon

9.1 Leistungsmerkmalbeschreibung

9.1.1 Mobility-Sitzung

Dieses Leistungsmerkmal ist eine Erweiterung des statischen HFA (HiPath Feature Access).

Der Mobile HFA zugrunde liegende Gedanke ist die Nutzung der Eigenschaften (Classmarks, Name, Nummer, Tasten) eines Teilnehmers an anderen Telefonen irgendwo auf der Welt. Ein solcher Anwender wird als „mobiler Teilnehmer“ bezeichnet.

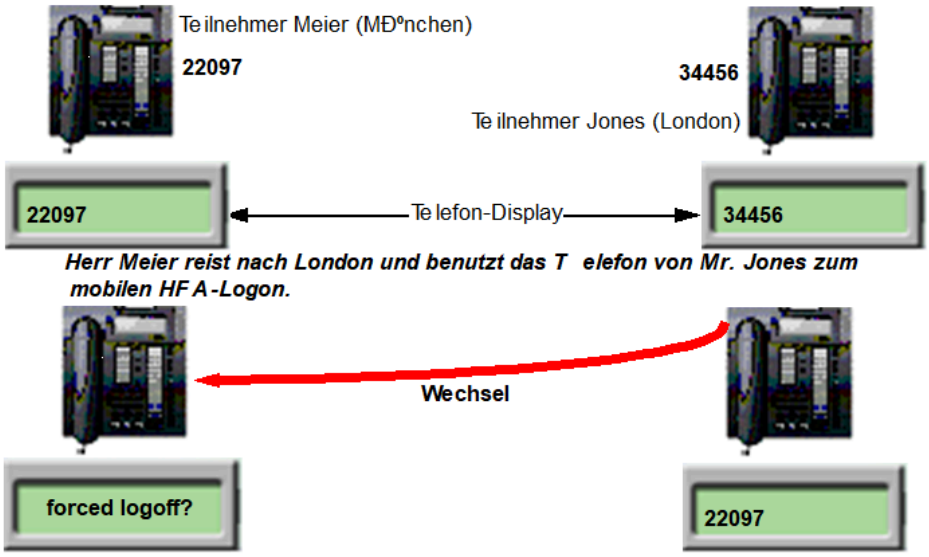
Der mobile Teilnehmer hat ein Telefon in seinem Heimatbüro und reist an einen anderen Ort (z.B. zu einer anderen Niederlassung oder ins Ausland). Dort benutzt er als Besucher ein Telefon („besuchtes“ Telefon). Er gibt eine Kennzahl zur Aktivierung von „Mobile HFA“, seine Heimat-Rufnummer, seine PIN und eventuell ein Passwort ein, um das „besuchte“ Telefon mit denselben Eigenschaften nutzen zu können wie sein Heimat-Telefon.

Bei erfolgreichem Verlauf (ausreichende Classmarks, Telefontypen usw.) wird sein Heimat-Telefon außer Betrieb gesetzt (erzwungene Abmeldung - „forced logoff“). Der mobile Teilnehmer kann das „besuchte“ Telefon nun in derselben Weise nutzen wie sein Heimat-Telefon. So werden beispielsweise Name und Rufnummer des Heimat-Telefons angezeigt, wenn der mobile Teilnehmer einen Anruf tätigt bzw. empfängt, die Classmarks des Heimat-Telefons haben Gültigkeit usw.

Beendet der Besucher Mobile HFA durch Logoff, werden die ursprünglichen Eigenschaften des Heimat- und des „besuchten“ Telefons wiederhergestellt. Der Zeitraum zwischen der An- und Abmeldung von Mobile HFA an einem „besuchten“ Telefon wird als „Mobility-Sitzung“ bezeichnet.

Der Besitzer des „besuchten“ Telefons ist während dieser Zeit nicht erreichbar. Alle Anrufe beim Besitzer des „besuchten“ Telefons werden an ein CFNR-Ziel umgeleitet.

Aktivieren des Leistungsmerkmals



Aktivieren des Leistungsmerkmals

Alle Anrufe für 34456 werden nun an die zentrale CFNR (Anrufumleitung bei Nichtmelden) für Teilnehmer Jones (Administration durch AMO ZIEL) weitergeleitet.

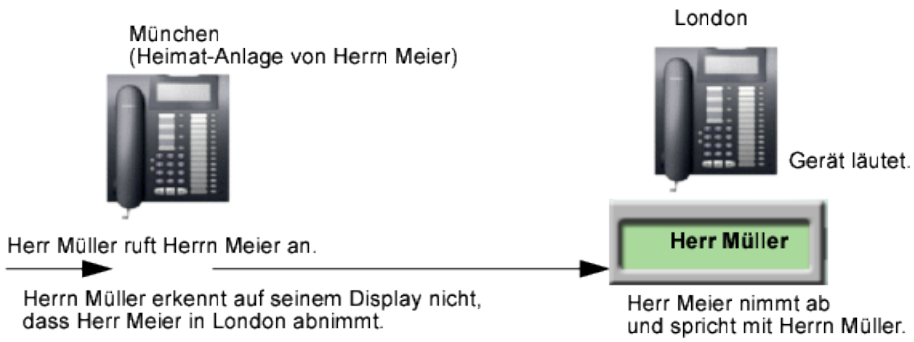
Vor seiner Rückreise nach München nimmt Herr Meier das mobile Logoff in London (per KZP oder Menü) vor. Falls er es vergisst, kann er dies auch von München aus nachholen. In beiden Fällen werden die beiden Telefon binnen Sekunden in ihren Originalzustand zurückversetzt.

Währen das Londoner Telefon in mobiler Benutzung ist, kann niemand den Telefonapparat von Herrn Meier in München benutzen.

Für Mr. Jones bestimmte Anrufe läuten nicht an dessen Gerät.

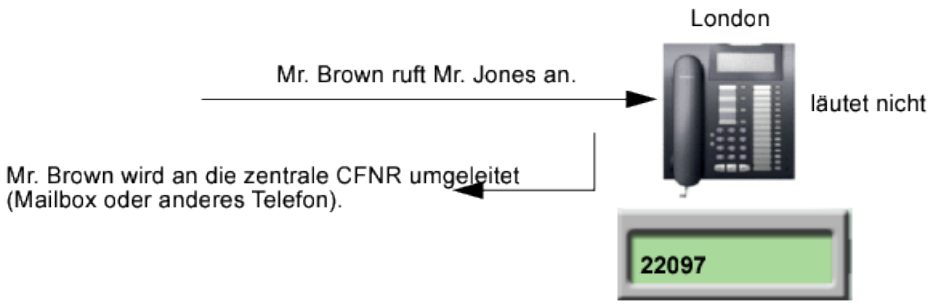
Das Leistungsmerkmal kann mit Passwörtern, Funktionssperre und leitungsabhängigen Classmarks vor Missbrauch geschützt werden.

Anruf bei mobilem Teilnehmer



Anruf bei mobilem Teilnehmer

Anruf bei „besuchtem“ Telefon



Anruf bei „besuchtem“ Telefon

9.1.2 Shared Desk Area - gemeinsamer Arbeitsbereich

Das Leistungsmerkmal „Mobile HFA Logon“ ermöglicht die Nutzung eines gemeinsamen Arbeitsbereichs („Shared Desk Area“). Der gemeinsame Arbeitsbereich ist ein Szenario, in dem Anwendern Telefone dynamisch zugewiesen werden können. Bei einer Anlage werden eine Anzahl von Anwendern ohne feste Telefone und Telefone mit virtuellen Teilnehmern eingerichtet. Die Telefone werden über verschiedene Räume oder Gebäude verteilt. Die Anzahl der Telefone kann deutlich unter der Anzahl der potenziellen Anwender liegen.

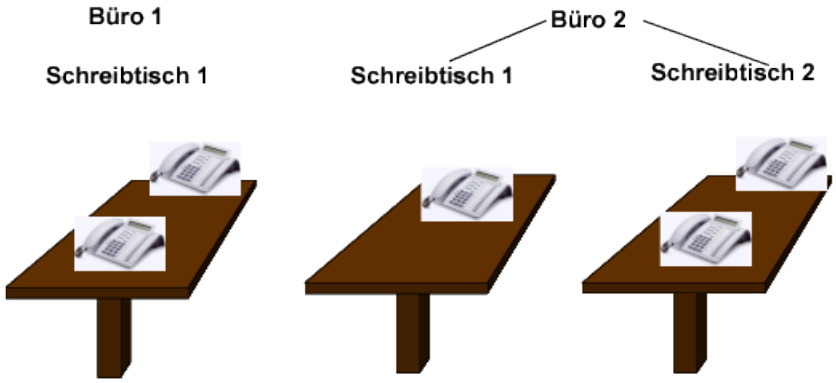
Die tatsächlichen Anwender dürfen jedes Telefon des Arbeitsbereichs („Desk Area“) nutzen. Ein Endgerät kann nacheinander von verschiedenen Teilnehmern benutzt werden.

Zum Beispiel kann Anwender Jones ein Telefon ab 9:00 Uhr benutzen. Anwender Brown kann dasselbe Telefon nutzen, nachdem Mr. Jones das Büro verlassen hat. Beide Anwender können dasselbe Telefon mit den ihnen zugewiesenen Eigenschaften verwenden.

Mr. Jones meldet sich an einem Telefon mit seiner Telefonnummer und seinem Passwort an. Nach erfolgreicher Anmeldung kann er als „Mr. Jones“ telefonieren.

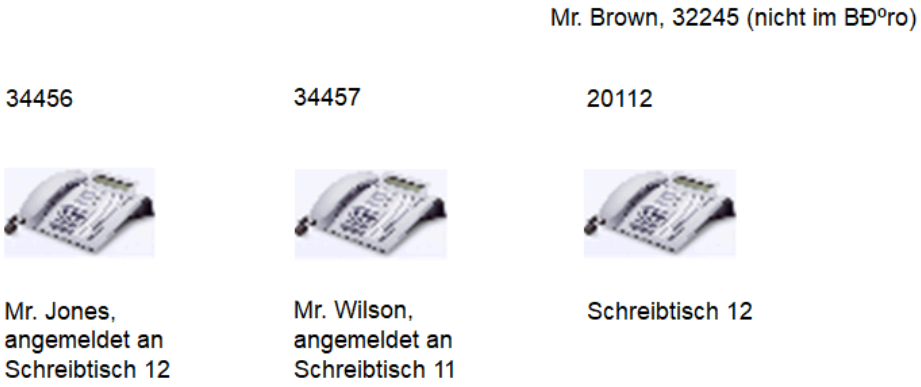
Seine Sitzung endet, wenn er sich abmeldet oder wenn sich ein anderer Anwender (Mr. Brown) an diesem Telefon anmeldet.

Nach einer Abmeldung initialisiert sich das Telefon wie konfiguriert. Aus diesem Grund muss jedes physikalische Telefon mit einer virtuellen Rufnummer („Dummy“-Rufnummer) eingerichtet werden.



Meldet ein Anwender seine Sitzung ab bzw. wird diese beendet, indem sich ein anderer Anwender an dem Gerät anmeldet, wechselt der erste Anwender in den Status „besucht“. Das bedeutet, dass alle für ihn bestimmten Anrufe an das zentrale CFNR-Ziel umgeleitet werden.

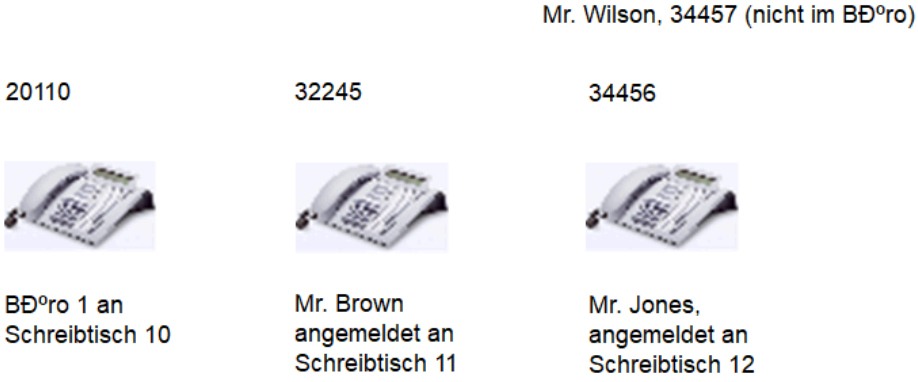
Im folgenden Beispiel verweisen mit „3“ beginnende Telefonnummern auf Anwender der in der Anlage konfigurierten gemeinsamen Arbeitsbereiche (Shared Desk Areas). Die „Dummy“-Telefone haben „Namen“ wie „Büro 1, Schreibtisch 12“ und entsprechende, mit „2“ beginnende Telefonnummern: 20112 (=Büro 1, Schreibtisch 12).



Mr. Jones und Mr. Wilson sind an den Telefonen an Schreibtisch 10 und Schreibtisch 11 angemeldet.

Anrufe bei ...		
Name	Anzahl	Aktion
Mr. Brown	32245	werden umgeleitet an zentrale CFNR
Mr. Jones	34456	läuten an Schreibtischtelefon 10
Mr. Wilson	34457	läuten an Schreibtischtelefon 11
Schreibtisch 10	20110	werden umgeleitet an zentrale CFNR
Schreibtisch 11	20111	werden umgeleitet an zentrale CFNR
Schreibtisch 12	20112	läuten an Schreibtischtelefon 12

Mr. Brown meldet sich jetzt an Schreibtischtelefon 11 an (beendet Mr. Wilsons Sitzung). Mr. Jones meldet sich ab und meldet sich an Schreibtisch 12 an.



Anrufe bei ...		
Name	Nummer	Aktion
Mr. Brown	32245	läuten an Schreibtischtelefon 11
Mr. Jones	34456	läuten an Schreibtischtelefon 12
Mr. Wilson	34457	werden umgeleitet an zentrale CFNR
Schreibtisch 10	20110	läuten an Schreibtischtelefon 10
Schreibtisch 11	20111	werden umgeleitet an zentrale CFNR
Schreibtisch 12	20112	werden umgeleitet an zentrale CFNR

9.2 Benutzeroberfläche

Wichtig: Die Vorgehensweisen zur Aktivierung und Deaktivierung sind bei Mobility und Shared Desk Area identisch.

Der Anwender hat zwei Möglichkeiten zur Aktivierung von Mobile HFA Logon:

- per KZP (Kennzahlpunkt) und
- per Servicemenü.

Eine dritte Möglichkeit steht nur der Administration zur Verfügung: Die Verwaltung über AMO ACTDA.

9.2.1 Aktivierung/Deaktivierung per KZP

Die Aktivierung/Deaktivierung des Leistungsmerkmals per KZP erfolgt am „besuchten“ Telefon.

9.2.1.1 HFA-Logon

Eingabe des KZP für „Mobile HFA Logon“.

Dann wird der Anwender aufgefordert, seine Heimat-Rufnummer (mit # abschließen) und seine PIN (mit # abschließen) einzugeben.

Die Display-Meldung lautet „MOBILE HFA LOGON STARTED“. Verlaufen alle Checks positiv, erhält der Anwender dieselben Anzeigen am Display wie an seinem Heimat-Telefon, so als ob er seinen üblichen Arbeitsplatz nicht verlassen hätte.

Wenn die Checks nicht positiv verlaufen (falsches Passwort, falsche Heimat-Rufnummer, fehlende Merkmale...), erscheint eine ablehnende Meldung auf dem Display.

- Mobility-Sitzung (physikalische Erweiterung des Heimat-Telefons)
- Das Display am Heimat-Telefon zeigt „Forced Logon - Cancel Mobility?“ an und kann nicht benutzt werden, auch nicht für Notrufe. Erst nach Beendigung der Mobility-Funktion ist es wieder betriebsbereit. Diese Aktion ist jedoch passwortgeschützt (Telefonpasswort - nicht das Mobility-Passwort).
- Gemeinsamer Arbeitsbereich (kein physikalisches Heimat-Telefon)
- Wenn das Heimat-Telefon nicht physikalisch existiert, kann am Heimat-Telefon nichts angezeigt werden. Eine Beendigung vom Heimat-Telefon aus ist nicht möglich.

9.2.1.2 HFA-Logoff

Zur Abmeldung wird das KZP für Logoff eingegeben.

Die Display-Meldung lautet „MOBILE HFA LOGOFF STARTED ... “.

Bald darauf erscheint die ursprüngliche Anzeige am „besuchten“ Telefon, und an der Heimat-Anlage wird das Heimat-Telefon des Anwenders wieder initialisiert.

9.2.2 Aktivierung über Menü

Die Menüpunkte „MOBILE HFA LOGON/LOGOFF“ für Mobile HFA sind im Servicemenü enthalten. Der Anwender ruft das Servicemenü am „besuchten“ Telefon auf und steuert die Menüpunkte zum mobilen HFA-Logon/-Logoff mit den Tasten „<“ und „>“ an.

Das Leistungsmerkmal Mobile HFA kann auch über das Servicemenü und die Ziffern „8“ (mobile HFA logon) bzw. „9“ (mobile HFA logoff) gesteuert werden.

Nach Bestätigung des Logon wird der Anwender zur Eingabe seiner Heimat-Rufnummer und PIN (siehe weiter oben) aufgefordert.

Nach der Bestätigung einer Aktion ist das Verhalten dasselbe wie bei der KZP-Aktivierung.

9.2.3 Aktivierung mit AMO ACTDA

AMO ACTDA erfordert drei Parameter: Rufnummer des „besuchten“ Telefons, Heimat-Rufnummer und PIN.

Die Aktivierung mit AMO ACTDA kann nur an der Anlage erfolgen, wo das „besuchte“ Telefon eingerichtet ist.

Die AMO zeigt eine Meldung an, wenn das Logon erfolgreich bzw. erfolglos verläuft (Letzteres mit Begründung).

9.3 Voraussetzungen

Dieses Leistungsmerkmal wird durch verschiedene Flags in der Anlage des „besuchten“ Telefons und der Anlage des Heimat-Telefons eingeschränkt.

Mögliche Endgeräte für Mobile HFA

Das Leistungsmerkmal funktioniert nicht an allen Telefontypen. Die Firmware beider Telefone muss Mobile HFA unterstützen. Derzeit verfügen die folgenden Telefone über diese Funktionalität:

- optiPoint 410 (außer 410 entry),
- optiPoint 420 (Tasten mit Electronic-Labeling-Funktion)
- optiPoint 600
- OpenStage 20/20G/40/40G/60/60G/80/80G

Wichtig: Wird das OpenStage-Endgerät in Verbindung mit einem optiClient verwendet, muss im optiClient der Endgerätetyp „optiPoint 420 advance“ eingestellt werden. Für weitere Informationen siehe Abschnitt 4.1.1, „OpenStage-Endgerät in Verbindung mit einem optiClient“.

AMO Voraussetzungen

- Das AMO FEASU-Bit **MOBHFA** muss auf beiden Seiten gesetzt werden.
- Das Heimat-Telefon muss in AMO SDAT das Leitungsmerkmal **MHFAHOME** haben.
- Das „besuchte“ Telefon muss in AMO SDAT das Leitungsmerkmal **MHFATBV** („to be visited“) haben.
- Für das Heimat-Telefon muss eine PIN mit dem COPIN-Merkmal „**MOBIL**“ zugewiesen werden.

Hardware

Für Mobile HFA geeignete Telefone werden an die Common Gateway-Baugruppe (STMI2/4-Baugruppe) angeschlossen.

Paswort-Einstellungen

Für den mobilen Teilnehmer sollte ein Mobile-Passwort hinzugefügt werden. Dieses Passwort verhindert, dass die erzwungene Abmeldung („forced logoff“) am Heimat-Anschluss ohne Passwort beendet werden kann.

- optiPoint-Endgeräte

- Das Passwort wird im Konfigurationsmenü des Endgeräts im Untermenü „02=System“ zugewiesen.
- OpenStage-Endgeräte
- Das Passwort kann entweder über das WBM des Endgeätes gesetzt werden (**Administrator Pages > User mobility > Cancel mobility passowrd**) oder direkt am Endgerät selber über das Menü **Admin > Passwort > Mobility**.

9.4 Service Informationen

9.4.1 Mobile HFA in Verbindung mit anderen Leistungsmerkmalen

9.4.1.1 OpenStage-Endgerät in Verbindung mit einem optiClient

Allgemeine Hinweise zum Konfigurieren eines optiClient in Verbindung mit einem openStage-Telefon

- Das OpenStage Typ „nn“ muss mit der passenden Standardtastenbelegung „openStage nn“ konfiguriert werden.
- Die Tastenbelegung eines OpenStage-Telefons (AMO TAPRO) darf nicht geändert werden, während der optiClient aktiv ist.
- Die vom Teilnehmer vorgenommenen persönlichen Tasteneinstellungen dürfen für die optiClient/openStage-Kombination nicht aktiviert werden.
- Wenn der Benutzer zuletzt die Kombination optiClient/optiPoint verwendete, muss er über die neue Tastenbelegung informiert werden, die in der optiClient-Anwendung eingesehen werden kann. Der Grund hierfür sind die festgelegten Tastenfunktionen der OpenStage-Telefone.
- Bei Nichtbeachtung der genannten Einschränkungen kann die korrekte Tastenbelegung nach einem Wechsel zwischen OpenStage und optiClient nicht gewährleistet werden. Dem kann nur durch Löschen und erneutes Konfigurieren der kompletten Verbindung abgeholfen werden.
- Diese Vorgehensweise gilt auch für den so genannten Tandem-Modus (optiClient verwendet dieselbe Nummer wie die Heimatstation. In diesem Fall ist die Heimatstation das OpenStage.)

Konfiguration einer neuen optiClient/OpenStage-Verbindung

- Neue Konfiguration des openStage-Telefons mit der korrekten Standardtastenbelegung beim Konfigurieren des optiClient (OPTIIP&API).
- In der optiClient-Anwendung muss das Gerät „optipoint 420 advance“ ausgewählt werden.

Austausch einer vorhandenen optiClient/optiPoint-Konfiguration gegen optiClient/OpenStage

1) Neugenerierung der Benutzerdaten
2) Löschen der kompletten Verbindung

Wichtig: Das Löschen ist notwendig, da derzeit keine andere Möglichkeit besteht, die so genannte Schattentabelle

für Tastenzuordnungen zu löschen. Wenn die Verbindung nicht ordnungsgemäß gelöscht wird, kann die korrekte Tastenbelegung weder auf dem optiClient noch auf dem OpenStage gewährleistet werden. Ob die Schattentabelle gelöscht werden muss, hängt vom Verlauf der bisherigen Verbindung ab (z.B. davon, ob andere Telefontypen angeschlossen wurden).

3) Nun können Sie die Telefone austauschen und anschließen das OpenStage wie in Allgemeine Hinweise zum Konfigurieren eines optiClient in Verbindung mit einem openStage-Telefon beschrieben konfigurieren (oder umgekehrt).

Wichtig: Weitere Informationen finden Sie in der readme-Datei des optiClient unter „âMobile Registrationâ mit OpenStage Hardware-Endgeräten“.

9.4.1.2 Leistungsmerkmal „Fangen“ an der „besuchten“ Anlage

Ist das Leistungsmerkmal „Fangen“ an der „besuchten“ Anlage aktiviert (AMO PERSI), führen Anmeldeversuche, die aufgrund der Eingabe eines falschen Passworts fehlschlagen, zu einer entsprechenden Ausgabe am Betriebsterminal der „besuchten“ Anlage.

Die ausgegebene Warnung sieht folgendermaßen aus:

```
F2754 M4 N0063 MC TRACE BPA PIN TRACE 04-02-10 13:25:12
ALARM CLASS:CENTRAL:024
STNO INTERN:3581 PIN:25587
FORMAT:34
```

Klartext: An Anschluss 3581 erfolgte ein Anmeldeversuch mit PIN 25887.

9.4.1.3 Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))

Siehe Dokumentation zum Thema „Signalisierungs- und Sprachverschlüsse-löung (SPE)“.

9.4.2 Einschränkung

Das „Mobile HFA Logon“ Leistungsmerkmal wird vom optiClient nicht unterstützt und muss durch Anmelden mit unterschiedlichen Benutzerprofilen realisiert werden. Anwender, die optiClient mit unterschiedlichen Rufnummern verwenden wollen, müssen mit unterschiedlichen Benutzerprofilen arbeiten.

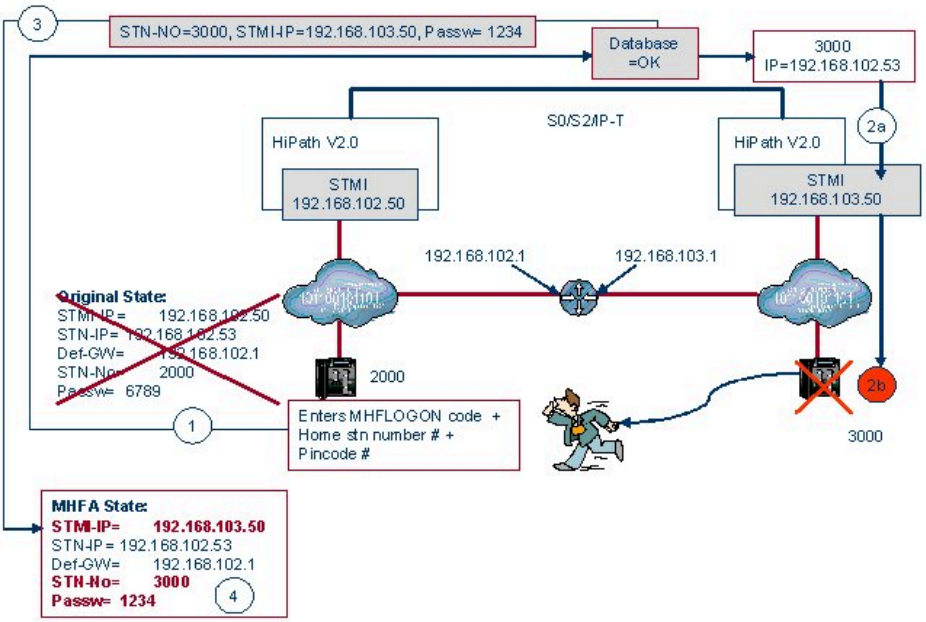
9.4.3 Sprachunterstützung

Das Leistungsmerkmal verwendet die Sprache der Heimat-Anlage. Von der Anlagen-Software gesteuerte Menü- und Anzeigetexte werden also in der Sprache der Anlage angezeigt („Bitte wählen“, „Passwort eingeben“ usw.).

Von der Firmware des Telefons gesteuerte Meldungen (direkt, nicht anlagenabhängig) erscheinen nur auf Englisch („Cancel logoff“, „logging on to home...“).

Ist in der Anlage eine andere Sprache als Englisch eingestellt, werden die Texte in zwei Sprachen angezeigt.

9.4.4 Funktionsabläufe bei Logon



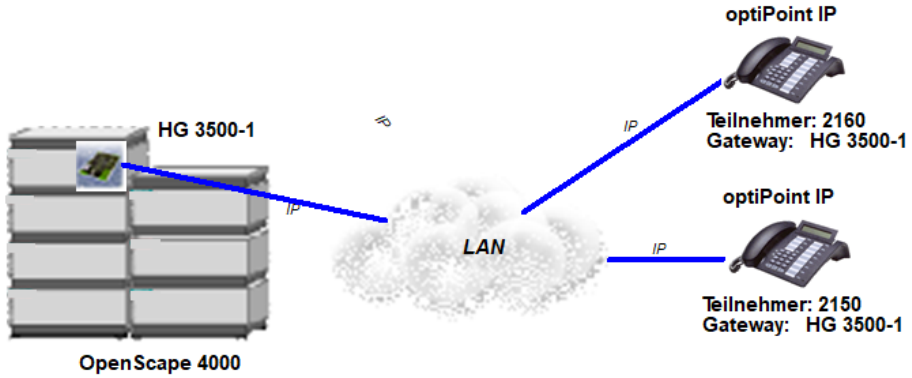
9.5 Generierung

Wichtig: Wichtige Wartezeit Nachdem alle AM-Befehle zur Installation von Mobile HFA ausgeführt wurden, müssen 3 Minuten bis zum ersten mobilen HFA-Logon vergehen. HFA-Baugruppen und IP-Telefone benötigen zur Selbstinitialisierung bis zu 3 Minuten. Ein HFA-Logon vor erfolgreichem Ablauf der Selbstinitialisierung wird möglicherweise fehlschlagen.

- Vorbereitung
  - Vorbereitung: Speicherreservierung für Baugruppen und Teilnehmer
  - Einrichten der Baugruppe
  - Einrichtung der Teilnehmer
  - Vergabe von Berechtigungen und Classmarks für Leistungsmerkmal, Teilnehmer ...
  - Einrichtung der KZP
  - Einrichtung der Anrufumleitungsziele
  - Sonstiges

9.5.1 Beispiel 1: Zwei HFA-Teilnehmer auf demselben Host

Teilnehmer 2150 soll die Berechtigung erhalten, sich am Endgerät von Teilnehmer 2160 zu identifizieren. Teilnehmer 2160 soll keine Möglichkeit zur Identifikation erhalten. Für 2160 ankommende Rufe sollen an Anschluss 4444 umgeleitet werden, wenn 2150 das Telefon von 2160 benutzt.




```
EINR-DIMSU:TYP=SYSTEM,CGW=1;
EINR-BFDAT:FCTBLK=1,FUNCTION=HG3530,BGBKAN=BKAN60;
AENDERN-BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3530,ANZSATZ=30,ANZBKAN=30;
/* Konfiguration von 30 HG 3530-Sätzen mit 30 B-Kanälen
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA;
EINR-BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=85,SACHNR="Q2316-
X",FCTID=1,LWVAR="0",FCTBLK=1,ALARMNR=0;
EINR-CGWB:LTU=3,EBT=85,SMODE=NORMAL,IPADR=192.168.1.85,NETMASK=255.255.255.0;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=85;
EINR-SBCSU:TLNNU=2150,ART=OPTI,ANSCHL=IP2,LAGE=1-3-85-0,GERKON=OPTIIP, ...;

EINR-SBCSU:TLNNU=2160,ART=OPTI,ANSCHL=IP2,LAGE=1-3-85-1,GERKON=OPTIIP, ...
EINR-WABE:RNR=*95,KZP=MHFALGON,PRUEF=N;

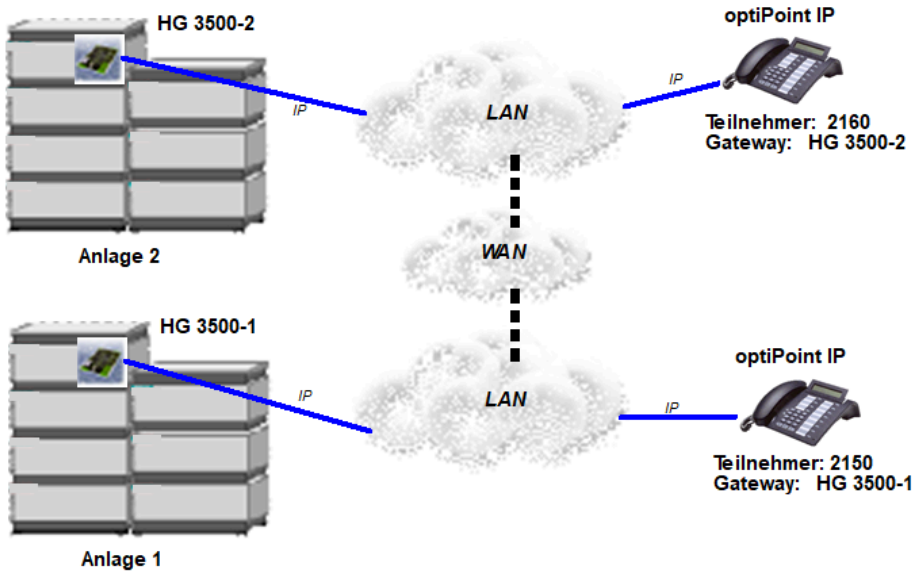
EINR-WABE:RNR=*96,KZP=MHFALGOF,PRUEF=N;
EINR-PERSI:TYP=TLN,RUFNU=2150,NAME="STEFAN*",PIN1="258861",PININDIV=J;

AEND-PERSI:TYP=COPIN,COPIN=1,PINTYP=MOBIL, ...;
AEND-SDAT:TLNNU=2150,TYP=MERKMAL,EMERK= MHFAHOME;

AEND-SDAT:TLNNU=2160,TYP=MERKMAL,EMERK=MHFATBV;
AEND-FEASU:TYP=FREI,LM=MOBHFA;
EINR-ZIEL:TYP=AUL,QLRUFNU=2160,SI=VOICE,ZLRUFNU=4444,UART=CFNR,KART=G
EN,AULVAR=SYSTEM;
REGENERIEREN-RICHT;
```

9.5.2 Beispiel 2: Zwei HFA-Teilnehmer an verschiedenen Anlagen

Die Teilnehmer 2150 und 2160 sollen die Berechtigung erhalten, sich am Endgerät des anderen Teilnehmers zu identifizieren. Anrufe für Teilnehmer 2160 sollen an seine Mobilrufnummer 017544444444 umgeleitet werden, wenn sein Telefon für „Mobile HFA Logon“ genutzt wird. Anrufe für Teilnehmer 2150 sollen an den Anschluss 4444 umgeleitet werden, wenn sein Telefon für „Mobile HFA Logon“ genutzt wird.



Generierung der Anlage 1:

```
EINR-DIMSU:TYP=SYSTEM,CGW=1;

EINR-BFDAT:FCTBLK=1,FUNCTION=HG3530,BGBKAN=BKAN60;
AEND-BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3530,ANZSATZ=30,ANZBKAN=30;
/* Konfiguration von 30 HG 3530-Sätzen mit 30 B-Kanälen
AEND-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA;
EINR-BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=85,SACHNR="Q2316-
X",FCTID=1,LWVAR="0",FCTBLK=1,ALARMNR=0;
EINR-CGWB:LTU=3,EBT=85,SMODE=NORMAL,IPADR=192.168.1.85,NETMASK=255.255.255.0;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=85;
EINR-SBCSU:TLNNU=2150,ART=OPTI,ANSCHL=IP2,LAGE=1-3-85-0,GERKON=OPTIIP, ...;
EINR-WABE:RNR=*95,KZP=MHFALGON,PRUEF=N;

EINR-WABE:RNR=*96,KZP=MHFALGOF,PRUEF=N;
EINR-PERSI:TYP=TLN,RUFNU=2150,NAME="OPTI IP
1*",PIN1="0512",PININDIV=JA;

AEND-PERSI:TYP=COPIN,COPIN=1,PINTYP=MOBIL,....;
AEND-SDAT:TLNNU=2150,TYP=MERKMAL,EMERK= MHFAHOME;

AEND-SDAT:TLNNU=2150,TYP=MERKMAL,EMERK=MHFATBV;
AEND-FEASU:TYP=FREI,LM=MOBHFA;
EINR-
ZIEL:TYP=AUL,QLRUFNU=2150,SI=VOICE,ZLRUFNU=4444,UART=CFNR,KART=GEN,AULVAR=SYSTEM;
REGENERIEREN-RICHT;
```

Generierung der Anlage 2:

```
EINR-DIMSU:TYP=SYSTEM,CGW=1;

EINR-BFDAT:FCTBLK=1,FUNCTION=HG3530,BGBKAN=BKAN60;
AEND-BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3530,ANZSATZ=30,ANZBKAN=30;
/* Konfiguration von 30 HG 3530-Sätzen mit 30 B-Kanälen
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA;
```

```
EINR-BCSU:TYP=IPGW,LTG=1,LTU=3,EBT=85,SACHNR="Q2316-
X",FCTID=1,LWVAR="0",FCTBLK=1,ALARMNR=0;
EINR-CGWB:LTU=3,EBT=85,SMODE=NORMAL,IPADR=192.168.2.97,NETMASK=255.255.255.0;
RESTART-BSSU:ADRART=LAGE,LTU=3,EBT=85;
EINR-SBCSU:TLNNU=2160,ART=OPTI,ANSCHL=IP2,LAGE=1-3-85-0,GERKON=OPTIIP,...;
EINR-WABE:RNR=*95,KZP=MHFALGON,PRUEF=N;

EINR-WABE:RNR=*96,KZP=MHFALGOF,PRUEF=N;
EINR-PERSI:TYP=TLN,RUFNU=2160,NAME="OPTI IP 10*",PIN1="0612",PININDIV=JA;

AEND-PERSI:TYP=COPIN,COPIN=1,PINTYP=MOBIL,....;
AEND-SDAT:TLNNU=2160,TYP=MERKMAL,EMERK= MHFAHOME;

AEND-SDAT:TLNNU=2160,TYP=MERKMAL,EMERK=MHFATBV;
AEND-FEASU:TYP=FREI,LM=MOBHFA;
EINR-
ZIEL:TYP=AUL,QLRUFNU=2160,SI=VOICE,ZLRUFNU=0017544444444,UART=CFNR,KART=GEN,AULVAR=SYSTEM
REGENERIEREN-RICHT;
```

9.5.3 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ACTDA	ABMED=GERFREI	d	Erlaubt das Abmelden nur im Freizustand.
	COND=IDLESTN	e	Allows the logoff only if station is idle.
	ABMED=UNBED	d	Erlaubt das Abmelden in jedem Fall.
	COND=UNCOND	e	Condition for logoff: Unconditional logoff
	ACTION=MLOGON	d	Aktivieren des Leistungsmerkmals: Logon eines Mobile HFA-users
	ACTION=MLOGON	e	Activate the feature: Logon of mobile hfa-user
	ACTION=MLOGOFF	d	Deaktivieren des Leistungsmerkmals: Logoff eines Mobile HFA-users
	ACTION=MLOGOFF	e	Deactivate the feature: Logoff of mobile hfa-user
	BESRNR	d	Rufnummer des besuchten Teilnehmers
	VISSTNO	e	Station number of the visited station
	HEIMPIN	d	PIN des Besuchers
	HOMEPIN	e	PIN of the visitor
	HEIMRNR	d	Heimrufnummer des Besuchers

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	HOMESTNO	e	Home station no. of the visitor
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	BKAN3530	d	Anzahl der B-Kanaele fuer die HG3530 Funktion
	BCHN2430	e	Number of b-channels for HG3530 function
	FCTID	d	Function Id ist immer 1
	FCTID	e	Function id is always set to 1
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index (choose a free function block between 1-20)
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
	LWVAR	e	Loadware variant
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP gateway (common gateway board)
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/or 120 b-channels.
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	Continue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Terminate block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.
	FCTBLK	e	This index describes the function block which should be configured on the CGW board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function.
CGWB	SMODE=NORMAL	d	Standby Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Standby Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Standby Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Standby Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Standby Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Standby Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	Source IP address of common gateway board

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network addresss part but different host address parts (also the Default Router must fulfill this requirement).
DIMSU	CGW	d	Speicherreservierung für eine Common Gateway Baugruppe und Baugruppen bezogene Teilnehmerdaten
	CGW	e	Number common gateway boards
FEASU	LM	d	LM=MOBHFA
	CM	e	CM=MOBHFA
	TYP	d	TYP=FREI Aktivieren des Leistungsmerkmals
	TYPE	e	TYPE=A Activate the feature
PERSI	COPIN	d	Class of PIN
	COPIN	e	Class of PIN
	PIN1	d	PIN (Passowrt für HFA)
	PIN1	e	PIN (password for HFA)
	PINTYP	d	PINTYP=MOBIL COPIN-Typ fuer netzweiten Transfer der COPIN im CorNet Protokoll
	COTYPE	e	COTYPE=MOBILE COPIN type

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	RUFNU	d	Rufnummer des Teilnehmers
	STNO	e	Station number
	TYP=COPIN	d	Mindestens eine COPIN (1-15) muss das Attribut Mobil haben.
	TYPE=COPIN	e	At least one COPIN (1-15) must have the attribute Mobile.
	TYP=TLN	d	Teilnehemr einrichten
	TYPE=STN	e	add a station
SBCSU	ANSCHL=IP2	d	Anschluss-Art der Geräte IP2=Anschluss ueber IP (HFA Gateway Version 2)
	CONN=IP2	e	Device Connection Type IP2=Connection via IP (HFA gateway version 2)
	ART=OPTI	d	Hauptrufnummer des IP-Telefonanschluss einrichten
		e	
	GERKON=OPTIIP	d	Geräte-Konstellation eines Teilnehmers OPTIIP=IP Sprachterminal
	DVCFIG=OPTIIP	e	Device Configuration OPTIIP=Digital IP voice terminal
	IPPASSW	d	passwort fuer ip login prozedur
	IPPASSW	e	Password for IP logon procedure
SDAT	EMERK	d	EMERK=MHFAMOE Merkmal des Heinat-Telefons EMERK=MHFATBV Merkmal des „besuchten“ Telefons
	AATTR	e	AATTR=MHFAMOE HFA home phone of visitor AATTR=MHFATBV mobile HFA phone which can be visited
	TLNNU	d	Teilnehmerrufnummer

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	STNO	e	Station number
	Typ	d	TYP=MERKMAL Teilnehmermerkmale administrieren
	ATTRIBUT	e	TYPE=ATTRIBUT Administrate subscriber attributes (service=voice)
WABE	KZP=MFALGON	d	Kennzahlpunkt für Aktivierung
	DAR=MFALGON	e	Logon by a mobile hfa subscriber
	KZP=MFALGOF	d	Kennzahlpunkt für Deaktivierung
	DAR=MFALGOF	e	Logoff by a mobile hfa subscriber
	PRUEF	d	Prüfumfang
	CHECK	e	Scope of check
	RNR	d	2 Rufnummern für Aktivierung / Deaktivierung (*95/*96)
	CD	e	2 station numbers for activation / deactivation (*95/*96)
	VKS	d	Verkehrssituation (5 = Teilnehmer-Vorwahl)
	CPS	e	Call progress state
	WABE	d	WABE-Gruppe
	DPLN	e	Feature access group
ZAND	APIMAX	d	Maximale Anzahl der gleichzeitig aktiven API Sessions. DB-Initialisierung: 10
	APIMAX	e	Maximum number of allowable active API sessions.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	KENNL	d	Linearisierungs- und Kompandierungskennlinien bei der PCM-Kodierung/Dekodierung. Der eingegebene Wert wird zum einen in die zentralen Anlagendaten übernommen, zum anderen bei eingerichteter LTG auch in die entsprechenden COFI-Daten. Der Wert in den zentralen Anlagendaten ist auch gültig bei der Konfi-guration von NCUI-Baugruppen in IPDA-Shelfs.Es sollte daher nach Konfiguration von IPDA-Shelfs dieser Wert nicht mehr geändert werden!
	CODE	e	Speech coding.The entered value will be issued once to central system data and once for assigned LTG in the according COFI-data. The value in central system data is also valid for configuration of NCUI-boards in IPDA shelfs. Therefore this value should not be changed after configuration of IPDA-shelfs!
	TYP=CIT	d	Konfigurieren von fiktiven Geräten, Einstellungen für API Schnittstelle
	TYPE=CIT	e	Configure virtual stations, settings for API interface
	TYP=CONFC	d	Länderspezifische Einstellung für KENNL, K- oder TDAEMPF. Dieser Zweig gilt nur für kompakte Hardware.
	TYPE=CONFC	e	Selection of country-specific settings for CODE, CONFAT STNAT. This branch is only for compact hardware.
ZIEL	AULVAR=SYSTEM	d	Systemumleitung
	CFVAR=SYSTEM	e	system call forwarding
	KART	d	KART=GEN (alle Anrufe) Kommende Belegungsart des AUL-Zieles
	ITYPE	e	ITYPE=GEN (all calls) incoming seizure of fwd feature
	QLRUFNU	d	Quellenrufnummer
	SRCNO	e	station number of source

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SI=VOICE	d	Service Sprache
	SI=VCE	e	service voice
	TYP=AUL	d	Verbindungstyp Anrufumleitung
	TYPE=FWD	e	Call Forwarding
	UART=CFNR	d	Anrufumlenkung bei nicht melden
	DTYPE=CFNR	e	call forwarding no reply
	ZLRUFNU	d	Zielrufnummer
	DESTNOF	e	destination number for forwarding

10 IP Distributed Architecture (IPDA)

10.1 Leistungsmerkmalbeschreibung IPDA

OpenScape 4000 bietet die Möglichkeit, Access Points über ein IP-Netz zu verteilen. Diese Access Points sind Rahmen, die Standard OpenScape 4000 Anschlussbaugruppen aufnehmen. Die Teilnehmeranschlüsse an den Access Points werden genau so behandelt, als wären sie direkt, wie bisher üblich, an einem OpenScape 4000 System angeschlossen. Auch die Administration der gesamten über IP verteilten Komponenten erfolgt als **ein** System über einen Einstiegspunkt der OpenScape 4000 Anlage.

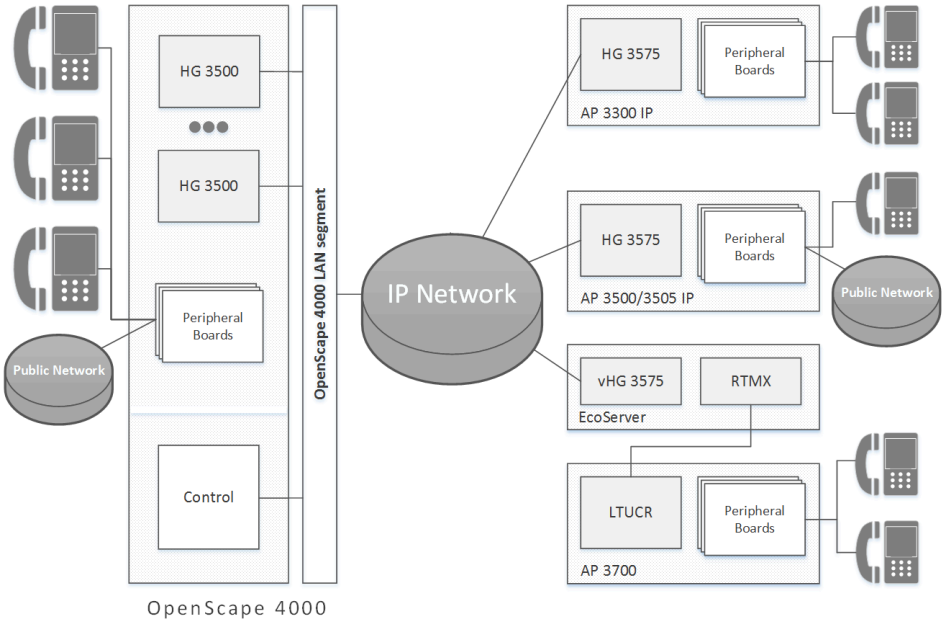


Abbildung 164: Architekturübersicht

Die „IP Distributed Architecture“ besteht aus folgenden Hauptkomponenten:

• OpenScape 4000	Der Kommunikationsserver, welcher auch alle Komponenten der „IP Distributed Architecture“ steuert. Die reichhaltige Menge der vermittlungstechnischen Leistungsmerkmale steht damit auch für die „IP Distributed Architecture“ zur Verfügung.
• HG 3500	Diese IP-Gateway Baugruppe erlaubt Payload-Verbindungen zwischen Teilnehmer-/Amts- und Querverbindungssätzen im zentralen Teil der OpenScape 4000 Anlage und Teilnehmer-/Amts- und Querverbindungssätzen in den verteilten Access Points.
• IP Access Points	Es gibt drei Arten von IP basierten Access Points

• AP 3300 IP	Dieser traditionelle Flexpack Rahmen mit IP Integration bietet 16 Steckplätze für OpenScape 4000 Peripheriebaugruppen
• AP 3500 IP	19"-Shelf (3 Einheiten hoch), das in einem 19"-Rack montiert werden kann, ermöglicht kostengünstige Konfigurationen für kleine Standorte. Als Basisbox bietet es 3 Slots für OpenScape 4000-Peripheriebaugruppen. Die Anzahl der Slots kann über eine AP 3505 IP-Erweiterungsbox (3 Einheiten hoch) auf 7 erhöht werden. Sowohl die AP 3500 IP- als auch die AP 3505 IP-Erweiterungsbox können mit einer redundanten Stromversorgung ausgestattet werden.
Beide Access Point-Typen sind mit HG 3575-Verbindungsmodul ausgestattet, das die Verbindung zur IP-Infrastruktur (10/100BT) herstellt. Die IP-basierten Access Points erlauben den Einsatz der meisten aktuellen und zukünftigen Module, die in klassischen OpenScape 4000-Shelfs betrieben werden können.	
• OpenScape 4000 SoftGate	Das OpenScape 4000 SoftGate ermöglicht kostengünstige Zweigstellen mit zuverlässigen OpenScape 4000 Survivability-Optionen sowie eine einfache IT-Integration in die OpenScape 4000 Lösungs- und Management-Suite. Diese Softwareanwendung bietet vollen HiPath Feature Access (HFA) für IP-Endpunkte, Verbindung zu SIP Service Providern sowie „Native SIP“-Konnektivität für Trunking und Teilnehmer mit grundlegenden Funktionen, das auf einem Standardserver mit Linux basiert. Ein OpenScape 4000 SoftGate-Standort integriert sich hinsichtlich Leistungsmerkmalen und Administration nahtlos wie ein IPDA Access Point (AP 3700 IP) in das Kommunikationssystem und -netzwerk.
• Enterprise Gateway	Dem OpenScape Enterprise Gateway liegt Hardware und Software von OpenScape 4000 zugrunde. Es handelt sich um den Nachfolger der AP 3700-9-Baugruppenrahmen mit HG3575. Alle Funktionen von IP Distributed Architecture (IPDA) sind verfügbar. Weitere Informationen finden Sie unter OpenScape 4000 V8, Enterprise Gateway, Servicedokumentation.
• OpenScape 4000 EcoServer	Enterprise GW-Bereitstellung mit optionaler APE (Survivable Enterprise GW) installiert
• AP 3700 IP	19"-Shelf (10 Einheiten hoch), das in einem 19" -Rack montiert werden kann, verfügt über neun Slots für OpenScape 4000-Peripheriebaugruppen. Der Rahmen wird mit drei PSU-Modulen geliefert, die in einer 2+1-Redundanzkonfiguration betrieben werden.

• LTUCR-Steuerungsbaugruppe	Die LTUCR-Baugruppe (Line Trunk Unit Control Replacement) ist die Schnittstelle zwischen den zentralen und peripheren Einheiten der Anlage. Sie wählt die Signale der jeweils aktiven Steuerung aus und gibt sie an die entsprechenden Baugruppen im LTU-Shelf weiter. Die LTUCR empfängt auch die Signale der Peripheriebaugruppen und leitet sie an die zentrale Steuerung weiter.

Die Baugruppen HG 3500 und HG 3575 haben jeweils einen Ethernet-Anschluss vom Typ 10/100BT zur Verbindung mit dem IP Netz (Technische Daten-LAN-Schnittstelle).

10.1.1 Skalierbare Erhöhung der Anlagenkapazität

OpenScape 4000 unterstützt bis zu 83 über IP verbundene Access Points (AP 3300 IP, AP 3500/3505 IP oder AP 3700 IP) zusätzlich zu den bis zu 15 direkt angeschalteten Rahmen (AP 3300 bzw. AP 3700).

Dadurch kann die maximale Anzahl von digitalen Teilnehmersätzen in einem System auf 12000 erhöht werden.

10.1.2 Verteilte Durchschaltung

Mit OpenScape 4000 beschränkt sich die Durchschaltung der Payload (B-Kanäle) nicht auf das zentrale Koppelfeld

- Gespräche innerhalb IP basierter Access Points werden direkt und folglich ohne Laufzeit im IP-Netz, in einem lokalen TDM Koppelfeld durchgeschaltet. Das Koppelfeld auf der HG 3575 Baugruppe hat eine Kapazität von 256 Kanälen.
- Gespräche zwischen unterschiedlichen IP basierten Access Points werden im IP-Netz durchgeschaltet.
- Gespräche, die über IP basierte Access Points hinausgehen, werden sowohl im IP-Netz, als auch in der zentralen OpenScape 4000 Anlage durchgeschaltet.

10.1.3 Zeitsynchronisation

Für viele Funktionen der OpenScape 4000 ist eine exakte Uhrzeit erforderlich (Gebührenerfassung, uhrzeitabhängige Wege, Nachtschaltung, etc.). Alle Uhren im System (bis zu 84) müssen synchron laufen.

Es gibt zwei Möglichkeiten, die Zeitsynchronisation durchzuführen:

1) Im IP-Netz steht ein Zeit-Server zur Verfügung, der die Zeitsynchronisation aller Prozessoren der OpenScape 4000 (Host System und alle Survivability Units) mittels Network Time Protocol unterstützt.

2) Im IP-Netz steht **kein** Zeit-Server zur Verfügung. Die OpenScape 4000 Plattform stellt dann ihre lokale Uhrzeit zur Synchronisation aller Survivability Units über das Netzwerk zur Verfügung.

Mehr Informationen zur Einstellung von Datum und Zeit und zum Thema „Zeitsynchronisation“ finden Sie in der Dokumentation **OpenScape 4000, Installation, Konfiguration und Migration, Installationsanleitung**.

10.1.4 Rufszenarien

Zum besseren Verständnis der vermittlungstechnischen Abläufe und ihrer Verteilung auf die Komponenten der IP Distributed Architecture werden im Folgenden ein paar typische Rufszenarien näher betrachtet.

10.1.4.1 Access Point interner Ruf

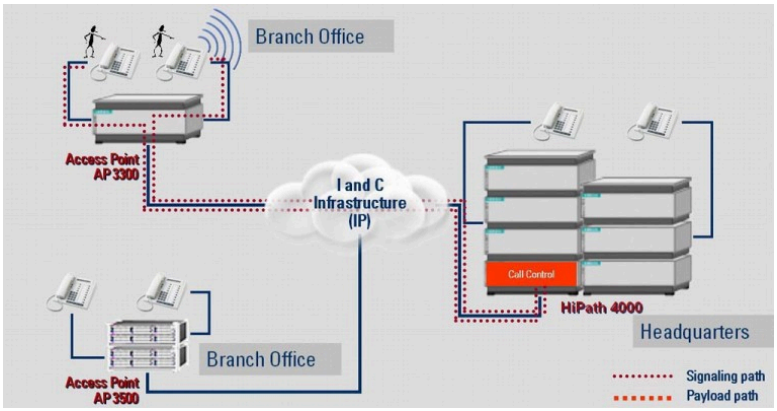


Abbildung 165: Signalisierung bei Access Point internem Ruf

Die Signalisierung von und zu den beteiligten Telefonen geht immer über das IP-Netz zur Vermittlungstechnik in der OpenScape 4000 Zentrale und von dort aus zurück.

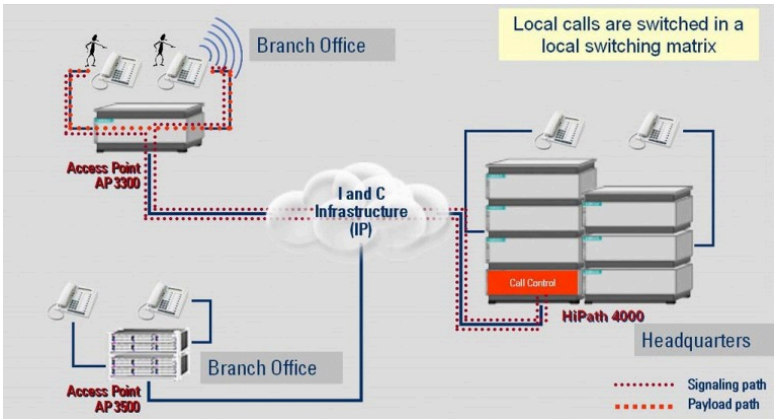


Abbildung 166: Sprachverbindung (Payload) bei Access Point internem Ruf

Die zentrale Vermittlungstechnik baut die Sprachverbindung auf und stellt alle Leistungsmerkmale bereit. Die Sprachverbindung wird in diesem Fall innerhalb des Access Points im TDM-basierten Koppelfeld der HG 3575 Baugruppe durchgeschaltet. Es wird dadurch keine Last im IP-Netz erzeugt und kein Kanal der Transportkapazität aus dem Access Point in das IP-Netz belegt.

10.1.4.2 Ruf zwischen 2 Access Points

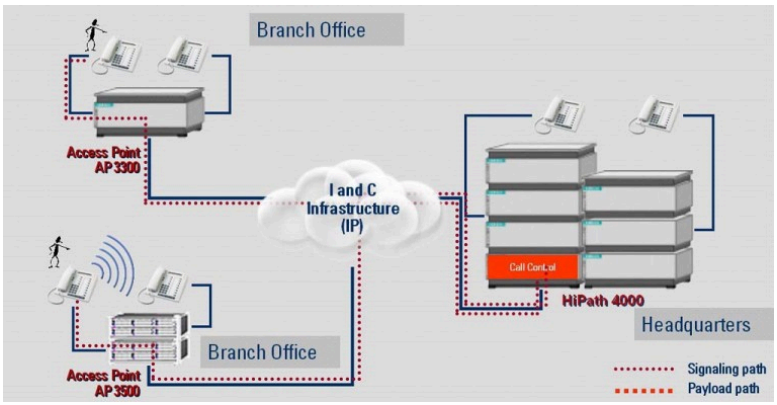


Abbildung 167: Signalisierung bei Ruf Access Point <-> Access Point

Die Signalisierung von und zu den beteiligten Telefonen geht immer über das IP-Netz zur Vermittlungstechnik in der OpenScape 4000 Zentrale und von dort aus zurück.

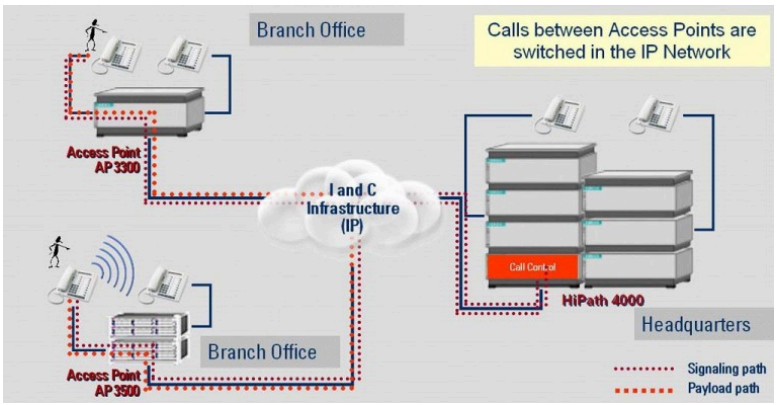


Abbildung 168: Sprachverbindung (Payload) bei Ruf Access Point <-> Access Point

Die zentrale Vermittlungstechnik baut die Sprachverbindung auf und stellt alle Leistungsmerkmale bereit. Die Sprachverbindung zwischen den beiden Access Points wird in diesem Fall mit Hilfe der HG 3575 Baugruppen im IP-Netz durchgeschaltet. Bei beiden Access Points wird je 1 Kanal der verfügbaren Transportkapazität in das IP-Netz belegt.

10.1.4.3 Ruf zwischen Access Point und Zentralsystem

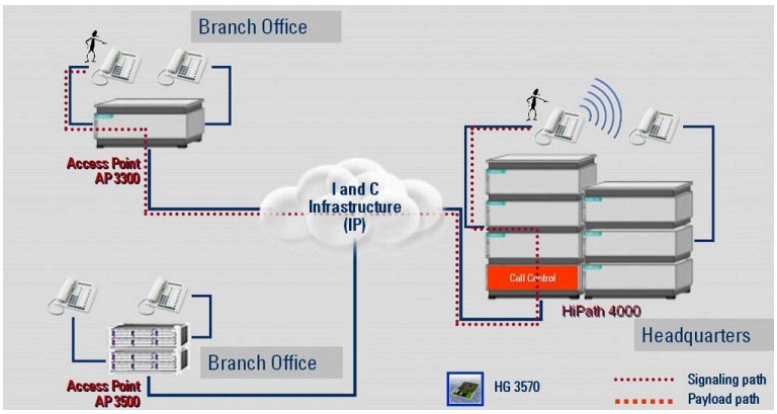


Abbildung 169: Signalisierung bei Ruf Access Point <-> Zentrale

Die Signalisierung von und zu dem beteiligten Telefon im Access Point geht über das IP-Netz zur Vermittlungstechnik in der OpenScape 4000 Zentrale und von dort aus zurück.

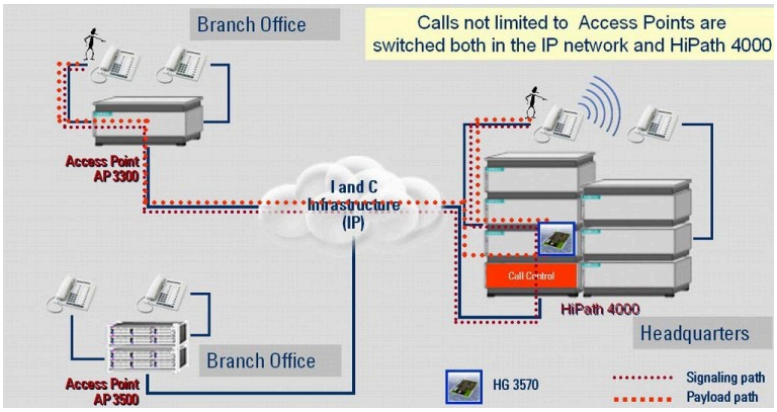


Abbildung 170: Sprachverbindung (Payload) bei Ruf Access Point <-> Zentrale

Die zentrale Vermittlungstechnik baut die Sprachverbindung auf und stellt alle Leistungsmerkmale bereit. Die Sprachverbindung aus dem Access Points wird mit Hilfe der HG 3575 Baugruppe in das IP-Netz geschaltet. Die HG 3500 Baugruppe arbeitet als Gateway und setzt den IP-Datenstrom wieder in einen für die Zentrale verarbeitbaren PCM Datenstrom um. Dieser wird innerhalb der Zentrale an den dort angeschlossenen Teilnehmer vermittelt. Das Gespräch wird also sowohl im IP-Netz als auch im OpenScape 4000 Zentralsystem durchgeschaltet. Sowohl beim Access Point, als auch bei der Gateway-Baugruppe wird je 1 Kanal der verfügbaren Transportkapazität in das IP-Netz belegt.

10.1.4.4 Amtszugang / Vernetzung

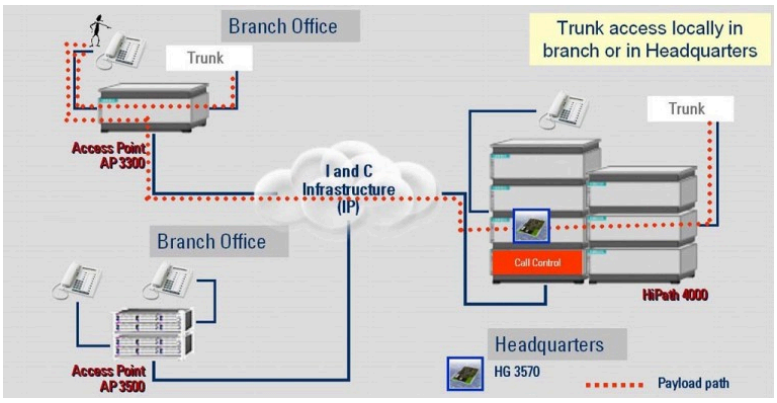


Abbildung 171: Amtszugang / Vernetzung

In einem Access Point können auch lokale Amtszugänge eingerichtet werden. Die Least Cost Routing Funktion der OpenScape 4000 entscheidet in Abhängigkeit vom Standort des Teilnehmers, welcher Amtszugang verwendet werden soll.

10.1.5 Survivability für Signalisierung und Payload

Im Basisausbau (ohne die Survivability Leistungsmerkmale) ist die Funktion einer IPDA-Installation völlig abhängig von der Verfügbarkeit und Zuverlässigkeit der genutzten LAN/WAN-Infrastruktur. Der Ausfall der IP-Anbindung eines Access Points führt zu dessen Ausfall.

Ein Totalausfall der IP-Infrastruktur führt zum Ausfall aller Access Points. Nur die Funktion der Zentralanlage und ihrer „klassisch“ angebundenen Peripherie bleibt erhalten.

Survivability für Signalisierung und Payload stellt sicher, dass OpenScape 4000 auch im verteilten Einsatz höchste Verfügbarkeit bietet. Das öffentliche Telefonnetz/ eine alternative LAN-Verbindung (im Falle von Signaling Survivability) kann als Ausweichweg genutzt werden, falls das IP-Netz ausfällt oder vorübergehend nicht die nötige Qualität für Sprachübertragung bietet.

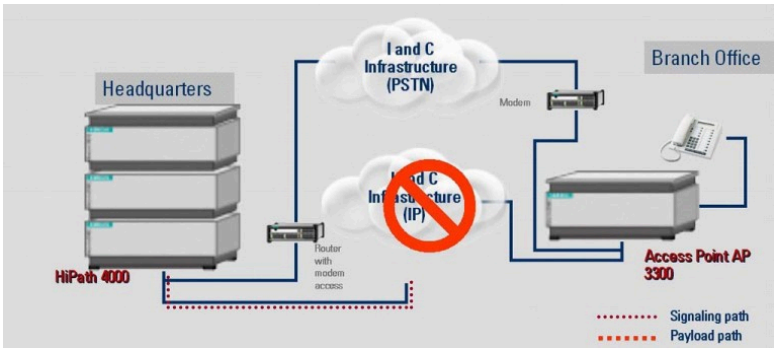


Abbildung 172: Survivability: Störung im IP-Netz

Ist die IP-Verbindung eines Access Points/OpenScape 4000 SoftGates zur Zentrale gestört, sind keine Interaktionen zwischen Access Point/OpenScape 4000 SoftGate und Zentrale möglich. Von den Endgeräten und Leitungssätzen

im Access Point/OpenScape 4000 SoftGate kommende Meldungen werden auf der (v)HG 3575 zwischengepuffert, aus der Zentrale kommende Meldungen werden im Zentralprozessor gepuffert. Überschreitet die Dauer der Störung einen einstellbaren Grenzwert, so setzt sich der Access Point/das OpenScape 4000 SoftGate zurück und trennt damit auch alle Gespräche.

10.1.5.1 Signaling Survivability

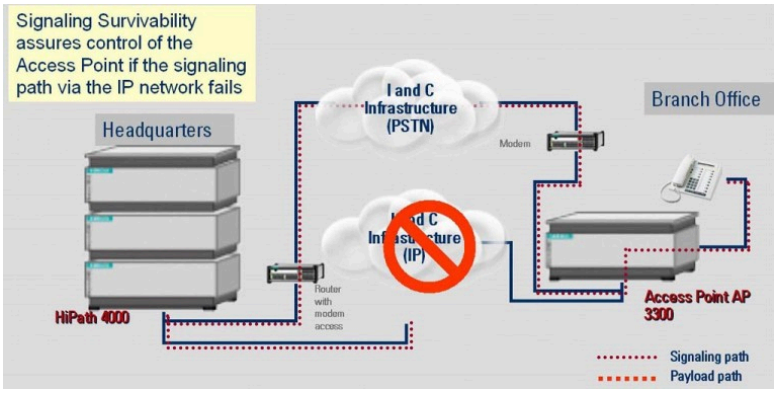


Abbildung 173: Signaling Survivability Beispile: Signalisierung über PSTN

Signaling Survivability erhält die Steuerung des Access Points/OpenScape 4000 SoftGates, wenn Signalisierung über das IP-Netz nicht mehr möglich ist.

Mehr Informationen finden Sie im Abschnitt 2.6, „Signaling Survivability“.

10.1.5.2 Payload Survivability

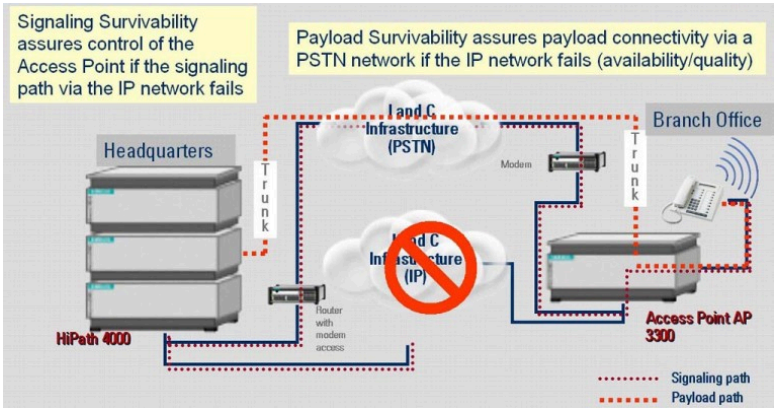


Abbildung 174: Payload Survivability: Umweg für die Payload über PSTN

Die Payload Survivability erlaubt es *anlageninterne* Gespräche über Amt zu führen. Die OpenScape 4000 ruft sich damit quasi selber an und verbindet daraus ein internes Gespräch zwischen unterschiedlichen Systemteilen. Der Weg für Payload Survivability wird auch automatisch als Überlauf gewählt, wenn bereits die gesamte Kapazität der HG 3575 in das IP-Netz genutzt wird.

Wichtig: Einschränkung von Leistungsmerkmalen bei der Nutzung von Payload Survivability, siehe Abschnitt 2.9.4, „Einschränkungen“.

10.1.6 Signaling und Payload Separation (SPS)

10.1.6.1 Leistungsmerkmalbeschreibung

Das Leistungsmerkmal „Signaling und Payload Separation“ ermöglich es in einer verteilten Architektur (IPDA) eines OpenScape 4000 Systems den Übertragungsweg für Signalisierungsinformationen und Sprachdaten zu trennen.

- Die Signalisierungsinformationen (Signaling) zwischen Hostsystem und Access Point wird über das kundeneigenen IP-Netz übertragen (Enterprise WAN).
- Die Sprachdaten (Payload) werden mittels Payload-Survivability Funktion über das öffentliche Vermittlungsnetz (PSTN) übertragen.

„Signaling und Payload Separation“ setzt auf den bereits verfügbaren Survivability-Lösungen auf. Dem zu Folge erfolgt das Routing der Signalisierungsverbindung auf Basis der bisher bekannten Mechanismen. Die Sprachdaten (RTP-Strom) werden über Verbindungen gerouted, die mittels WAML bzw. ISDN-Router über PSTN-Verbindungen zu den Standorten aufgebaut werden.

10.1.6.2 Voraussetzungen

- ISDN-Amtszugänge an jedem Standort.
- Signalisierungs- und Payloadverbindungen sind über WAML oder externen ISDN-Router aufzubauen.
- Die Bandbreitenüberwachung bzw. Einschränkung muss vom Ressourcen-Manager vorgenommen werden.
- Signaling and Payload Separation darf nur in Sterntopologien/IPDA-Konstellationen eingesetzt werden.
- Es sind verschiedene HG 3500- Baugruppen für Trunking und WAML-Funktionalität erforderlich.
- Derzeit sind nur 8 statische Verbindungen je HG 3500 einrichtbar. Deswegen ist die Anzahl von Subnetzen für die AP's eingeschränkt. Im ungünstigsten Fall (jeder AP befindet sich in einem anderen Subnetz und es ist keine Kombination von Subnetze mittels Netmask möglich) wird damit die Anzahl der über SPS erreichbaren AP's auf 8 begrenzt (ohne externen ISN-Router). Desweiteren können nur 8 WAML in einem Hostsystem eingerichtet werden.
- Verzögerungen in der Signalisierung können zu fehlerbehafteten Ergebnissen bei Rufbehandlung führen und damit das Verhalten von Leistungsmerkmalen beeinflussen (z.B. Sammelanschluss, Anrufübernahmegruppe).
- Auf Grund der Tatsache, dass bei der Anrufsignalisierung noch keine Verbindungen zu Stande gekommen ist, kann es in Szenarien einer Übernahme von Gesprächen über SPS-Verbindungen zu Verzögerungen bei der Rufannahme kommen.

- Die Payload Separierung ist zielorientiert und nur innerhalb eines OpenScape 4000 Systems verfügbar. Ist das OpenScape 4000 System mit weiteren Systemen vernetzt können netzweite Leistungsmerkmale (z.B. Netzweite Anrufübernahmegruppen) nicht mehr unterstützt werden.
- Die einzelnen Leitungsgruppen müssen ohne Parameter für Aufschalten/ Nottrennen konfiguriert werden.

10.1.6.3 Konfiguration

Für Informationen zur Konfiguration siehe Abschnitt 2.10, „Signaling und Payload Separation (SPS)“.

10.1.7 Redundante LAN-Schnittstelle

Für eine erhöhte Ausfallsicherheit sollten die IPDA Baugruppen HG 3500 und HG 3575 jeweils über LAN-Kabel an zwei verschiedene Switches angeschlossen werden (siehe hierzu Abschnitt 6.4, „Redundante LAN-Schnittstelle“).

10.1.8 LAN-Überwachung

Das Leistungsmerkmal LAN-Überwachung wurde mit der Separated Duplex-Funktion eingeführt. Durch die separate LAN-Infrastruktur von BPA und BPB steigt die Wahrscheinlichkeit, dass der Standby-BP auch dann noch LAN-Verbindungen zu den APs herstellen kann, wenn am aktiven BP ein LAN-Problem vorliegt.

Bei der IPDA LAN L1 Link-Überwachungsfunktion wird ein Switch von der LAN-Überwachungsfunktion nur dann ausgelöst, wenn die L1 Link-Überwachung nicht funktioniert. Die L1-Links des aktiven BPs und des Standby-BPs bleiben aktiv, auch wenn alle APs ausgefallen sind.

10.1.8.1 Leistungsmerkmalbeschreibung

Die Sicherheitstechnik prüft während des Normalbetriebs jede Minute den Status der LAN-Verbindungen zu den konfigurierten APs. Wenn bei der Prüfung festgestellt wird, dass kein konfigurierter AP verbunden ist, und verschiedene Bedingungen erfüllt sind (siehe Abschnitt 1.8.2, „Serviceinformationen“ > Umschaltbedingungen), wird eine Umschaltung ausgelöst, um zu testen, ob der Standby-BP eine LAN-Verbindung zu den APs herstellen kann.

In dieser Implementierung wird der Standard-BP vor der Umschaltung nicht gefragt, ob LAN-Verbindungen zu den APs möglich sind. Stattdessen wird die Umschaltung ausgelöst und anschließend am neuen aktiven BP geprüft, ob nun LAN-Verbindungen hergestellt werden können. Wenn nicht, wird eine erneute Umschaltung zum ursprünglich aktiven BP ausgelöst.

Wenn ein BP eine LAN-Verbindung zu einem AP herstellen kann, wird die LAN-Überwachungsfunktion auf diesem BP reinitialisiert, um für den Fall eines erneuten Verlusts aller AP-Verbindungen eine weitere Umschaltung zu ermöglichen.

Sonderfälle

- Es gibt einen Sonderfall, in dem EXEC-USSU:UPDATAP; ausgeführt wird. In diesem Szenario werden die LAN-Verbindungen zu allen APs angehalten und neu gestartet. Dies könnte eine Umschaltung auslösen, weil alle Bedingungen der LAN-Überwachungsfunktion erfüllt sind. Aus diesem Grund prüft die Sicherheitstechnik, ob diese Situation vorliegt, um eine unnötige Umschaltung zu vermeiden.
- Wenn der AMO-Befehl RES-USSU:ALLE; ausgeführt wird, werden alle APs zurückgesetzt. Um sicherzustellen, dass auch in diesem Szenario keine unerwünschte Umschaltung stattfindet, wurde eine Umschaltverzögerung von 1 Minute eingebaut, nach deren Ablauf die Umschaltbedingungen erneut geprüft werden. Nur wenn diese Bedingungen nach wie vor erfüllt sind, wird die Umschaltung gestartet.

10.1.8.2 Service Information

Umschaltebdingungen

Vor dem Auslösen einer Umschaltung werden die folgenden Bedingungen geprüft:

- Der BP ist aktiv und arbeitet im normalen Betriebsmodus (d. h. der letzte Restart/Reload-Vorgang ist abgeschlossen).
- Es wurde noch keine Umschaltung aufgrund dieser LAN-Überwachungsfunktion ausgelöst.
- Der Partner-BP ist in Bereitschaft und die eigene DB und die DB des Partner-BPs sind konsistent. (-> Voraussetzungen für die erfolgreiche Umschaltung).

Hinweis

Sollte der aktive BP nach einer zweiten von der LAN-Überwachungsfunktion verursachten Umschaltung noch immer keine LAN-Verbindung zu APs herstellen können, behält er diesen Status bei, bis das defekte LAN (auf dem aktiven BP) wieder in Betrieb ist. Dann beginnt die LAN-Überwachung wieder zu arbeiten.

Ein praktisches Beispiel: wenn beide LANs gleichzeitig abgeschnitten werden, führt die LAN-Überwachung zwei Umschaltungen aus und stellt die Überwachung dann ein, bis das LAN des aktiven BPs repariert ist.

DEP ADVISORY-Nachrichten

Für die LAN-Überwachungsfunktion wurden die folgenden DEP ADVISORY-Nachrichten implementiert:

1) Umschaltung wurde ausgelöst:

```
F4266 M8 N0096 SOFTREST BPA   DEP      ADVISORY
       xx-
xx-xx yy:yy:yy
      ALARM CLASS:CENTRAL:005
      FORMAT:42
      NO AP SHELF CONNECTED
      PARTNER CC AVAILABLE
      SWITCHOVER INITIATED
```

2) Umschaltung wird aufgrund des AMO ZANDE-Schalters NOLANMON abgewiesen:

```
F4266 M8 N1979 NO ACT   BPA   DEP      ADVISORY
       xx-
xx-xx yy:yy:yy
      ALARM CLASS:CENTRAL:023
      FORMAT:42
      NO AP SHELF CONNECTED,
      SWITCHOVER REJECTED:
      CHECK AMO ZANDE NOLANMON
```

3) Umschaltung wird abgewiesen, weil bereits eine Umschaltung ausgelöst wurde::

```
F4266 M8 N1979 NO ACT   BPA   DEP      ADVISORY
       xx-
xx-xx yy:yy:yy
      ALARM CLASS:CENTRAL:023
      FORMAT:42
      NO AP SHELF CONNECTED,
      SWITCHOVER REJECTED:
      NO FURTHER SWITCHBACK
```

4) Umschaltung wird abgewiesen, weil der Partner-BP nicht in Bereitschaft ist:

```
F4266 M8 N1979 NO ACT   BPA   DEP      ADVISORY
       xx-
xx-xx yy:yy:yy
      ALARM CLASS:CENTRAL:023
      FORMAT:42
      NO AP SHELF CONNECTED,
      SWITCHOVER REJECTED:
      PARTNER IS NOT STANDBY
```

10.1.8.3 Generierung (Beispiel)

Die LAN-Überwachungsfunktion ist standardmäßig aktiviert.

Sie kann mit dem AMO ZANDE-Parameter **NOLANMON** deaktiviert werden:

```
CHANGE-ZANDE:TYPE=ALLDATA2,NOLANMON=YES;
```

Anmerkung: Trotz standardmäßig aktivierter LAN-Umschaltfunktion ist es möglich, dass manche Kunden keine Umschaltung wünschen, wenn sie über eine große Anzahl fester LTU-Shelfs und nur über einen oder wenige IP-Shelfs verfügen.

10.1.8.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
ZANDE	NOLANMON	d	Leistungsmerkmal LAN-Überwachung
	NOLANMON	e	LAN Monitoring feature

10.1.9 Verschiedene Zeitzonen - Different Time Zones (DTZ)

Das Leistungsmerkmal „Different Time Zones (DTZ)“ berücksichtigt die Situation, dass sich ein IPDA-Shelf bzw. Access Point (AP-IP) oder HFA-IP Telefone in anderen Zeitzonen als das Host-System befinden können. In diesen Fällen soll statt der Systemzeit die lokale Tageszeit im Display der digitalen Telefone, die mit dem Remote-AP verbunden sind, bzw. im Display der HFA-IP Telefone angezeigt werden.

Eine detaillierte Beschreibung finden Sie im Abschnitt „Verschiedene Zeitzonen - Different Time Zones (DTZ)“.

10.1.10 A-Law/µ-Law Konvertierung im AP-Shelf

Es ist möglich Telefone in AP-Shelves anzuschließen, die mit anderen Kompandierungskennlinien arbeiten als das Host-System (z.B. Host-System in Deutschland (a-Law), Access Point in USA (µ-Law)).

Eine detaillierte Beschreibung finden Sie im Abschnitt 2.15, „A-Law/µ-Law Konvertierung im AP-Shelf“.

10.1.11 Ansagen, Töne und MFV-Wähltonempfänger pro Access Point

Es ist möglich, die Sprachen- und Ländereinstellungen mit AMO UCSU für jeden Access Point gesondert festzulegen. Aus diesem Grund können verschiedene Access Points dieselben oder unterschiedliche SIU-Init-Datendateien aufweisen.

Eine detaillierte Beschreibung finden Sie im Abschnitt 2.16, „Verschiedene Ansagen, Töne und DTMF DialTone Empfänger pro Access Point“.

10.1.12 Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point

Mit HiPath 4000 V6 bietet das System 5 Sprachen für die Textanzeigen am Endgerät, die im Host System für das komplette System (inklusive Access Points) konfiguriert werden.

Ab OpenScape 4000 V7 ist es möglich, 5 Sprachen für jeden Access Point (AP Shelf) gesondert und zum Host System unterschiedlich zu konfigurieren. Deshalb kann ein Endgerät, dass an einem Access Point angeschlossen ist andere Sprachen für die Textanzeigen haben als ein Endgerät, dass am Host System angeschlossen ist.

Eine detaillierte Beschreibung finden Sie im Abschnitt 2.17, „Verschiedene Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point“.

10.1.13 Weitere Eigenschaften

- Hohe Sprachqualität
- Wegen der systembedingt höheren Verzögerung des Sprachsignals in IP-Netzen beeinflusst Echo die Sprachqualität negativ, wenn es nicht vor der

Übertragung entfernt wird. Deshalb haben die Baugruppen HG 3500 und HG 3575 integrierte Echo-Canceller

Niedriger Bedarf an Bandbreite

Überträgt man Sprache unkomprimiert (nach G.711) über IP, so wird wegen der Verpakkung in das IP-Protokoll Bandbreite benötigt, als über ISDN.

Soll weniger Bandbreite belegt werden, kann das Sprachsignal komprimiert werden. HG 3500 und HG 3575 bieten optional Kompression nach G.729A Standard (statt 64 nur 8 kbps). Zusätzlich kann durch Unterdrückung von Sprachpausen Bandbreite gespart werden. Silence Suppression unterbindet die Übertragung von Stille auf der Leitung. (G.729AB, bzw. G.711 Annex 2)

- Unterstützung von Quality of Service im IP Netzwerk durch Priorisierung
- OpenScape 4000 IP Distributed Architecture unterstützt die Priorisierung im IP-Netz auf Basis folgender Standards:
  - IEEE 802.1 p/q (VLAN-Tagging) auf Schicht 2
  - IETF RFC 2474 (DiffServ) auf der IP Schicht
- Transportkapazität in das IP-Netz
- HG 3500 und HG 3575 können abhängig von der HW-Variante und der Konfiguration bis zu 120 B-Kanäle gleichzeitig über das IP-Netz übertragen (siehe „Gateways HG 3500 und HG 3575“, Abschnitt 2.6, „B-Kanäle“).
- Unterstützung von Networkmanagement auf Basis SNMP
- HG 3500 und HG 3575 unterstützen Networkmanagement auf Basis des SNMP Protokolls. Statistische Daten aus den anwendbaren Standard-MIBs sowie zusätzlich Daten aus proprietären MIBs lassen sich abfragen.

10.2 Einrichtung des Leistungsmerkmals IPDA

IP Distributed Architecture stellt mehr eine Erweiterung der Plattform dar, als ein typisches neues Leistungsmerkmal. Deshalb wird die Einrichtung des Leistungsmerkmals im folgenden in typische Schritte gegliedert, die nacheinander ausgeführt werden sollen:

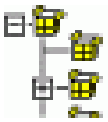
- Einrichten: OpenScape 4000 LAN Segment - Abschnitt 2.1, „OpenScape 4000 LAN Segment“
- Einrichten: Access Point (*networked* oder *direct link*) - Abschnitt 2.2, „Access Point“
- Einrichten: HG 3500 als HG3570 - Abschnitt 2.3, „HG 3500 als HG 3570 im OpenScape 4000 System“
- Einrichten: Teilnehmer-, Amts- und Querverbindungen in Access Points - Abschnitt 2.4, „Teilnehmersätze in Access Points“

Bei Bedarf müssen die folgenden Schritte nacheinander ausgeführt werden:

- Einrichten: Sonderrouten - Abschnitt 2.5, „Sonderrouten“
- Einrichten: Signaling Survivability - Abschnitt 2.6, „Signaling Survivability“
- Einrichten: Qualitätsüberwachung für die Signalisierungsverbindung über IP - Abschnitt 2.7, „Qualitätsüberwachung für die Signalisierungsverbindung über IP“
- Einrichten: Source Dependent Routing - Abschnitt 2.8, „Source Dependent Routing“
- Einrichten: Payload Survivability - Abschnitt 2.9, „Payload Survivability“
- Signalisierung und Nutzlasttrennung - Abschnitt 2.10, „Signaling und Payload Separation (SPS)“

- Anrufumlenkung im Survivability-Modus zu einem anderen Access Point - Abschnitt 2.11, „Anrufumlenkung im Survivability-Modus zu einem anderen Access Point“
- Konfiguration: Musikeinspeisung - Abschnitt 2.12, „Externe Music-On-Hold“
- Informationen zu CMI - Abschnitt 2.13, „Hinweise zu CMI“
- Konfiguration: IP-Adressänderungen - Abschnitt 2.14, „IP-Adressänderungen“
- Sollen an einem in Betrieb befindlichen System die IP-Adressen im OpenScape 4000 LAN Segment verändert werden (z.B. weil der Netzbetreiber die Netzwerkadresse ändert), müssen die Hinweise in diesem Abschnitt beachtet werden.
- Konfiguration: a-Law/µ-Law Konvertierung - Abschnitt 2.15, „A-Law/µ-Law Konvertierung im AP-Shelf“
- Konfiguration: Ansagen, Töne und MFV-Wähltonempfänger pro Access Point - Abschnitt 2.16, „Verschiedene Ansagen, Töne und DTMF DialTone Empfänger pro Access Point“
- Konfiguration: Verschiedene Display-Sprachen/nationale Zeichensätze pro Access Point - Abschnitt 2.17, „Verschiedene Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point“

In den jeweiligen Abschnitten findet sich ein Einrichtebeispiel sowie die ausführliche Erklärung aller erforderlichen AMOs und AMO-Parameter. Dabei wird unterschieden, ob die Einrichtung

	mit dem Configuration Manager oder
	mittels AMO durchgeführt wird.

Das Einrichten des Leistungsmerkmals „Access Point Emergency“ wird in „Access Point Emergency“, Kapitel 2, „Einrichtung des Leistungsmerkmals APE (Access Point Emergency)“ beschrieben.

10.2.1 OpenScape 4000 LAN Segment

Das OpenScape 4000 LAN Segment ist der Teil der Kundennetzes, in welches die IP-Komponenten des zentralen Anlagenteils, sowie direkt (nicht über Router) angeschlossene Access Points eingebracht werden.

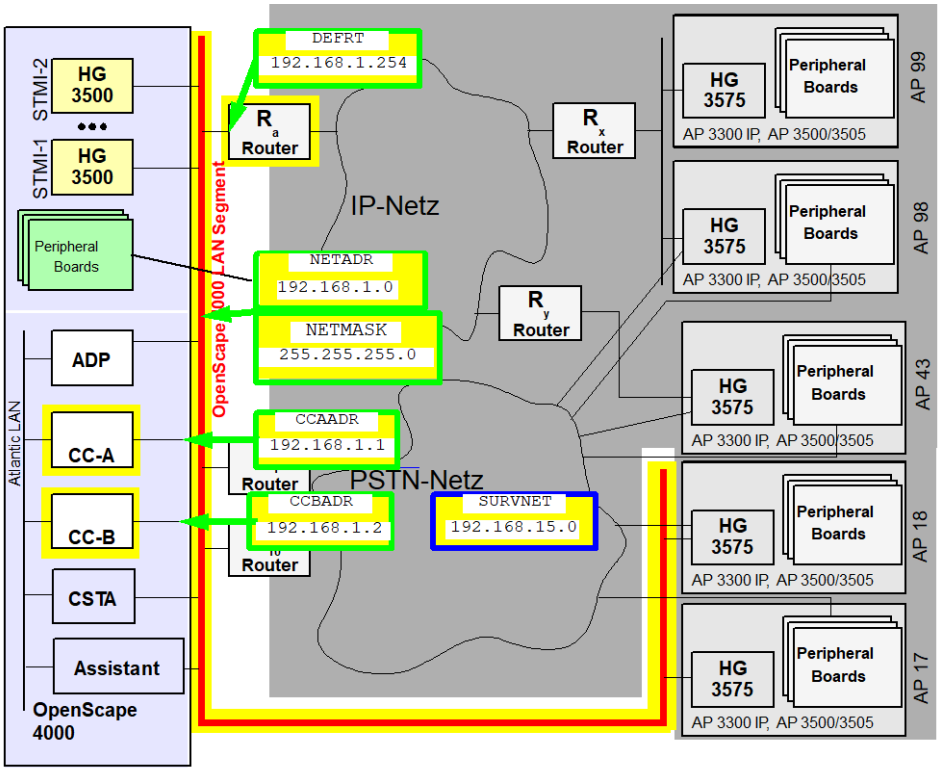


Abbildung 175: OpenScape 4000 LAN Segment

EINRICHTEN-SIPCO:	NETADR=192.168.1.0,	NETMASK=255.255.255.0,
	IPMODE=IPV4,	DEFRT=192.168.1.254,
	CCAADR=192.168.1.1,	CCBADR=192.168.1.2,
	SURVNET=192.168.15.0;	

Im Maximalausbau benötigt eine Konfiguration erhebliche Mengen an IP-Adressen in diesem Netz, nämlich.

• CC-A, CC-B, ADP:	3
• OpenScape 4000 Assistant:	1
• OpenScape 4000 CSTA:	1
• HG 3500:	max. 83
• direkt angeschlossene HG 3575:	max. 83
• Survivability Router:	max. 10

Es ist daher empfehlenswert, für den zentralen Anteil einer großen OpenScape 4000 Installation ein eigenes LAN Segment einzurichten und darin keine weiteren Knoten zuzulassen (insbesondere Fileserver etc.)

Für Demo-Installationen, bei denen das OpenScape 4000 LAN Segment isoliert bleibt, können IP-Adressen aus den privaten Adressbereichen nach RFC 1597 genommen werden, die nicht der internationalen Koordinierung bedürfen. Sie

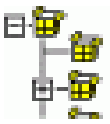
benötigen keine internationale Koordinierung. Beispielsweise empfiehlt sich der Bereich 192.168.1.1 - 192.168.1.255 mit der Netzmaske 255.255.255.0 als Klasse C Adressbereich.

Generierung

Adressen (LSNET)

Der erste Schritt zur Einrichtung von IP Distributed Architecture ist das Einrichten des OpenScape 4000 LAN Segments.

Einrichten:

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, die erforderlichen IP-Adressen eingeben und auf **Sichern** klicken.

	`EINR-SIPCO:NETADR=192.168.1.0,`
	` NETMASK=255.255.255.0,`
	`DEFRT=192.168.1.254, IPMODE=IPV4,`
	` CCAADR=192.168.1.1,`
	`CCBADR=192.168.1.2, SURVNET=192.168.15.0;`

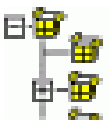
Wichtig: Obwohl die CCA-/CCB-Adresse bereits bei der Konfiguration mit dem LAN Wizard eingegeben werden musste, muss sie hier ein weiteres Mal mit AMO SIPCO konfiguriert werden.

Soll eine isolierte Konfiguration eingerichtet werden, muss der Default-Router mit der Null-Adresse `0.0.0.0` eingerichtet werden. In diesem Fall dürfen dann nur „direct link“ Access Points (siehe Abschnitt 2.2.2, „Einrichten eines „direct link“ Access Points“) konfiguriert werden. In Bild 3 „OpenScape 4000 LAN Segment“ ist Router Ra der Default Router.

Falls kein zweiter Prozessor existiert, muss die Angabe des **CCBADR** Parameters entfallen.

Der Parameter **SURVNET** kann entfallen, wenn keine Signaling Survivability benötigt wird. Wurde vom Kunden aber Signaling Survivability gekauft, ist also der entsprechende Lizenzzähler größer als Null, so muss eine Survivability-Netz Adresse (siehe **Signaling Survivability**) angegeben werden. Dies kann auch durch einen Dummy-Eintrag (Null-Adresse `0.0.0.0`) geschehen, allerdings ist die Funktion der Signaling Survivability damit nicht gegeben.

Die Lizenzen für Signaling Survivability können folgendermaßen abgefragt werden:

	**Configuration Management > HiPath Inventory Management > HIM-Anlagendaten > Leistungsmerkmale > Marketing Einheiten** Auf **Suchen** klicken > Registerkarte **Vertriebsleistungsmerkmale** > Eintrag **Signaling Survivability**

	ABFRAGEN-CODEW; Eintrag „SIGNALING SURVIVABILITY“

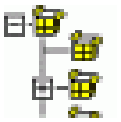
Die mit EINRICHTEN-SIPCO übergebenen Werte werden sofort gültig.

Wichtig: Prüfen Sie vor dem EINRICHTEN-SIPCO die IP-Adressen, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. **CCAADR** und **CCBADR** dürfen nicht erreichbar sein - sonst wird die entsprechende Adresse bereits benutzt. **DEFRT** muss erreichbar sein (sofern nicht 0.0.0.0).

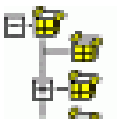
Wichtig: **Nach** dem EINRICHTEN-SIPCO muss der aktive Prozessor in seinem Netzsegment erreichbar sein. Der Standby-Prozessor in Duplex-Systemen reagiert nicht (solange er Standby ist). Da zu diesem Zeitpunkt noch keinerlei Routen eingerichtet sind, kann der aktive Prozessor ping-Anfragen aus anderen Netzsegmenten nicht beantworten!

Ändern:

Alle hier eingerichteten Parameter können nachträglich mit geändert werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, Adressen ändern und auf **Sichern** klicken.
	AENDERN-SIPCO:TYP=LSNET;

Nach dem AENDERN werden die Parameter aber nicht sofort wirksam, sondern erst nach einem Restart der Anlage. Die Datenbasis muss vorher auf Platte gesichert werden.

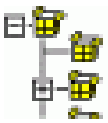
	Der Restart kann nur über den Expertenmodus ausgelöst werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	EXEC-UPDAT:BP,ALL; EXEC-REST:SYSTEM,RESTART;

Wichtig: Das Ändern der IP-Adressen hat vielfältige Auswirkungen auf ein laufendes System. Sind Änderungen erforderlich, muss eine feste Änderungsreihenfolge eingehalten

werden, da sonst Access Points unwiederbringlich abgekoppelt werden. Siehe dazu Abschnitt 2.14, „IP-Adressänderungen“.

Löschen:

Soll, z.B. nach Ende einer Teststellung, IPDA wieder komplett von der Anlage entfernt werden, so muss nach dem Deinstallieren aller Access Points und HG 3500 auch die SIPCO-Konfiguration wieder gelöscht werden. Danach können auch die Anschlüsse/LAN-Module für das OpenScape 4000 LAN Segment wieder entfernt werden. Ein Restart der Anlage ist erforderlich.

	Das Löschen kann nur über den Expertenmodus ausgeführt werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)

	`LOESCHEN-SIPCO;`
	`EXEC-UPDAT:BP,ALL;`
	
	`EXEC-REST:SYSTEM,RESTART;`

Liste der AMO-Parameter für Einrichten / Ändern:

Tabelle 30: Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	NETADR	d	Netzadresse des OpenScape 4000 LAN Segments gilt für CC-A, CC-B, alle HG 3500 (STMI2/4), Default-Router, Survivability-Router und direkt angeschlossene Access Points
	NETADR	e	Network Address of the OpenScape 4000 LAN Segment valid for CC-A, CC-B, every HG 3500 (STMI2/4), default router, survivability router and directly linked Access Points
	NETMASK	d	Netzmaske des OpenScape 4000 LAN Segments gültig wie NETADR
	NETMASK	e	Netmask of the OpenScape 4000 LAN Segment valid like NETADDR

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DEFRT	d	Default-Router im OpenScape 4000 LAN Segment über diesen Router sollen alle nicht direkt im OpenScape 4000 LAN Segment angeschlossenen Access Points von den HG 3500 Baugruppen erreicht werden. Angegeben wird die IP-Adresse der Router im OpenScape 4000 LAN Segment. Falls kein Default-Router benutzt werden soll, z. Falls kein Default-Router benutzt werden soll, z. B. für isolierte Demo-Installationen mit „direct link“ APs, muss die Adresse 0.0.0.0 angegeben werden.
	DEFRT	e	Default Router in the OpenScape 4000 LAN Segment via this router all Access Points that are not directly linked to the OpenScape 4000 LAN Segment shall be reached by all HG 3500 boards.. The IP address of this router in the OpenScape 4000 LAN Segment is to be given. If no default router shall be used, e.g. for stand-alone demo installations with „direct link“ APs, give the address 0.0.0.0.
	IPMODE	d	IP Mode. Muss für IPDA **IPV4** sein.
	IPMODE	e	IP mode. Must be set to **IPV4** for IPDA.
	CCAADR	d	IP-Adresse des CC-A Prozessors im OpenScape 4000 LAN Segment
	CCAADR	e	IP address of the CC-A Prozessor in the OpenScape 4000 LAN Segment
	CCBADR	d	IP-Adresse des CC-B Prozessors im OpenScape 4000 LAN Segment Nicht angeben, wenn kein CC-B im System
	CCBADR	e	IP address of the CC-B Prozessor in the OpenScape 4000 LAN Segment Omit, if no CC-B in the system

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SURVNET	d	Netzadresse des Survivability Netzes Die Netzmaske für das Survivability Netz ist mit 255.255.255.0 ebenso fest vorgegeben wie die Adressierung der einzelnen Knoten. Die Survivability-Router 1..10 haben die Adressen 1..10, die Access Points 17..99 die Adressen 17..99 im letzten Byte. Die vorgegebene Netzmaske schränkt die Klasse (A,B oder C) der Netzadresse nicht ein. Das Survivability Netz kann ein Subnetz eines Klasse A Netzes mit Netzmaske 255.255.255.0 sein.
	SURVNET	e	Network Address of the Survivability Network The netmask for the Survivability Network is fixed to 255.255.255.0 as well as the individual node adresses. The survivability routers 1..10 are addressed 1..10, Access Points 17..99 have address 17..99 in the last byte. The given netmask does not limitate the class (A,B or C) of the network address. The Survivability Network can be a subnet of a class A network with netmask 255.255.255.0.

Quality of Service Parameter (DIFFSERV)

Eingestellt werden können die folgenden Parameter:

- der QoS-Unterstützung auf Schicht 2 nach IEEE 802.1 q/q [`VLAN, VLANID`]
- der QoS-Unterstützung auf Schicht 3 nach IETF RFC 2474 (DiffServ) [`TOSPL, TOSSIGNL`]
- der niedrigste verwendete Port für Payload-Verbindungen (UDP/RTP +RTCP) [`UDPPORT`]

Die Ethernet-Schnittstelle **muss** bei allen beteiligten Schnittstellenpartnern (CC-A und CC-B bzw. LAN-Switch, -Router) **identisch** eingestellt werden.

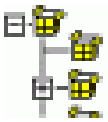
Wichtig: Die feste Einstellung eines Schnittstellenpartners führt zusammen mit der „Autonegotiate“ Einstellung des anderen Partners zu Problemen. **Vorsicht:** Fehlerhafte Einstellungen können vom System meist nicht erkannt und daher nicht gemeldet werden. Gerade wenn ein Gerät auf vollduplex, das andere auf halbduplex arbeitet, ist das nicht sofort bemerkbar. Unter hoher Last wird das auf halbduplex eingestellte Gerät verstärkt späte Kollisionen melden und die Paketverzögerung steigt stark an. Unterstützen die LAN-Ports, mit denen CC-A und CC-B verbunden sind, keine Autonegotiation, oder funktioniert diese nicht zuverlässig, so müssen die Ethernet-Schnittstellen der Zentralprozessoren auf feste Werte eingestellt werden.

Nur wenn alle Router im Netzsegment des Access Points VLAN-Tagging unterstützen, darf VLAN-Tagging auch eingeschaltet werden. Ähnliches gilt für die DiffServ CodePoints. Unterstützen die Router kein DiffServ, müssen die Standard TOS-Werte ohne DiffServ eingestellt werden. Wird DiffServ unterstützt - aber nicht die CodePoints, so müssen die vom Netzbetreiber festgelegten Werte eingestellt werden.

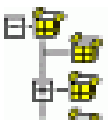
Da bestimmte Hersteller von Netzwerkkomponenten entgegen IEEE 802.1p/q die Priorisierung nur mit VLAN-ID > 0 unterstützen, kann auch die VLAN-ID eingestellt werden. Generell gilt, dass von der HG 3575 Baugruppe bei aktiviertem VLAN-Schalter die Priorisierungsbits gesetzt werden. Werte siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Laut Standard muss dann die VLAN-ID auf Null gesetzt sein, was mit der Standardeinstellung auch geschieht.

Die Parameter zur Einstellung der TOS-Bytes für die unterschiedlichen Verkehrsarten werden mit den DiffServ CodePoints gemäß der QoS-Empfehlung versorgt. VLAN-Tagging gemäß IEEE 802.1 p/q ist abgeschaltet (**VLAN=NEIN**).

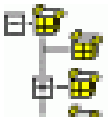
Wird im OpenScape 4000 LAN Segment VLAN-Tagging gemäß IEEE802.1 p/q unterstützt, so kann es wie folgt eingeschaltet werden:

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf Registerkarte **Anlagendaten** im Bereich **Diensttyp** die Checkbox **VLAN Tagging** aktivieren, dann auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=DIFFSERV,VLAN=JA;`

Wird DiffServ nicht unterstützt, müssen die TOS-Bytes mit Inhalt gemäß RFC 791 eingestellt werden (siehe Tabelle 3 „TOS-Werte“ im Dokument Gateways HG 3500 und HG 3575“).

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf Registerkarte **Anlagendaten** im Bereich **Diensttyp** die TOS-Werte eingeben, dann auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=DIFFSERV,TOSPL=16,TOSSIGNL=20;`

Wurde einer der Parameter **VLAN** oder **VLANID** geändert, muss ein Update auf Harddisk und anschließend ein Restart der Anlage durchgeführt werden.

	**Configuration Management > Netzwerk > Anlage** Im Pulldownmenü Aktion den Punkt **Sichern** anklicken. Der Restart kann nur über den Expertenmodus ausgelöst werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)

	`EXEC-UPDAT:BP,ALL;`
	
	`EXEC-REST:SYSTEM,RESTART;`

Hinweis:

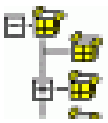
VLAN-Tagging verändert den Paket-Header. Viele L2-Switches oder Router verstehen entweder Pakete mit, oder ohne Tagging. Das heißt,

- die betroffenen Switches/Router müssen ebenfalls angepasst werden.
- während die Einstellungen nicht übereinstimmen, können (möglicherweise) keine Pakete übertragen werden
  - Die Umstellung der HG 3500 unterbricht Payload-Verbindungen
  - Die Umstellung der OpenScape 4000 CCs unterbricht den Kontakt zu allen Access Points

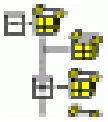
  Eine Änderung von **TOSPL** wird unmittelbar auf alle HG 3500 geladen und wird dort sofort wirksam, ohne den Betrieb der Baugruppe zu unterbrechen.

  Der Parameter **TOSSIGNL** wird erst mit Abbau und Wiederaufbau der Verbindung wirksam, für die der **TOS**-Wert eingestellt wird.

  Das Ab- und wieder Aufbauen der Verbindungen zwischen OpenScape 4000 Zentrale und Access Point kann geschehen durch
- einen Softrestart der OpenScape 4000 Anlage - betrifft dann alle Teilnehmer

	Der Softrestart kann nur über den Expertenmodus ausgelöst werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`EXEC-REST:UNIT,BP,SOFT;`

- durch AUSSCHALTEN-USSU und EINSCHALTEN-USSU für jeden einzelnen Access Point - betrifft dann nur die jeweiligen Teilnehmer.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldown-Menü Aktion **Ausschalten** anklicken. Nach der Bestätigung vom System, dass der AP ausgeschaltet wurde, mit **Aktivieren** wieder einschalten .

	`AUSSCHALTEN-USSU:LTU=xx;`
	
	`EINSCHALTEN-USSU:EINHEIT=LTG,LTU=xx;`

Die TOS-Bytes an den Access Points werden spezifisch für jeden Access Point eingerichtet.

Sollen im Kundennetz die Payloadverbindungen z.B. zwecks port-basierter Priorisierung in einem bestimmten Portbereich liegen, so kann dies folgendermaßen eingestellt werden:

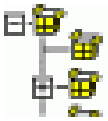
	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf Registerkarte **Anlagendaten** im Bereich **Diensttyp** die Basisadresse des UDP-Ports eingeben, dann auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=DIFFSERV,UDPPORT=40000;`

Tabelle 31: Parameter AMO SIPCO im AENDERN-Zweig unter TYP=DIFFSERV

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	TOSPL	d	TOS-Byte für die VoIP Payload-Verbindungen zwischen OpenScape 4000 und Access Point. Gültig für Pakete von beliebigen HG 3500 in Richtung Access Point.
	TOSPL	e	TOS Byte for the VoIP payload connections between OpenScape 4000 and Access Point. Valid for packets from any HG 3500 towards Access Point.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	TOSSIGNL	d	TOS-Byte für die Signalisierungsverbindungen zwischen OpenScape 4000 und Access Point. *(auch für Supervisory und RTO)* Gültig für Pakete vom CC-A, CC-B in Richtung Access Point.
	TOSSIGNL	e	TOS Byte for the Signaling connections between OpenScape 4000 and Access Point. *(also for Supervisory and RTO)* Valid for packets from CC-A, CC-B towards Access Point.
	VLAN	d	Schaltet VLAN-Tagging nach IEE 802.1p/q ein (JA) bzw. aus (NEIN). Gültig für VoIP Payload-Verbindungen von beliebigen HG 3500 in Richtung Access Point. Gültig für Pakete vom CC-A, CC-B in Richtung Access Point.
	VLAN	e	Switches VLAN Tagging according to IEEE 802.1p/q on (YES) or off (NO). Valid for VoIP payload connections from any HG 3500 towards Access Point. Valid for packets from CC-A, CC-B towards Access Point.
	VLANID	d	VLAN-ID Wert für alle HG 3500 sowie CC-A und CC-B Nur von Bedeutung, wenn VLAN=JA. 12 Bit Wert, der gemäß IEEE 802.1 p/q Standard auf Null gesetzt sein muss, wenn Priorisierung verwendet wird (VLAN=JA). Von dieser Standardeinstellung darf nur abgewichen werden, wenn Netzwerkkomponenten bestimmter Hersteller erzwingen, dass bei Nutzung der Priorisierung eine VLAN-ID > 0 zu verwenden ist.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	VLANID	e	VLAN-ID value for all HG 3500, CC-A and CC-B Only relevant if VLAN=YES. 12 Bit value that, according to IEEE 802.1 p/q, has to be set to zero when prioritization is used (VLAN=YES). This standard setting may only be changed, if network components of certain vendors enforce the usage of VLAN-ID > 0 while using prioritization.
	UDPPORT	d	Einstellung des Basis-Ports (niedrigste Portnummer) für Payloadverbindungen im IPDA-System Für jede Payload-Verbindung werden an den beteiligten Gateways HG 3500 bzw. Für jede Payload-Verbindung werden an den beteiligten Gateways HG 3500 bzw. HG 3575 ein UDP Port für RTP und ein weiterer für RTCP benötigt. Die Portnummern werden in einem Bereich von [UDPPORT .. UDPPORT+247] vergeben. RTP belegt dabei immer eine gerade Nummer, RTCP die nächst höhere ungerade. Wertebereich: [4352 .. 65038], nur gerade Zahlen erlaubt.
	UDPPORT	e	Setting of the Base Port (lowest port number) for Payload Connections in the IPDA System For every payload connection one UDP port is required for RTP and another for RTCP. The port numbers are assigned in a range of [UDPPORT .. UDPPORT+247]. RTP always uses an even number, RTCP the next higher odd one. Value range: [4352 .. 65038], only even numbers allowed.

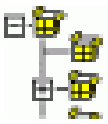
Weitere Parameter

Mit dem EINRICHTEN-SIPCO werden auch noch weitere Systemparameter auf Default-Werte eingestellt, welche durch AENDERN-SIPCO verändert werden können. Diese Parameter sind in 2 Gruppen zusammengefasst.

System-Zeitverhalten (TIMING)

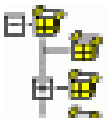
Unter TYP=TIMING können zentrale Werte des System-Zeitverhaltens für die Überwachung der IP-Verbindungen eingestellt werden. Werden die hier eingestellten Werte überschritten, schaltet das System die Kommunikation zwischen OpenScape 4000 und Access Point auf Modem-Verbindung „Signaling Survivability“ um, bzw. der Access Point geht vorübergehend außer Betrieb.

Um die geänderten Werte in den betroffenen Access Points wirksam werden zu lassen, müssen diese **alle** neu geladen werden mit

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü Aktion auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt. Vor dem `EXEC-USSU:UPDATAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden. Andernfalls wären nach einem Reload der Anlage die Daten auf dem System und auf der HG 3575 unterschiedlich und könnten nur durch `EXEC-USSU:UPDATAP,`LTU-Nummer`,UL` wieder synchronisiert werden.

Wurde der Parameter **PINGTIME** verändert, müssen auch **alle** HG 3500 neu geladen werden mit

	**Configuration Management > Anlagendaten > Wartung > BG-Wartung** Auf **Suchen** klicken und alle **STMI2** und **STMI4** auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.

	`RESTART-BSSU:ADRART=SACHNR,SACHNR=Q2316-X;`
	`und`
	`RESTART-BSSU:ADRART=SACHNR,SACHNR=Q2316-X10;`
	`und`
	`RESTART-BSSU:ADRART=SACHNR,SACHNR=Q2324-X500;`
	`und`
	`RESTART-BSSU:ADRART=SACHNR,SACHNR=Q2316-X510;`
	`und`
	`RESTART-BSSU:ADRART=SACHNR,SACHNR=Q2343-X;`

Wichtig: Bestehende Verbindungen werden dadurch getrennt.

Wichtig: Es ist wichtig, dass TIMING-Änderungen wirklich auf alle Access Points und HG 3500 geladen werden, da sonst die Systemreaktion auf Timerabläufe inkonsistent wird!

Tabelle 32: Parameter AMO SIPCO im AENDERN-Zweig unter TYP=TIMING

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	PINGTIME	d	Zeitdauer, während der nach einer **schlechten** VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575 die Verbindungsqualität getestet wird. Ist die Verbindungsqualität bei Beendigung einer Verbindung zwischen 2 HG 3500/75 als schlecht markiert, wird für die Zeitdauer PINGTIME die Verbindung getestet. Fällt während dieser Zeit die Prüfung gut aus, wird die Prüfung abgebrochen und die Verbindung zwischen den betroffenen HG 3500/75 sofort wieder auf gut gesetzt. Ist das Ergebnis schlecht, wird während der gesamten Zeit weiter geprüft und erst nach Ablauf der PINGTIME die Verbindung auf gut gesetzt wird. Weitere Informationen siehe Bild 21 „Sperren der IP-Verbindung für Payload wegen „Bad Quality““. Der Wert wird in [s], Sekunden angegeben. **Wenn Payload Survivability konfiguriert ist, wird empfohlen, das Intervall des Parameters PINGTIME auf einen höheren Wert als den Standardwert von 60 Sekunden zu ändern.** **Z. B. 15 Minuten (900 Sekunden)**

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	PINGTIME	e	Time interval for testing the payload quality between 2 HG 3500/HG 3575 after a VoIP payload connection has been terminated with quality marked **bad**. Is the payload quality for a connection between 2 HG 3500/75 marked as bad upon termination of the connection, the connection is going to be tested for the duration of PINGTIME. With positive test results during this time interval the test ist stopped immediately and the connection is marked good again. With negative results the tests will be continued until PINGTIME expires. After that the connection will be marked good again. For further Information see Bild 21 „Sperren der IP-Verbindung für Payload wegen „Bad Quality““ The value is entered in [s], seconds. **When Payload Survivability is configured, it is recommended to change the PINGTIME parameter interval to a value higher than the default 60 seconds.** **E.g. 15 minutes (900 seconds)**
	RESTIME	d	Zeit zwischen einem Schnittstellenfehler aus dem „Keep Alive“ der Signalisierungsverbindung und dem Rücksetzen des Access Points (Wartezeit bis AP-Restart). Wird ein Schnittstellenfehler des „Keep Alive“ der Signalisierungsverbindung gemeldet, startet das Zeitintervall RESTIME. Nach dem Schnittstellenfehler können keine neuen Gespräche vom/zu den betroffenen AP aufgebaut werden; bestehende Verbindungen bleiben abhängig vom IP-Netzwerk bestehen, jedoch kann es zu Nullwegen (100% Paktetloss) kommen. Nach Ablauf des Zeitintervalls wird der Access Point zurückgesetzt. Alle Payload-Verbindungen gehen verloren, es sind keine neuen Payload-Verbindungen möglich, bis es der OpenScape 4000 Zentrale wieder gelingt, Kontakt zum Access Point herzustellen. Der Wert wird in [s], Sekunden angegeben.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	RESTIME	e	Time between an interface fault specified in the „Keep Alive“ message from the signaling link and the access point reset. The RESTIME interval starts when an interface fault is reported in the „Keep Alive“ message from the signaling link. New calls cannot be set up from/to the relevant AP following the interface fault; existing connections are maintained depending on the IP network, but null paths can occur (100% packet loss). The access point is reset when the time interval expires. All payload connections are lost and no payload connections are available until the OpenScape 4000 central system succeeds in establishing contact with the access point. The value is specified in seconds [s].
	SUPVTIME	d	Maximale Zeitdauer, während der auf ein Paket auf der Überwachungsverbindung (Supervisory-Verbindung) gewartet wird. Nur bei aktivierter Signaling Survivability. Auf der Supervisory-Verbindung werden in sehr kurzen Intervallen „Keep Alive“ Meldungen gesendet. Kommt für länger als SUPVTIME kein Paket an, wird der Weg über das IP-Netz als gestört betrachtet, die Modemverbindung zum Access Point aktiviert und dieser Weg für die Signalisierungsverbindung zwischen OpenScape 4000 und Access Point verwendet. Der Wert wird in [s], Sekunden angegeben.
	SUPVTIME	e	Maximum time waiting for a packet on the Supervisory connection Only if Signaling Survivability is activated. On the Supervisory connection „keep alive“ messages are sent in very short intervals. If SUPVTIME exceeds without a packet arrived, the way through the IP networks is considered as disturbed. The modem connection to the Access Point is activated. The signaling between OpenScape 4000 and Access Point is routed via the modem connection. The value is entered in [s], seconds.

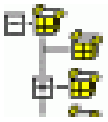
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	APESWDLYd		APE Umschalteverzögerung *nur wirksam mit dem Leistungsmerkmal AP Emergency!* siehe Abschnitt 2.10, „Festlegen der Umschalteverzögerung“ Das Umschalten eines Access Points in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Es ist entweder Null - „schalte sofort“ einzutragen, oder die Zeit, welche von der OpenScape 4000 Zentrale benötigt wird, um einen RELOAD durchzuführen. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99].
	APESWDLYe		APE Switch Over Delay *only effective with the feature AP Emergency!* siehe „Access Point Emergency“ > Abschnitt 2.10, „Festlegen der Umschalteverzögerung“ The switch-over of an Access Point into Emergency Mode can be delayed for a configurable amount of time. It shall either be set to zero - „switch immediately“, or to the amount of time which the central OpenScape 4000 system needs to perform a RELOAD. The value is entered in minutes. Range [0 .. 99].

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ALVTIME	d	Maximale Zeitdauer für den „Keep Alive“ Mechanismus der Signalisierungsverbindungen zwischen OpenScape 4000 und den Access Points. Vergeht diese Zeit ohne Antwort, wird ein Schnittstellenfehler gemeldet und der Access Point wird aus der ATTENDANCE LIST genommen (F5308, LTUC OUT OF ATTENDANCE LIST). Der Wert wird in [s], Sekunden angegeben. Wertebereich [20 .. 90] **Hinweis:** Wenn Signaling Survivability konfiguriert ist, muss dieser Parameter auf einen Wert eingestellt werden, der größer ist als die Maximalzeit für den kompletten Aufbau der Signalisierungsverbindung über Modem!
	ALVTIME	e	Maximum time interval for the „keep alive“ mechanism of the signaling connections between OpenScape 4000 and the Access Points. If there is no answer during this interval, an interface error will be reported and the access point is taken out of the ATTENDANCE LIST (F5308, LTUC OUT OF ATTENDANCE LIST). The value is entered in [s], seconds. Range [20 .. 90]. **Hinweis:** When Signaling Survivability is configured, this parameter must be set to a value greater than the maximium duration of the complete setup of signaling connection via modem!

Payload Qualität (PLQUAL)

Unter TYP=PLQUAL werden die Grenzwerte für die Überwachung der Payload-Qualität, d.h. der Sprachverbindungen eingestellt. Werden die Obergrenzen überschritten, werden weitere Sprachverbindungen zwischen den betroffenen Baugruppen (HG 3500 bzw. 3575) über den Alternativweg aufgebaut, falls einer eingerichtet ist. Unterschreiten der Untergrenze legt den Standardweg wieder zurück in das IP-Netz.

Die Delay-Werte beziehen sich immer nur auf eine Richtung (A -> B oder B -> A), nicht auf das „Round-Trip-Delay“ (A -> B -> A). Sie werden aus dem Real Time Transmission Control Protocol abgeleitet.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf Registerkarte **Anlagendaten** unter **Payload Quality** die Grenzwerte eingeben und auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=PLQUAL, DLYHILIM=200, DLYLOLIM=120, LFRHILIM=3,LFRLOLIM=2;`

Die geänderten Parameter werden sofort und ohne Betriebsunterbrechung auf alle Access Points und HG 3500 geladen.

Tabelle 33: Parameter AMO SIPCO im AENDERN-Zweig unter TYP=PLQUAL

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	DLYHILIM	d	Obere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert wird in [ms], Millisekunden eingegeben.
	DLYHILIM	e	Upper delay limit for VoIP payload connections between HG 3500/HG 3575. When delay exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is entered in [ms], milliseconds.
	DLYLOLIM	d	Untere Grenze für die Verzögerung der VoIP Payload-Verbindung zwischen HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert wird in [ms], Millisekunden eingegeben.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DLYLOLIM	e	Lower delay limit for VoIP payload connections between HG 3500/HG 3575. When delay falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is entered in [ms], milliseconds.
	LFRHILIM	d	Obere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575. Bei Überschreiten dieses Wertes wird die Verbindung zwischen den 2 betroffenen HG 3500/75 als schlecht markiert. Künftige Verbindungen zwischen diesen HG 3500/75 werden solange über einen Alternativweg geführt (sofern einer eingerichtet ist), bis die Verbindung wieder auf gut gesetzt wird. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an.
	LFRHILIM	e	Upper limit for the fraction of lost packets on VoIP payload connections between 2 HG 3500/HG 3575. When the fraction of lost packets exceeds this value, the connection between the 2 involved HG 3500/75 is marked as bad. Future connections between these HG 3500/75 will be routed via an alternate path (if set up) until the connection is marked good again. The value is the ratio of lost to sent packages in percent.
	LFRLOLIM	d	Untere Grenze für die Paketverlustrate der VoIP Payload-Verbindung zwischen 2 HG 3500/HG 3575. Bei Unterschreiten dieses Wertes wird eine vorher als schlecht markierte Verbindung zwischen 2 HG 3500/75 wieder auf gut gesetzt. Der Wert gibt das Verhältnis von verlorenen zu gesendeten Paketen in Prozent an.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LFRLOLIM	e	Lower limit for the fraction of lost packets on VoIP payload connections between 2 HG 3500/HG 3575. When the fraction of lost packets falls below this value, a connection between 2 HG 3500/75 that was previously marked as bad is marked good again. The value is the ratio of lost to sent packages in percent.

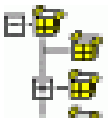
Bandbreitentabelle (BANDW)

Die Administration der systemweiten Bandbreitentabelle erfolgt mit dem AMO SIPCO, AENDERN-Zweig unter TYP=BANDW.

Direct Media Connection (DMCDATA)

Unter **TYP=DMCDATA** werden DMC spezifische Daten im CGW-IPDA Pool eingestellt.

Zusätzlich wird über den Parameter **NWDMC** eingestellt, welcher Codec-Typ für DMC-Verbindungen in Netzwerk-Szenarien mit TDM-Teilnehmern verwendet wird (G.711 oder G.729). Diese Information dient ausschließlich als Information für den Resource Manager.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf Registerkarte **Anlagendaten** das Feld **„Direct Media Connection (DMC) aktiviert** aus- bzw. einschalten, den Codec-Typ auswählen und auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=DMCDATA, DMCERL=NEIN, NWDMC=G729;`

Die geänderten Parameter sind wirksam.

Tabelle 34: Parameter AMO SIPCO im AENDERN-Zweig unter TYP=DMCDATA

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	DMCERL	d	Direct Media Connection erlaubt. Legt fest, ob Direct Media Connections auf allen HG 3500 zu unterstützen sind, oder nicht.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DMCALLWD	e	Direct Media Connections allowed. Specifies whether Direct Media Connections are to be supported by all HG 3500 gateways - or not.
	NWDMC	d	Codec-Typ für DMC-Verbindungen in Netzwerk-Szenarien mit TDM-Teilnehmern. G711 oder G729
	NWDMC	e	Codec Type for DMC connections in networking scenarios with TDM subscribers. G711 or G729

10.2.2 Access Point

Beim Einrichten eines Access Points muss unterschieden werden, ob es sich

- um einen **Access Point** handelt, der **über Router in einem anderen Netzsegment als dem OpenScape 4000 LAN Segment** angeschaltet ist (networked) (siehe Abschnitt 2.2.1, „Einrichten eines „networked“ Access Points“),

oder

- um einen **Access Point, der direkt am OpenScape 4000 LAN Segment angeschaltet ist (direct link)** (siehe Abschnitt 2.2.2, „Einrichten eines „direct link“ Access Points“).

Bild 4 „Unterschied zwischen „networked“ und „direct link“ Access Point“ zeigt die Unterschiede.

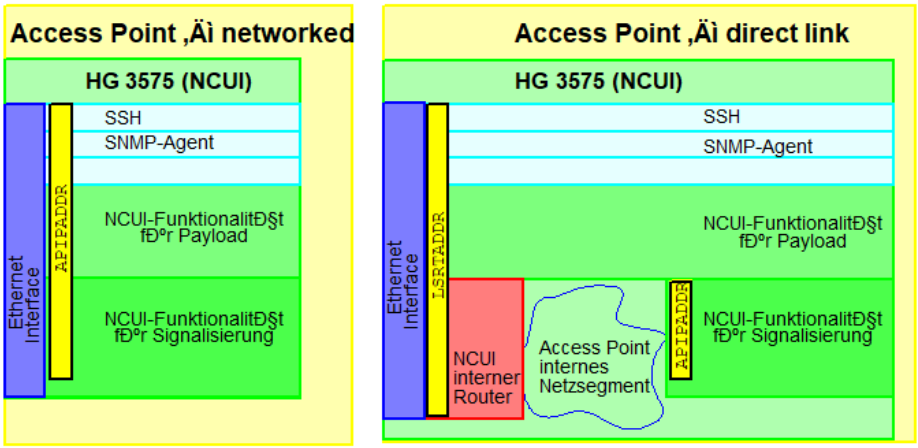


Abbildung 176: Unterschied zwischen „networked“ und „direct link“ Access Point

In jedem Fall muss ein Access Point nicht nur im System eingerichtet werden. Um ihn ansprechen zu können, müssen einige Daten bei der Erstinbetriebnahme auch lokal am Access Point eingegeben werden (siehe

Abschnitt 2.2.5, „Lokale Konfiguration eines Access Point“). Es sollte immer zuerst die Systemadministration durchgeführt werden und danach die lokale Inbetriebnahme des Access Points. Die am Access Point einzugebenden Daten können vom Configuration Management oder mittels „Expertenzugang“ direkt aus den im System eingerichteten Daten abgeleitet werden.

10.2.2.1 Einrichten eines „networked“ Access Points

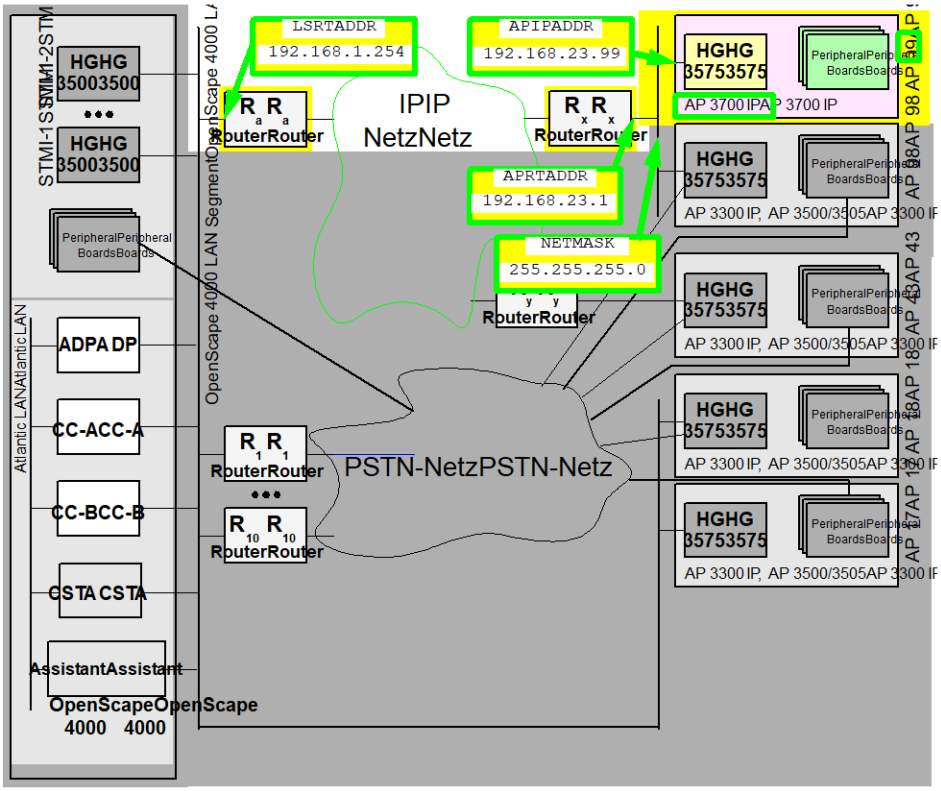


Abbildung 177: Einrichten eines „networked“ Access Points

ADD-UCSU:	ART=AP,	LTU=99,
	LTSACHNR=Q2305-X35	SRCGRP=2,
	FRMTYPE=AP 9837009,	VERBART=APNW,
	LSRTADR=192.168.1.254,	APRTADR=192.168.23.1,
	STANDOID=2,	STANDORT=“BLN ROHRDAMM 85. GEB. 30-222â##,
	TEL=03038612345,	FAX=03038654321,
	PLCHECK=JA,	ANZBKAN=40,
	CONVLAW=NO,	SIGMODE=HSRTCP;
EINRICHTEN-APRT:	TYP=APNET,	LTU=99,
	APIPADR=192.168.23.99,	NETMASK=255.255.255.0;

In Bild 5 „Einrichten eines „networked“ Access Points“ sind die wesentlichen Informationen eingezeichnet, die für das Einrichten eines „networked“ Access Points benötigt werden

- Die Tatsache, dass der Access Point über Router mit dem OpenScape 4000 LAN Segment verbunden ist“: Verbindungsart APNW, also „networked“.
- Die LTU-Nummer des Access Points, also 99.
- Die LTU-Sachnummer bezeichnet die verwendete HG 3575.
- Der Rahmentyp des Access Points leitet sich aus der Typenbezeichnung ab.
- Die IP-Adresse des Access Points: 192.168.23.99.
- Die IP-Adresse für den TAP/Service PC Anschluss am Access Point: 192.168.23.199.
- Die IP-Adresse des Routers (Port), über den der AP99 zum OpenScape 4000 LAN Segment gelangt: 192.168.23.1.
- Die Netzmaske im Segment des AP99: 255.255.255.0.
- Die IP-Adresse des Routers (Port) am OpenScape 4000 LAN Segment, über den AP99 von den zentralen Komponenten im OpenScape 4000 LAN Segment erreicht werden kann, hier also: 192.168.1.254.
- Durch Begrenzung der B-Kanalzahl wird im Einrichtebeispiel indirekt die von AP99 belegbare Bandbreite reduziert. Dieser Mechanismus funktioniert unabhängig von der Begrenzung der Bandbreite durch den Resource Manager im Leistungsmerkmal „Large Enterprise Gatekeeper“. Weitere Informationen hierzu finden Sie im Kapitel 3, „Lastkalkulation“.
- Soll Payload Quality Handling aktiviert werden? Details siehe Abschnitt 2.9, „Payload Survivability“.
- Der Source Group Index wird im Abschnitt 2.8, „Source Dependent Routing“ genau erklärt.

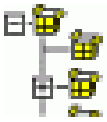
Weitere Daten werden mit den entsprechenden AMO-Parametern näher erklärt.

Generierung

Ein Access Point wird durch drei AMOs (UCSU, APRT, STMIB) konfiguriert und durch USSU eingeschaltet.

UCSU

Mit dem AMO UCSU wird der Access Point als neuer Rahmen des Systems eingerichtet und seine Erreichbarkeit über Router sichergestellt.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Neu** klicken und LTU des Access Points eingeben. Auf Registerkarte **Allgemein** und **IP-Schnittstelle (NW)** (Anschlussart=APNW) die erforderlichen Daten eingeben und auf **Sichern** klicken .
	`EINRICHTEN-UCSU:ART=AP,LTU=99,LTSACHNR=Q2305-X35,SRCGRP=2,FRAMET-YP=AP37009,VERBART=APNW,LSRTADR=192.168.1.254,APR-TADR=192.168.23.1,STANDOID=2,STANDORT="BLN ROHRDAMM 85. GEB. 30-222",TEL=03038612345,FAX=03038654321,PLCHECK=JA,ANZBKAN=40,KON-VLAW=NEIN;`

Wichtig: Die Parameter **FRAMETYP** und **VERBART** können nach dem EINRICHTEN nicht geändert werden!

Wichtig: Prüfen Sie vor dem `EINRICHTEN-UCSU` die IP-Adressen, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. **LSRTADR** und **APRTADR** müssen erreichbar sein.

Tabelle 35: APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description	
UCSU	LTSACHNR	d	Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/ NCUI4.	
	LTPARTNO	e	Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used.	
	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group für “Source Dependent Routing". (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben.	
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group for “Source Dependent Routing". This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there.	
	FRAMETYP	d	Typ des LTU-Rahmens (Shelf Typ)	
			AP-Typ	FRAMETYP
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	FRMTYPE	e	Type of the LTU Frame (Shelf Type)	
			AP-Type	FRAMETYPE
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	VERBART	d	Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APNW - Access Point via Network: Access Point und Zentrale werden in unterschiedlichen IP-Netzen betrieben, welche über Router miteinander verbunden sind.
	CONNTYPE	e	Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APNW - Access Point via Network: Access Point and central switch are located in different IP-Networks interconnected by routers.
	LSRTADR	d	Adresse des Routers im OpenScape 4000 LAN Segment VERBART=APNW: IP Adresse des Routers (Ports) im OpenScape 4000 LAN Segment, über den der Access Point / das Netz, in dem sich der Access Point befindet, erreichbar ist.
	LSRTADDR	e	Address of the Router in the OpenScape 4000 LAN Segment CONNTYPE=APNW: IP address of the router (port) in the OpenScape 4000 LAN Segment, via which the Access Point / the network, where the Access Point is located, is reachable.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	APRTADR	d	Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht. VERBART=APNW: Über diesen Router muss der Access Point CC-A, CC-B, ADP und die HG 3500 Baugruppen im OpenScape 4000 LAN Segment erreichen sowie alle anderen Access Points *). *)Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.
	APRTADDR	e	Address of the Router in the Access Point's Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network. CONNTYPE=APNW: Via this router the Access Point must be able to reach CC-A, CC-B, ADP and the HG 3500 boards in the OpenScape 4000 LAN Segment as well as all other Access Points*). *) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.

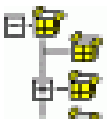
AMO	Parameter	Sprache/ Language	Beschreibung/Description
	STANDOID	d	Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!
	LOCID	e	Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already exisiting Access Point can be taken. System components in another room, floor or building are listed under a different location ID.
	STANDORT	d	Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LOCATION	e	Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed.
	TEL	d	Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	PHONE	e	Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point.
	FAX	d	Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	FAX	e	Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point.
	PLCHECK	d	Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Abschnitt 2.9, „Payload Survivability“
	PLCHECK	e	Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Abschnitt 2.9, „Payload Survivability“
	ANZBKAN	d	Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. -> Kapitel 3, „Lastkalkulation“

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	BCHLCNT	e	B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. siehe Kapitel 3, „Lastkalkulation“
	KONVLAW	d	Konvertierung von A-Law zu µ-Law bzw. µ-Law nach A-Law auf der HG 3575 Baugruppe.
	CONVLAW	e	Conversion from A-law to µ-law or µ-law to A-law on the HG 3575 board.

APRT

Mit dem AMO APRT werden dem Access Point die eigene IP-Adresse zugewiesen.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **IP-Interface (NW)** IP-Adressen eingeben und auf **Sichern** klicken.
	`EINRICHTEN-APRT:TYP=APNET, LTU=99,APIPADR=192.168.23.99, NET-MASK=255.255.255.0;`

Wichtig: Prüfen Sie vor dem `EINRICHTEN-APRT` die IP-Adressen, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. **APIPADR** darf nicht erreichbar sein - sonst wird die entsprechende Adresse bereits benutzt. **APIPADR** muss für jeden Access Point unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.

Tabelle 36: APNW: Parameter des AMO APRT im EINRICHTEN-Zweig unter TYP=APNET

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	APIPADR	d	Eigene IP-Adresse des Access Points VERBART*)=APNW: IP-Adresse des Access Points an dessen Ethernet-Port. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Parameter VERBART in Tabelle 18 „APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP“
	APIPADDR	e	Own IP Address of the Access Point CONNTYPE*)=APNW: IP address of the Access Pointâs ethernet port. APIPADDR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, ART=AP: siehe parameter CONNTYPE in Tabelle 18 „APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP“
	NETMASK	d	Netzmaske des Netzes, dem APIPADR angehört
	NETMASK	e	Netmask of the network which APIPADDR is part of

Mit dem AMO APRT können weitere Funktionen eines Access Points eingerichtet werden.

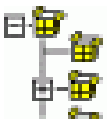
- Signaling Survivability
- Payload Survivability - Alternativwege -> Abschnitt 2.9, „Payload Survivability“
- zusätzliche Routen im IP-Netz, welche nicht über die Default-Router im Netz des Access Points bzw. im OpenScape 4000 LAN Segment erreicht werden können/sollen ->Abschnitt 2.5, „Sonderrouten“

STMIB

Mit STMIB muss nichts speziell eingerichtet werden. Die AENDERN Zweige erlauben die Einstellung einer Vielzahl von Parametern. Details sind in Abschnitt 2.2.3, „Ändern der mit AMO STMIB einstellbaren Parameter eines Access Points“ beschrieben.

USSU

Um den Access Point nach der Konfiguration auch tatsächlich in Betrieb zu nehmen, muss er eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP konfigurieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=CONFAP,LTU=xx;`

Ab diesem Zeitpunkt versucht dann die OpenScape 4000 Zentrale, den Access Point zu erreichen und, sobald sie darin erfolgreich war, zu laden.

Wichtig: Vor dem `EXEC-USSU:CONFAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden. Andernfalls wären nach einem Reload der Anlage die Daten auf dem System und auf der HG 3575 unterschiedlich und könnten nur durch `EXEC-USSU:UPDATAP`,LTU-Nummer,`UL` wieder synchronisiert werden.

Um den Access Point bei der Erstinbetriebnahme von der Zentrale aus erreichen zu können, müssen einige Daten lokal am Access Point eingegeben werden (siehe Abschnitt 2.2.5, „Lokale Konfiguration eines Access Point“).

10.2.2.2 Einrichten eines „direct link“ Access Points

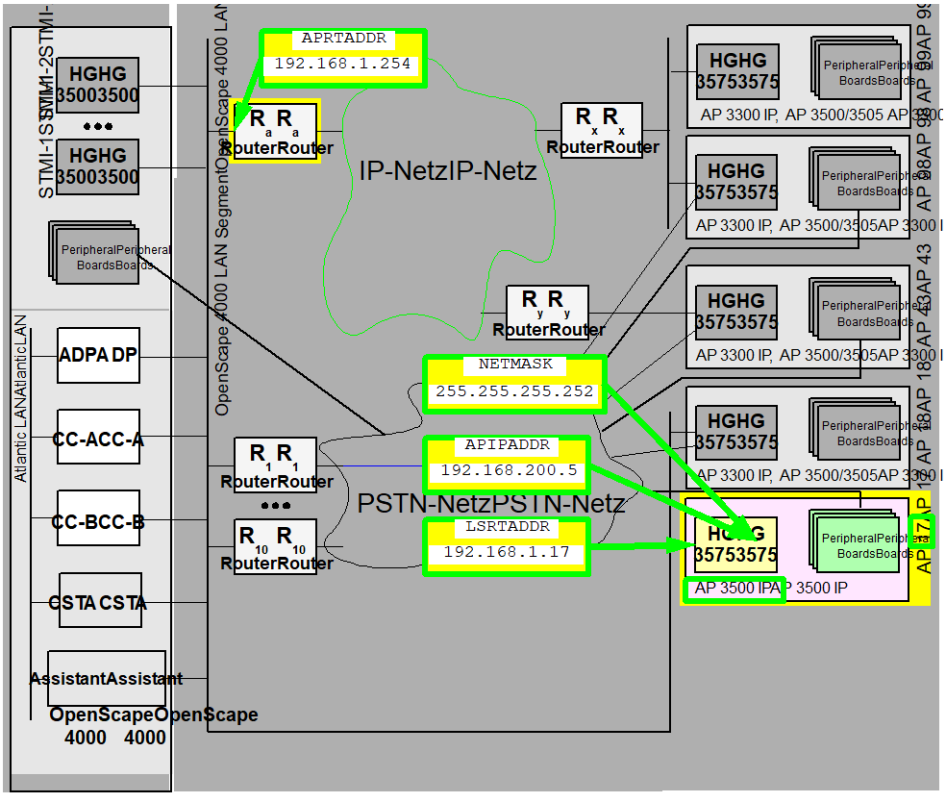


Abbildung 178: Einrichten eines „direct link“ Access Points

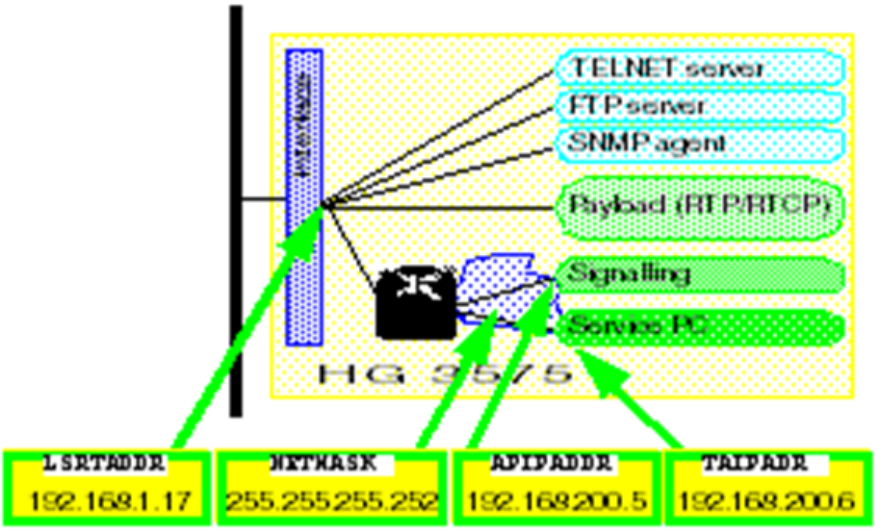


Abbildung 179: Interne Adresszuordnung eines „direct link“ Access Points

ADD-UCSU:	ART=AP,	LTU=17,
	LTSACHNR=Q2302-X10	SRCGRP=1,
	FRAMETYP=INCH19,	VERBART=APDL,
	LSRTADR=192.168.1.17,	APRTADR=192.168.1.254,
	STANDOID=1,	STANDORT="MCH MACHTLFINGERSTR.1 GEB. 7202-111",
	TEL=08972223456,	FAX=08972265432,
	PLCHECK=JA,	ANZBKAN=20,
	KONVLAW=NEIN;	
EINRICHTEN-APRT:	TYP=APNET,	LTU=17,
	APIPADR=192.168.200.5,	NETMASK=255.255.255.252;

Beim „direct link“ Access Point ist der Ethernet-Port des Access Points direkt am OpenScape 4000 LAN Segment angeschlossen und vom CC-A, CC-B ohne Router zu erreichen.

Das Leistungsmerkmal Signaling Survivability erfordert aber das Re-Routing einer Verbindung im Störungsfall (von LAN auf Modem). Damit das funktioniert, darf der Access Point „logisch“ nicht im OpenScape 4000 LAN Segment hängen. In diesem Fall wird also innerhalb des Access Points ein Router aktiviert, der Pakete aus dem OpenScape 4000 LAN auf die „logische“, innere Adresse des Access Points weiterleitet.

Dazu enthält der Access Point ein „logisches“ IP-Netz, in dem nur er selbst und gegebenenfalls der TAP/Service PC Anschluss eine Adresse haben. Um

Adressen zu sparen, kann für dieses Netz die Netzmaske 255.255.255.252 verwendet werden.

Auch diese Mini-Netze und deren Adressen sind mit dem Netzwerkverwalter des Kunden abzustimmen und dürfen sich natürlich nicht überschneiden.

In Bild 6 „Einrichten eines „direct link“ Access Points“ sind die wesentlichen Informationen eingezeichnet, die für das Einrichten eines „direct link“ Access Points benötigt werden:

- Die Tatsache, dass der Access Point direkt mit dem OpenScape 4000 LAN Segment verbunden ist: Verbindungsart APDL, also „direct link“.
- Die LTU-Nummer des Access Points, also 17.
- Die LTU-Sachnummer bezeichnet die verwendete HG 3575.
- Der Rahmentyp des Access Points leitet sich aus der Typenbezeichnung ab.
- Die interne IP-Adresse des Access Points: 192.168.200.5.
- Die IP-Adresse für den TAP/Service PC Anschluss am Access Point: 192.168.200.6.
- Die IP-Adresse des eigenen Ethernet Ports, über den der AP17 zum OpenScape 4000 LAN Segment gelangt: 192.168.1.17.
- Die Netzmaske im inneren Segment des AP17: 255.255.255.252.
- Die IP-Adresse des Routers (Port) am OpenScape 4000 LAN Segment, über den AP17 Access Points erreichen kann, die nicht direkt am OpenScape 4000 LAN Segment erreicht werden können (also „networked“ APs), hier also Router Ra: 192.168.1.254. Sind in der gesamten Konfiguration keine „networked“ APs enthalten, oder ist dies eine isolierte Demo-Installation, so enfällt dieser Router. Er **muss** dann mit der Null-Adresse 0.0.0.0 eingerichtet werden.
- Durch Begrenzung der B-Kanalzahl wird im Einrichtebeispiel indirekt die von AP99 belegbare Bandbreite reduziert. Dieser Mechanismus funktioniert unabhängig von der Begrenzung der Bandbreite durch den Resource Manager im Leistungsmerkmal „Large Enterprise Gatekeeper“. Weitere Informationen hierzu finden Sie im Kapitel 3, „Lastkalkulation“.
- Soll Payload Quality Handling aktiviert werden? Details siehe Abschnitt 2.9, „Payload Survivability“
- Der Source Group Index wird im Abschnitt 2.8, „Source Dependent Routing“ genau erklärt.

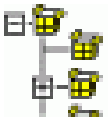
Weitere Daten werden mit den entsprechenden AMO-Parametern näher erklärt.

Generierung

Ein Access Point wird durch drei AMOs (UCSU, APRT, STMIB) konfiguriert und durch USSU eingeschaltet.

UCSU

Mit dem AMO UCSU wird der Access Point als neuer Rahmen des Systems eingerichtet und seine Erreichbarkeit über Router sichergestellt.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Neu** klicken und LTU des Access Points eingeben. Auf Registerkarte **Allgemein** und **IP-Schnittstelle (DL)** (Anschlussart=APDL) die erforderlichen Daten eingeben und auf **Sichern** klicken.
	`EINRICHTEN-UCSU:ART=AP,LTU=17,LTSACHNR=Q2302-X10,SRCGRP=1, FRAMETYP=INCH19, VERBART=APDL, LSRTADR=192.168.1.17, APR▶TADR=192.168.1.254,STANDOID=1,STANDORT="MCH MACHTLFINGERSTR.1 GEB. 7202-111", TEL=08972223456, FAX=08972265432, PLCHECK=JA, ANZBKAN=20, KONVLAW=NEIN;`

Die Parameter **FRAMETYP** und **VERBART** können nach dem EINRICHTEN nicht geändert werden!

Wichtig: Prüfen Sie vor dem `EINRICHTEN-UCSU` die IP-Adressen, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. **APRTADR** muss erreichbar sein. **LSRTADR** darf nicht erreichbar sein - sonst wird die entsprechende Adresse bereits benutzt. **LSRTADR** muss für jeden „direct link“ Access Point unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.

Tabelle 37: APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
UCSU	LTSACHNR	d	Sachnummer der LTU-Baugruppe, hier die Sachnummer der verwendeten NCUI2+/ NCUI4.
	LTPARTNO	e	Part Number of the LTU Board, here part number of the NCUI2+/NCUI4 used.
	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group für “Source Dependent Routing". (Wegesuche in Abhängigkeit vom Rufenden) Dieser Parameter ist wichtig für Source Dependent Routing und Payload Survivability und wird dort näher beschrieben.

AMO	Parameter	Sprache/ Language	Beschreibung/Description	
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group for “Source Dependent Routing". This parameter is relevant for Source Dependent Routing and Payload Survivability and will be described in more detail there.	
	FRAMETYP	d	Typ des LTU-Rahmens (Shelf Typ)	
			AP-Typ	FRAMETYP
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	FRMTYPE	e	Type of the LTU Frame (Shelf Type)	
			AP-Type	FRAMETYPE
			AP 3300 IP	L80XF
			AP 3500 IP	INCH19
			AP 3700 IP	AP37009
	VERBART	d	Art der Verbindung zwischen Access Point und Zentrale Für IPDA kommen nur die Werte APDL und APNW in Frage. APDL - Access Point Direct Link: - Access Point ist direkt am OpenScape 4000 LAN Segment angeschlossen, d.h. im selben IP-Netz.	
	CONNTYPE	e	Type of the Connection between Access Point and the Central Switch Only the values APDL and APNW are possible for IPDA. APDL - Access Point Direct Link: - Access Point is connected directly to the OpenScape 4000 LAN Segment, i.e. in the same IP network.	

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LSRTADR	d	Adresse des Routers im OpenScape 4000 LAN Segment VERBART=APDL: Dies ist die IP-Adresse am Ethernet-Port des Access Points, über den er mit dem OpenScape 4000 LAN Segment verbunden ist. Bei APDL enthält der Access Point einen lokalen Router der die IP-Adresse des Access Points (in einem eigenen Netzwerksegment) mit dem OpenScape 4000 LAN Segment verbindet. D.h. auch hier handelt es sich um die Adresse eines (wenn auch unsichtbaren) Routers. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO). LSRTADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.
	LSRTADR	e	Address of the Router in the OpenScape 4000 LAN Segment CONNTYPE=APDL: This is the IP address of the Access Point's ethernet port connected to the OpenScape 4000 LAN Segment. With APDL the AP contains a local router that connects the own IP address of the Access Point (in its own network segment) to the OpenScape 4000 LAN Segment. It's a router's address, even with the router invisible. This IP address must belong to the OpenScape 4000 LAN Segment (see NETADDR in AMO SIPCO) LSRTADDR must be different for every board. The AMO does not check compliance with this rule.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	APRTADR	d	Adresse des Routers im Netzwerk des Access Points IP Adresse des Routers (Ports) im Netz, in dem sich der Access Point befindet, über den der Access Point Adressen außerhalb dieses Netzes erreicht. VERBART=APDL: Über diesen Router muss der direkt am OpenScape 4000 LAN Segment angeschlossene Access Point alle Access Points erreichen, die sich in anderen Netzen befinden. Meist ist dies der Default-Router des OpenScape 4000 LAN Segments, welcher mit dem Parameter DEFRT im AMO SIPCO eingerichtet wird*). Sind in der gesamten Konfiguration keine „networked“ APs enthalten, oder ist dies eine isolierte Demo-Installation, so enfällt dieser Router. Geben Sie dazu hier die Null-Adresse 0.0.0.0 an. *)Ausnahmen für Sonderrouten sind möglich und werden im Routing Table Zweig des AMO APRT eingerichtet.
	APRTADDR	e	Address of the Router in the Access Point's Network IP address of the router (port) in the network where the Access Point is located, via which the Access Point reaches addresses outside of this network. CONNTYPE=APDL: Via this router an Access Point directly connected to the OpenScape 4000 LAN Segment must be able to reach all Access Points that are located in different networks. Usually this is the default router of the OpenScape 4000 LAN Segment, administered in parameter DEFRT with AMO SIPCO*). If there are no „networked“ APs in the whole configuration or if this is a stand-alone demo installation, this router is not needed. Give the address 0.0.0.0 for this purpose. *) Exceptions for special routes are possible. They are administered in the routing table branch of AMO APRT.

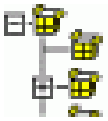
AMO	Parameter	Sprache/ Language	Beschreibung/Description
	STANDOID	d	Standort Identifikation Schlüsselzahl zur Identifikation des Standorts eines Access Points, der unterschiedlich zum Standort der Zentralanlage sein kann. Der Parameter wird benötigt, um den vertrieblichen Bestand (PARK-Daten) der Anlagenteile standortabhängig zu pflegen. Der Wert wird vom Konfigurator-Tool vergeben und muss so übernommen werden. Gegebenenfalls ist der Wert vom Systemplaner zu erfragen. Ist kein Tool-generierter Wert verfügbar, z.B. bei Teststellungen, soll der Wert 999 verwendet werden, um dies auszudrücken. Bei Erweiterungen an einem Standort (zusätzlicher Access Point) kann der Wert des bereits existierenden Access Points übernommen werden. Systemkomponenten in einem anderen Raum, Stockwerk, oder Gebäude werden unter einer anderen Standort-Identifikation geführt!
	LOCID	e	Location Identification Key number for identification of the location of an Access Point, which can differ from the location of the central switch. This parameter is necessary to maintain the sales database for the parts of the system, based on locations. The value is determined by the Configurator tool and must be taken over unchanged. If necessary, ask the system planner for the value. If no tool-generated value is available, e.g. for test and demo configurations, the value 999 shall be used to express this. For expansions at a certain location (additional Access Point), the value of the already exisiting Access Point can be taken. System components in another room, floor or building are listed under a different location ID.
	STANDORT	d	Angabe darüber, wo der Access Point zu finden ist. z.B. Firma, Ort, Straße, Gebäude, Stockwerk, Raumnummer, ... Maximal 48 Zeichen können eingegeben werden.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	LOCATION	e	Info, where to find the Access Point E.g. Company, city, street, building, floor, room number, ... A maximum of 48 characters is allowed.
	TEL	d	Telefonnummer am Standort des Access Points Nächstgelegenes Telefon, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	PHONE	e	Phone number at the Access Point The nearest phone, where a service engineer can be reached at the Access Point.
	FAX	d	Faxnummer am Standort des Access Points Nächstgelegenes Faxgerät, über das ein Techniker vor Ort am Access Point erreicht werden kann.
	FAX	e	Fax number at the Access Point The nearest fax, where a service engineer can be reached at the Access Point.
	PLCHECK	d	Payload Quality Check Gibt an, ob für diesen Access Point auf schlechte Payload Qualität reagiert werden soll (durch Sperren der Verkehrsbeziehung bzw. Weg über Payload Survivability) oder nicht. -> Abschnitt 2.9, „Payload Survivability“
	PLCHECK	e	Payload Quality Check Defines whether this Access Point shall react on bad Payload Quality (by blocking of the relation or routing via Payload Survivability Path) or not. -> Abschnitt 2.9, „Payload Survivability“

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ANZBKAN	d	Anzahl B-Kanäle Gibt an, wieviele B-Kanäle an der Schnittstelle zwischen Access Point und LAN gleichzeitig genutzt werden dürfen. Auf diese Weise lässt sich die maximale Bandbreite, die der Access Point im LAN benötigt, grob begrenzen. -> Kapitel 3, „Lastkalkulation“
	BCHLCNT	e	B Channel Count Defines how many B channels may be used concurrently at the interface between Access Point and LAN. By this the maximum bandwidth needed by an Access Point can be limited coarsely. siehe Kapitel 3, „Lastkalkulation“
	KONVLAW	d	Konvertierung von A-Law zu µ-Law bzw. µ-Law nach A-Law auf der HG 3575 Baugruppe.
	CONVLAW	e	Conversion from A-law to µ-law or µ-law to A-law on the HG 3575 board.

APRT

Mit dem AMO APRT wird dem Access Point die eigene (innere) IP-Adresse zugewiesen.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **IP-Schnittstelle (DL)** IP-Adressen eingeben und auf **Sichern** klicken.
	`EINRICHTEN-APRT:TYP=APNET, LTU=17,APIPADR=192.168.200.5, NET-MASK=255.255.255.252;`

Wichtig: Wenn Sie nach der Inbetriebnahme die (innere) IP-Adresse **APIPADR** durch **ping** prüfen möchten, müssen Sie auf dem Rechner, von dem aus Sie den **ping** absetzen, die Route zum AP-internen Netzsegment einrichten. => Host=APRT:**APIPADR**, Netmask=APRT:**NETMASK**,Router=UCSU:**LSRTADR**. **APIPADR** muss für jeden Access Point unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.

Tabelle 38: APDL: Parameter des AMO APRT im EINRICHTEN-Zweig unter TYP=APNET

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	APIPADR	d	Eigene IP-Adresse des Access Points VERBART*)=APDL: IP-Adresse des Access Points in seinem eigenen Netzwerksegment - nicht die IP-Adresse the Ethernet-Ports, welche in diesem Fall vom internen Router belegt wird. APIPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel. *) AMO UCSU, ART=AP: siehe Parameter VERBART in Tabelle 18 „APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP“
	APIPADDR	e	Own IP Address of the Access Point CONNTYPE*)=APDL: IP address of the Access Point in its own network segment - not the IP address of it's ethernet port which is assigned to the internal router in this case. APIPADDR must be different for every board. The AMO does not check compliance with this rule. *) AMO UCSU, UNIT=AP: see parameter CONNTYPE in Tabelle 18 „APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP“
	NETMASK	d	Netzmaske des Netzes, dem APIPADR angehört
	NETMASK	e	Netmask of the network which APIPADDR is part of

Mit dem AMO APRT können weitere Funktionen eines Access Points eingerichtet werden.

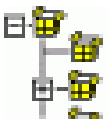
- Signaling Survivability
- Payload Survivability - Alternativwege -> Abschnitt 2.9, „Payload Survivability“
- zusätzliche Routen im IP-Netz, welche nicht über die Default-Router im Netz des Access Points bzw. im OpenScape 4000 LAN Segment erreicht werden können/sollen ->Abschnitt 2.5, „Sonderrouten“

STMIB

Mit STMIB muss nichts speziell eingerichtet werden. Die AENDERN Zweige erlauben die Einstellung einer Vielzahl von Parametern. Details sind in Abschnitt 2.2.3, „Ändern der mit AMO STMIB einstellbaren Parameter eines Access Points“ beschrieben.

USSU

Um den Access Point nach der Konfiguration auch tatsächlich in Betrieb zu nehmen, muss er eingeschaltet werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP konfigurieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=CONFAP,LTU=xx;`

Ab diesem Zeitpunkt versucht dann die OpenScape 4000 Zentrale, den Access Point zu erreichen und, sobald sie darin erfolgreich war, zu laden.

Wichtig: Vor dem `EXEC-USSU:CONFAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden. Andernfalls wären nach einem Reload der Anlage die Daten auf dem System und auf der HG 3575 unterschiedlich und könnten nur durch `EXEC-USSU:UPDATAP`, LTU-Nummer, `UL` wieder synchronisiert werden.

Um den Access Point bei der Erstinbetriebnahme von der Zentrale aus erreichen zu können, müssen einige Daten lokal am Access Point eingegeben werden (siehe Abschnitt 2.2.5, „Lokale Konfiguration eines Access Point“).

10.2.2.3 Ändern der mit AMO STMIB einstellbaren Parameter eines Access Points

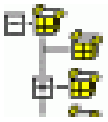
Siehe Kapitel 11, „Gateway HG 3575 - Ändern der mit AMO STMIB einstellbaren Parameter“ im Dokument „Gateways HG 3500 und HG 3575“.

10.2.2.4 Löschen eines Access Point

Soll ein Access Point aus der Konfiguration entfernt werden (im Beispiel AP 43), muss folgende Reihenfolge eingehalten werden:

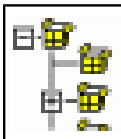
- Falls Payload Survivability eingerichtet ist, muss geprüft werden, ob der zu löschende Access Point den Amtszugang für eine Source Group leistet. Wenn ja, muss eine geeignete Ablösung gefunden werden.

- Falls Payload Survivability eingerichtet ist und mit dem Löschen dieses Access Points eine Source Group überflüssig wird, muss das LCR angepasst und gegebenenfalls die Source Group gelöscht werden.

	**Configuration Management > Anlagendaten > IPDA** **> IPDA - Payload Survivability** Auf **Suchen** klicken, den Access Point auswählen und dann auf **Löschen** klicken.
	`LOESCHEN-APRT:TYP=ALTROUT,SRCGRP=3;`

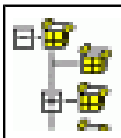
- Löschen aller Peripheriebaugruppen, die in diesem Access Point eingerichtet sind (das setzt seinerseits voraus, dass darauf keine Teilnehmer eingerichtet sind etc.)
- Falls Signaling Survivability für diesen Access Point eingerichtet ist:

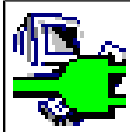
  Entfernen der Zuordnung dieses Access Points zu einem Survivability Router

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** die gewünschte Router-Nummer bei **Signaling Survivability** löschen und auf **Sichern** klicken.
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`

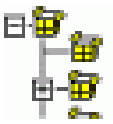
- Falls Sonderrouten eingerichtet sind: (Abschnitt 2.5, „Sonderrouten“)
  - Löschen der korrespondierenden Einträge in den Routing Tabellen anderer Access Points, falls diese Einträge nicht für weitere Access Points gültig bleiben.

  Im Beispiel in Bild 12 „Sonderrouten zwischen Access Points“ wird die Route über Router Rz überflüssig, wenn AP 43 gelöscht wird. Würde jedoch statt AP 43 der AP 98 gelöscht, müsste die Route bestehen bleiben, da sie auch für AP 99 gilt.

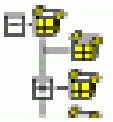
	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches Routing** Auf **Suchen** klicken und den Access Point auswählen. In den zu löschenden Zeilen der Routingtabelle Nulladressen (0.0.0.0) eintragen und auf **Sichern** klicken.

	`LOESCHEN-`
	`APRT:TYP=ROUTTBL,MTYP=NCUI,LTU=99,INDEX=1;`
	Hinweis: Hier wird nicht nach HW-Typ unterschieden. NCUI gilt für NCUI2 und NCUI4.

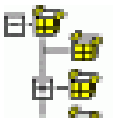
- Ausschalten des Access Points mit USSU:

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf **Ausschalten** klicken.
	`AUSSCHALTEN-USSU:LTU=43;`

- Abschalten der IP-Verbindung des Access Points mit USSU:

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:ART=DELAP,LTU=43;`

- Löschen des Access Points (CM):

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen, dann auf **Löschen** klicken.

- Löschen der IP-Netzwerkkonfiguration des Access Point:

	`LOESCHEN-APRT:TYP=APNET,LTU=43;`

- Löschen des Access Points mit UCSU:

	`LOESCHEN-UCSU:ART=AP,LTU=43;`

Wichtig: War der gelöschte Access Point für AP-Emergency konfiguriert, d.h. einer Emergency-Gruppe zugeordnet, so muss der folgende Hinweis beachtet werden: Die IP-Adresse des gelöschten Access Points darf erst wiederverwendet werden, wenn diese Änderung gesichert auf allen CC-AP übernommen wurde, d.h. das „Cloning“ mittels OpenScape 4000 Assistant > Backup & Restore abgeschlossen ist.

10.2.2.5 Lokale Konfiguration eines Access Point

Wenn ein Access Point im OpenScape 4000 System eingerichtet wurde, kann er nicht sofort in Betrieb gehen. Das zentrale System kann keinen Kontakt zum Access Point herstellen, solange dieser nicht mit den wesentlichen IP-Adressen etc. eingerichtet ist.

Um diese Erst-Konfiguration lokal am Access Point durchzuführen, gibt es eine „Expertenzugang“ Applikation. Dazu wird der TAP/Service-PC an der mit „Service“ bezeichneten RS232/V.24-Schnittstelle der HG 3575 angeschlossen und die Applikation gestartet.

Zum Login muss das Terminal-Login verwendet werden. Bei fabrikneuen Baugruppen ist das „TRM“, ein Passwort ist nicht gesetzt. War die Baugruppe bereits im Einsatz - und wurde dort Terminal-Login und Passwort verändert - so gelten die dort eingestellten Werte.

Ist im OpenScape 4000 System ein Duplex-Prozessor vorhanden (CC-B) so muss die Adresse in jedem Fall angegeben werden. Es ist schließlich nicht vorhersehbar, ob zu diesem Zeitpunkt gerade CC-A oder CC-B die aktive Rolle spielt. Falls kein CC-B in der Anlage existiert, entfällt die IP-Adresse für diesen Prozessor.

Die IP-Adresse des TAP muss nur angegeben werden, wenn von diesem Access Point aus auf die Administration des OpenScape 4000 Systems zugegriffen werden soll.

Wird in dem Ethernet Segment, an das der Access Point angeschlossen werden soll, VLAN-Tagging genutzt, so müssen dafür Einstellung bei der Erstinbetriebnahme gemacht werden. Wurde der Access Point in einem Netz mit VLAN-Tagging betrieben und soll jetzt ohne VLAN-Tagging laufen, muss diese Einstellung ebenfalls lokal geändert werden.

Soll der Access Point mit einer festen Einstellung der Ethernet-Schnittstelle bezüglich Bitrate und Modus betrieben werden, oder soll diese feste Einstellung (bei Umzug in ein anderes Netz) aufgehoben werden, muss diese Einstellung ebenfalls lokal gemacht werden.

Von den Parametern, die angezeigt und einstellbar sind, müssen nur einige tatsächlich eingegeben werden. Alle anderen Parameter werden aus dem OpenScape 4000 System geladen, sobald das zentrale System den Kontakt zum Access Point aufbauen kann;

Wichtig: Ändern eines Parameterwertes auf lokaler Ebene führt **nicht** zur Änderung des Wertes im System. Sämtliche lokal am Access Point eingestellten Parameter werden beim Laden der Baugruppe aus dem OpenScape 4000 System mit den im System eingestellten Werten überschrieben.

Auch bei der lokalen Konfiguration des Access Points wird wieder zwischen „networked“ und „direct link“ unterschieden.

Networked Access Point

Folgende Felder müssen ausgefüllt werden:

Tabelle 39: Grundinitialisierungsparameter für „networked“ Access Point

Parameter	Hinweis	AMO - Zweig - Parameter
IP-Adresse des Access Point	Darf nicht im gleichen Netz liegen wie die IP-Adresse des CC-A	APRT TYP=APNET - APIPADR
Netzmaske im Netz des Access Point	Netzmaske muss zur Klasse der IP-Adresse des Access Points passen.	APRT TYP=APNET - NETMASK
IP-Adresse des Default Routers im Netz des Access Point	Muss im gleichen Netz liegen wie die IP-Adresse des Access Points	UCSU ART=AP - APRTADR
IP-Adresse des CC-A		SIPCO TYP=LSNET - CCAADR
IP-Adresse des CC-B	Muss im gleichen Netz liegen wie die IP-Adresse des CC-A	SIPCO TYP=LSNET - CCBADR
Netzmaske des OpenScape 4000 LAN Segments	Netzmaske muss zur Klasse der IP-Adresse des CC-A passen.	SIPCO TYP=LSNET - NETMASK
VLAN-Tagging ein/aus		STMIB: MTYP=NCUI2, TYP=IFDATA - VLAN
VLAN-ID		STMIB: MTYP=NCUI2, TYP=IFDATA - VLANID
Betriebsart der Ethernet-Schnittstelle		STMIB: MTYP=NCUI2, TYP=IFDATA - BITRATE

Direct Link Access Point

Folgende Felder müssen ausgefüllt werden:

Tabelle 40: Grundinitialisierungsparameter für „direct link“ Access Point

Parameter	Hinweis	AMO - Zweig - Parameter
IP-Adresse des Access Points im OpenScape 4000 LAN Segment	Muss im gleichen Netz liegen wie die IP-Adresse des CC-A	UCSU ART=AP - LSRTADR
Netzmaske des OpenScape 4000 LAN Segments	Netzmaske muss zur Klasse der IP-Adresse des CC-A passen.	SIPCO TYP=LSNET - NETMASK
IP-Adresse des Default Routers im OpenScape 4000 LAN Segment	Muss im gleichen Netz liegen wie die IP-Adresse des CC-A	UCSU ART=AP - APRTADR
IP-Adresse des CC-A		SIPCO TYP=LSNET - CCAADR
IP-Adresse des CC-B	Muss im gleichen Netz liegen wie die IP-Adresse des CC-A	SIPCO TYP=LSNET - CCBADR
IP-Adresse des Access Points im AP-internen Netzsegment	Darf nicht im gleichen Netz liegen wie die IP-Adresse des CC-A	APRT TYP=APNET - APIPADR
Netzmaske des AP-internen Netzsegments	Netzmaske muss zur Klasse der IP-Adresse des Access Points im AP-internen Netzsegment passen.	APRT TYP=APNET - NETMASK
VLAN-Tagging ein/aus		STMIB: MTYP=NCUI2, TYP=IFDATA - VLAN
VLAN-ID		STMIB: MTYP=NCUI2, TYP=IFDATA - VLANID
Betriebsart der Ethernet-Schnittstelle		STMIB: MTYP=NCUI2, TYP=IFDATA - BITRATE

Hinweise für die lokale Konfiguration ohne „Expertenzugang“ Applikation finden sich in Kapitel 4, „Lokale Administration des Access Points am CLI mittels Terminal“.

10.2.2.6 Referenztakt im Access Point

Die OpenScape 4000 Zentrale hat einen hochgenauen Taktgenerator, der aus unterschiedlichen Quellen synchronisiert werden kann. Mögliche Quellen sind z.B. digitale Amtsleitungen. Die entsprechenden Anschlussbaugruppen können dann in den LTUs 1-15 den Takt einspeisen und den zentralen Taktgenerator synchronisieren. Die Einstellung, welche Sätze als Referenztaktlieferanten in Frage kommen und die Abfrage, welcher Lieferant gerade aktiv ist, wird über den AMO REFTA durchgeführt.

Access Points vom Typ AP 3300 IP, AP 3500 IP oder AP 3700 IP sind über das IP-Netzwerk asynchron angebunden. Damit kann aus den LTUs 17-99 keine Synchronisation des zentralen Taktgenerators erfolgen.

Wegen dieser asynchronen Anbindung kann auch der Access Point selber nicht vom Taktgenerator der zentralen Anlage synchronisiert werden. Deshalb sitzt auf der HG 3575 Baugruppe der Access Points ein eigener hochgenauer Taktgenerator.

Die Asynchronität der Taktgeneratoren in der OpenScape 4000 Zentrale und in den diversen Access Points ist für die Kommunikation zwischen diesen Komponenten nicht weiter störend. Die für die Sprachübertragung nötigen Jitter-Buffer gleichen problemlos auch den geringen Schlupf zwischen den Taktgeneratoren aus.

Werden in einem Access Point aber digitale Amts- oder Querverbindungssätze betrieben, so muss der lokale Taktgenerator auf den Takt des Netzwerks („Amtstakt“) synchronisiert werden.

Dazu wurde die Referenztaktverwaltung mit dem AMO REFTA erweitert. Das Grundprinzip ist einfach:

- Referenztaktquellen in den LTUs 1-15 werden zur Synchronisation des zentralen Taktgenerators verwendet.
- Referenztaktquellen in den LTUs 17-99 werden zur Synchronisation der lokalen Taktgeneratoren in den jeweiligen Access Point verwendet.

In einem OpenScape 4000 System mit 83 Access Points vom Typ AP 3300 IP oder AP 3500 IP muss jetzt also die Synchronisation von 84 Taktgeneratoren verwaltet werden. Deshalb können in einem solchen System auch 84 aktive Taktlieferanten (Zentrale + 83 Access Points) vorkommen.

10.2.2.7 Laden neuer Loadware auf eine HG 3575

Für das Ladekonzept für HG 3575 und HG 3500 über HTTPS siehe „Gateways HG 3500 und HG 3575“, Kapitel 5, „Ladekonzept der Gateway-Baugruppen“.

Die Loadware für eine HG 3575 ist sehr umfangreich. Wird beim Laden der Baugruppe festgestellt, dass die im Flash-Speicher der Baugruppe vorhandene Loadware nicht der auf der Festplatte der OpenScape 4000 Zentrale abgelegten entspricht, wird die Loadware neu auf die HG 3575 geladen.

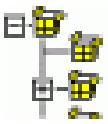
Das Laden erfolgt über FTP-Push (wenn nicht explizit die Ladefunktionen über https genutzt worden sind, z.B. Laden über LW Update Manager), wobei die HG 3575 sich die Loadware beim FTP-Server des HiPath 4000 Zentralprozessors (im RMX-System) abholt.

Der FTP-Server kann gleichzetig nur bis zu fünf HG 3575 Baugruppen laden. Sind also viele HG 3575 im System (maximal 83 Access Points möglich), so warten die anderen Baugruppen im Falle eines Systemreloads, bis sie an die Reihe kommen. Das kostet relativ viel Zeit und verlangsamt den Hochlauf der Anlage deutlich.

Wichtig: Mit dem Leistungsmerkmal „AP Multicast Loading“ wird die Downtime bei Systemhochrüstungen (Systemreload mit neuer Software-/Loadware-Version) verringert. Weitere Informationen siehe Abschnitt 2.2.8, „Update der Loadware in einem Access Point bei RMX-Hochrüstung (Gilt für neues Fix Release/Minor Release)“.

Deshalb kann, wenn eine neue Loadware ins System gebracht wurde, eine HG 3575 im Hintergrund, d.h. im laufenden Betrieb mit neuer Loadware versorgt werden. Hierfür sollte der Lowadware Update Manager im HiPath 4000 verwendet werden (siehe „Gateways HG 3500 und HG 3575“, Abschnitt 5.5, „Update der Loadware mit Hilfe des „LW Update Manager““).

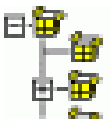
Als Alternative kann die Loadware auch weiterhin im laufenden Betrieb mittels FTP-Push übertragen werden, ohne sie allerdings sofort auszuführen. Derartige Aktionen sollten in der verkehrsschwachen Zeit ausgeführt werden, da der Loadware-Transfer die Bandbreite für Signalisierungsmeldungen reduziert. Das Laden ist auch bei Signaling-Survivability möglich. Dort ist der Effekt auf die verfügbare Signalisierungsbandbreite besonders kritisch.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** den Menüpunkt **Ausführen** wählen und den **Tätigkeitsmodus Laden der NCUI-LW-Dateien im Hintergrund** einstellen, bei **Zu ladende Dateien** die Option **LW** selektieren und mit OK bestätigen.
	`EXEC-USSU:ART=NCUILOAD,LTU=xx,FILES=LW;` Wird die LTU-Nummer nicht angegeben, werden alle HG 3575 geladen, die zu diesem Zeitpunkt dazu bereit (`READY`) sind.

Es ist auch möglich, SIU-Dateien auf diese Weise zu laden.

`FILE=`		
	`SIUTONES`	`TONES`
	`SIURECV`	`SIU-RECEIVERS`
	`SIUANN`	`SIU-ANNOUNCEMENTS`
	`SIUMOH`	`SIU -MUSIC ON HOLD`
	`SIUTDS`	`SIU -TDS`
	`LW`	`LW Datei -- NCUI`
	`ALLESIU`	`Alle möglichen SIU`
	`Alle`	**`Alle ladbaren Dateien`**

Zum Übernehmen der Loadware in den aktiven Betrieb sind folgende Aktionen notwendig:

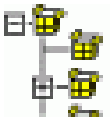
	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldown-Menü **Aktion** auf **Ausschalten** klicken. Nach der Bestätigung vom System, dass der AP ausgeschaltet wurde, mit **Aktivieren** wieder einschalten .

	`AUSSCHALTEN-USSU:LTG=1,LTU=xx;`
	
	`EINSCHALTEN-USSU:EINHEIT=LTG,LTG=1,LTU=xx;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt!

Ändern der Music-On-Hold (MOH) im System (AMO ZAND:MELODIE=x)

Beim Ändern der MELODIE-Einstellung muss folgende Kommandosequenz (je AP) ausgeführt werden, damit die Änderungen im AP sofort wirksam werden:

	**Configuration Management > Anlagendaten > IPDA** **> IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldown-Menü **Aktion** auf **Ausschalten** klicken. Nach der Bestätigung vom System, dass der AP ausgeschaltet wurde, mit **Aktivieren** wieder einschalten.

	`AUSSCHALTEN-USSU:LTG=1,LTU=xx;`
	
	`EINSCHALTEN-USSU:EINHEIT=LTG,LTG=1,LTU=xx;`

10.2.2.8 Update der Loadware in einem Access Point bei RMX-Hochrüstung (Gilt für neues Fix Release/Minor Release)

Das Leistungsmerkmal **AP Multicast Loading** ermöglicht das gleichzeitige Laden über Access Point Grenzen hinweg. Ursprünglich war das gleichzeitige Laden nur für solche Access Points möglich, bei denen die Baugruppen bereits mit der aktuellen Loadware versorgt waren. Mit „AP Multicast Laoding“ ist dieses Handling selbst dann möglich, wenn die Baugruppen neue Loadware brauchen.

Ablauf

1) Wie bisher wird mit Hilfe von FTP die neue Loadware für die HG 3575 auf die Access Points übertragen (maximal fünf Access Points pro Durchgang). Siehe auch Abschnitt 2.2.7, „Laden neuer Loadware auf eine HG 3575“.

   Nach erfolgreicher Übertragung und Aktivierung der neuen Loadware wird die TCP/IP-Verbindung zwischen Host System (HSR) und Access Point wieder hergestellt.

   Damit die im Hintergrund geladene Loadware von der NCUI übernommen wird, wird ein Warmboot initiert und ausgfeührt.

   Nach dem Neustart (Warmboot) mit der neuen Loadware erfolgt ein Golden-Loadware-Check. Sollte dieser Golden-Loadware-Check fehlschlagen, so startet die NCUI mit der alten Loadware und die neue Loadware (HD) wird erneut neu übertragen.

   Wichtig: Wenn keine neue Loadware für die HG 3575 zur Verfügung steht, entfällt dieser Schritt.

2) Die Loadware-Übertragung für die peripheren Baugruppen wird gestartet.
3) Nachdem die Loadwaren übertragen wurden, werden die Access Points in eine Ladeliste eingetragen.
4) Der erste Access Point, in der Ladeliste wird sofort komplett in Betrieb genommen (dauert ca. 15 Minuten). Während dieser Access Point in Betrieb genommen wird, werden weitere Access Points, die bereits mit dem Loadware-Transfer/Aktivierung fertig sind, in die Ladeliste eingetragen.
5) Sobald der erste Access Point in Betrieb gegangen ist, werden alle Access Points, die bis dahin in die Ladeliste eingetragen wurden, gleichzeitig geladen und in Betrieb genommen.

   Wichtig: Bisher wurden die APs in der Ladeliste sequentiell abgearbeitet bzw. in Betrieb genommen.

6) Während diese Access Points nun in Betrieb genommen werden, werden weitere Access Points, die mit dem Loadware-Transfer/Aktivierung fertig sind, in die Ladeliste eingetragen.
7) Sobald die Access Points in Betrieb genommen wurden, werden wieder alle in der Ladeliste gesammelten Access Points gleichzeitig in Betrieb genommen.
8) Diese Vorgänge werden so lange wiederholt, bis alle Access Points hochgerüstet sind.

10.2.2.9 Hinweise zum Austauschen von HG 3575 Baugruppen

Wird in einem System eine HG 3575 Baugruppe ausgetauscht, muss folgendes beachtet werden:

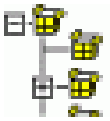
- Die HG 3575 Baugruppe darf nicht unter Spannung gezogen oder gesteckt werden.
- Die neue Baugruppe muss mit der Grundkonfiguration der alten Baugruppe eingerichtet werden (IP-Adressen etc.) Dazu kann mittels „Expertenzugang“ die Konfiguration der alten Baugruppe ausgelesen und auf Datei gespeichert - und von dort auf die neue Baugruppe gebracht werden.

Lässt die alte Baugruppe dies nicht mehr zu, müssen die Daten aus der Systemkonfiguration übernommen werden.

- Jede HG 3575 Baugruppe hat eine individuelle Ethernet MAC-Adresse. Durch Tausch der Baugruppe ändert sich die MAC-Adresse, die aus dem Netzwerk sichtbar ist.

Wichtig: Bitte informieren Sie den Netzbetreiber über die Veränderung. Dieser braucht die MAC-Adressen um bei IP-Adresskonflikten die beteiligten Geräte herauszufinden. Die MAC-Adresse der Baugruppe finden Sie auf einem Aufkleber auf der Lötseite der Leiterplatte.

- Nachdem die Baugruppe hochgelaufen ist, muss folgende AMO-Aktion ausgeführt werden:

	Das unbedingte Laden kann nur über den Expertenmodus angestoßen werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`EXEC-USSU:UPDATAP,LTU-Nummer,UL;`

Damit wird erzwungen, dass die gesamten Konfigurationsdaten vom System auf die Baugruppe geschrieben werden. Der Access Point wird dabei zurückgesetzt und läuft danach mit den aktuellen Daten hoch. Dies ist erforderlich, da das System nicht immer erkennen kann, dass die Baugruppe ausgetauscht wurde. Diese Aktion ist auch nötig, wenn dieselbe Baugruppe aus dem System genommen, lokal neu konfiguriert und wieder an gleicher Stelle ins System gebracht wurde.

Weitere Informationen zum Austausch von HG 3575-Baugruppentausch finden Sie im Dokument „Gateways HG 3500 und HG 3575“, Abschnitt 3.2.2, „Baugruppentausch“).

10.2.2.10 Hinweise zum 19" Access Point AP 3500 IP

Bild 8 „AP 3500 IP Frontansicht“ zeigt einen AP 3500 IP in Frontansicht. Der Rahmen ist mit zusätzlichen Befestigungswinkeln in 19â Gestelle montierbar und hat eine Höhe von 3HE.

Links ist Platz für 4 Baugruppen, wovon der oberste Platz von der HG 3575 (NCUI2/4) belegt wird. Auf den anderen Einbauplätzen können Peripheriebaugruppen der OpenScape 4000 eingesetzt werden. Diese Baugruppen werden durch eine separat gesteckte Metallblende abgedeckt. Auf dem Bild ist diese Blende am untersten Einbauplatz entfernt.

Auf der Rückseite können entweder die üblichen Hauptverteilerkabel aufgesteckt, oder mit Hilfe von steckbaren Patch-Panels direkt die Geräte über Western-Stecker angeschlossen werden.

Neben den Baugruppen sind übereinander 2 Stromversorgungsmodule untergebracht. Der AP 3500 IP kann mit einem Stromversorgungsmodul betrieben werden. Optional kann als Redundanz ein zweites betrieben werden.

Am rechten Rand befindet sich ein Lüftermodul. Wegen der horizontalen Baugruppenlage muss das System zwangsbelüftet werden.

Wichtig: Die Ein- und Auslassöffnungen für die Lüftung an der linken und rechten Gehäuseseite dürfen nicht abgedeckt werden. Betriebslage der Geräte ist waagrecht.

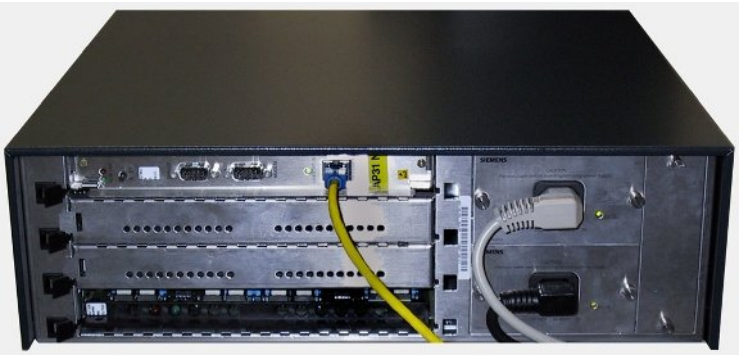


Abbildung 180: AP 3500 IP Frontansicht

Der AP 3500 IP kann durch einen gleich aufgebauten AP 3505 IP um vier Einbauplätze (keine HG 3575 im AP 3505) erweitert werden.

Besonderheiten

- Der AP 3500 IP stellt die linke, der optionale AP 3505 IP die rechte Hälfte eines konventionellen Baugruppenrahmens dar.
- Die Einbauteilungen zählen von unten nach oben, und zwar 1,2,3 und 4 im AP 3500 IP (4 ist HG 3575), sowie 5,6,7 und 8 im optionalen AP 3505 IP.
- Baugruppen mit Frontstecker können nur verwendet werden, wenn sie eine passende Metallblende haben (z.B. STMI2, DIUN2 ab Zustand -X-7, SLC24 ab Zustand -X200-9, PBXXX ab Zustand -X-F3, ...)
- SIVAPAC-Baugruppen mit Adapter werden nicht unterstützt, da sie nicht unter den Schirmdeckel passen. Als Ausnahme werden einige dieser Baugruppen mit einer neuen Plastikblende C39228-A402-C21 angepasst. (TMEW2, SLMA,TMDID,TMEMUS).

10.2.2.11 Hinweise zum 19" Access Point AP 3700 IP

Der Rahmen eines AP 3700 IP kann in 19"- Schränke eingebaut werden. Er muss dazu auf im Schrank montierte Gleitschienen/Tragschienen gestellt und mittels der mitgelieferten 19" Einbauwinkel an den Schrankholmen arretiert werden.

Der AP 3700 IP benötigt eine Höhe von 11 HE (10 HE + 1 HE Freiraum).

Wichtig: Der AP 3700 IP ist nicht zwangsbelüftet, er enthält also keine Lüfter. Bei der Aufstellung müssen die Anforderungen

an Luftzufuhr und Mindestluftdurchsatz in der Montageanleitung genau beachtet werden.

Die linke Shelf-Hälfte bietet Platz für fünf Peripherie-Baugruppen (Einbauteilung 1 .. 5). Auf dem zentralen Steckplatz (Einbauteilung 6) wird die HG 3575-2 (NCUI2) unterstützt. Die rechte Shelf-Hälfte bietet Platz für vier Peripherie-Baugruppen (Einbauteilung 7 .. 10).

Die Peripherie-Baugruppen werden, wenn sie nicht bereits mit einer passenden Metallblende ausgestattet sind (z. B. STMI2, Einbauplätze 4 und 9), durch eine separat gesteckte Metallblende abgedeckt (im Bild auf Einbauteilung 1 und 2). Nicht genutzte Einbauteilungen müssen mit Metallblende abgedeckt werden und die erforderliche Abschirmung sicherzustellen.

Baugruppen mit Frontstecker können nur verwendet werden, wenn sie eine passende Metallblende haben (z.B. STMI2, DIUN2 ab Zustand -X-7, SLC24 ab Zustand -X200-9, PBXXX ab Zustand -X-F3, ...)

SIVAPAC-Baugruppen mit Adapter werden nicht unterstützt, da sie nicht unter den Schirmdeckel passen. Als Ausnahme werden einige dieser Baugruppen mit einer neuen Plastikblende C39228-A402-C21 angepasst. (TMEW2, SLMA,TMDID,TMEMUS).

Der Projektierungsleitfaden ist also bezüglich der einsetzbaren Peripheriebaugruppen genau zu beachten.

Auf der Rückseite können entweder die üblichen Hauptverteilerkabel aufgesteckt, oder mit Hilfe von steckbaren Patch-Panels direkt die Geräte über Western-Stecker angeschlossen werden.

Unterhalb der Baugruppen können nebeneinander je nach Bedarf bis zu drei Stromversorgungsmodule gesteckt werden. Zwei Module sind für die Versorgung des Maximalausbaus ausreichend. Als Redundanz kann zusätzlich ein drittes Modul gesteckt werden.

Die Anschaltung der Stromversorgungsmodule kann an 115/230 V Wechselstrom oder 48 V Gleichstrom erfolgen. Die Speisung der bis zu drei Module erfolgt über einen gemeinsamen Stecker an der Gehäuse-Rückseite.

Im rechten Teil des AP 3700 IP ist Platz für eine Survivability Unit, eine cPCI Kassette mit einer eigenständigen Notfall-Steuerung.

10.2.3 HG 3500 als HG 3570 im OpenScape 4000 System

Mehr Informationen zum HG 3500 Gateway finden Sie im Dokument “Gateways HG 3500 und HG 3575““.

Das Common Gateway HG 3500 stellt als HG 3570 die Payload-Verbindungen zwischen dem zentralen OpenScape 4000 System und den im Rahmen der IP Distributed Architecture verteilten Access Points her.

- HG 3500 Gateways, konfiguriert als HG 3570, dürfen nur in den Peripherie-Rahmen (LTU 1-15) des zentralen Systems eingesetzt werden.
- Die von den HG 3570 Gateways eines Halb-Shelfs benötigten Time-Slots müssen blockierungsfrei zur Verfügung stehen. Die von der Baugruppen-Hardware bestimmte maximal unterstützte B-Kanalzahl lässt sich im AMO BFDAT durch den Parameter ANZBKAN auf niedrigere Werte begrenzen.
- Jeder Rahmen, in dem eine HG 3570 eingesetzt wird, muss mit einer LTUCX-Baugruppe ausgestattet sein.

- Es können bis zu 83 HG 3570 Gateways in einem OpenScape 4000 System eingesetzt werden. Die Payload-Verbindungen zwischen dem zentralen OpenScape 4000 System und den Access Points werden gleichmäßig über alle HG 3500 verteilt.
- Es gibt keinerlei Zuordnung der Payload-Verbindungen von HG 3575 zu HG 3500. Die Anzahl der HG 3500 im System orientiert sich am Verkehrsaufkommen, nicht an der Zahl der Access Points. Fällt eine HG 3500 aus, wird sie bei der Belegung neuer Gespräche ausgenommen. Eventuell vorhandene weitere HG 3500 übernehmen die Last.

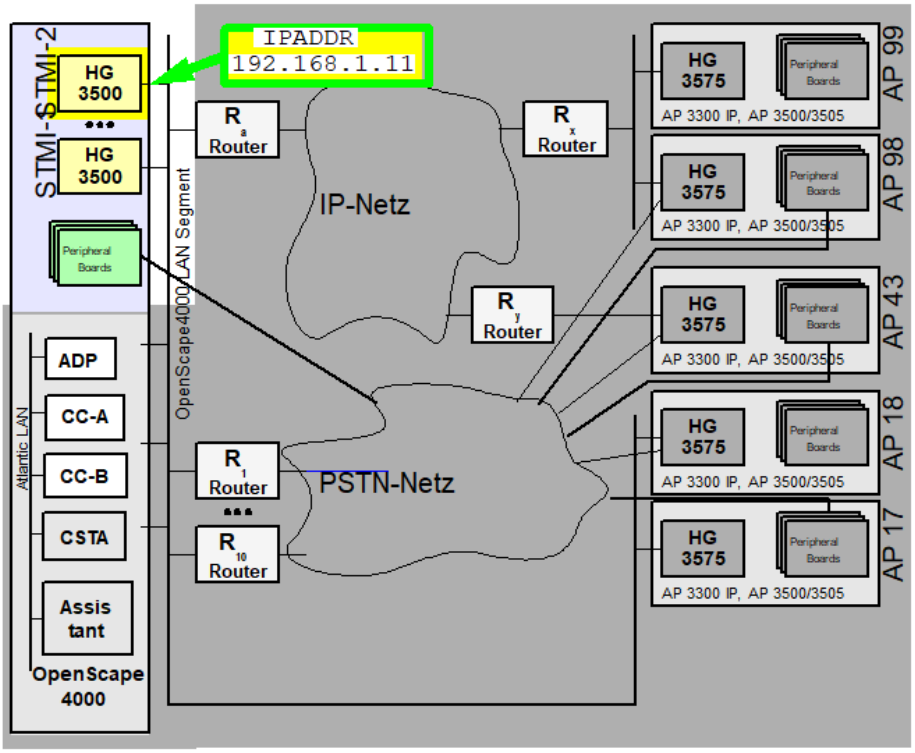


Abbildung 181: Einrichten einer HG 3500 für IPDA

EINR-BFDAT:	FCTBLK=1,	FUNCTION=HG3570,
	BGBKAN=BKAN60&BKNA120;	
AENDERN-BFDAT:	CONFIG=WEITER,	FCTBLK=1,
	FUNCTION=HG3570,	ANZBKAN=40;
AENDERN-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANTW=JA;	
EINR-BCSU:	TYP=IPGW,	LTU=5,
	EBT=91,	SACHNR=Q2316-X,
	FCTID=1,	FCTBLK=1,
	IPADR=192.168.1.11,	BKAN3570=40;
AENDERN-BCSU:	ART=HWYBDL,	LTU=5,
	EBT=91,	SACHNR=Q2316-X,
	HWYBDL=A;	

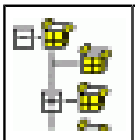
Generierung

Ein HG 3500-Modul mit **FUNCTION=HG3570** wird mit 3 AMOs konfiguriert: AMO BFDAT, AMO BCSU und AMO CGWB.

AMO CGWB wird jedoch nur benötigt, wenn zusätzlich zum Default-Router im LAN-Segment der OpenScape 4000 weitere Routen im IP-Netz benötigt werden. Siehe dazu Abschnitt 2.5, „Sonderrouten“.

BFDAT

Konfiguration der Funktionsblöcke auf dem Common Gateway für IPDA

	**Configuration Management > Systemdaten > Baugruppe > CGW-Funktionsblock** Klicken Sie auf **Neu**, geben Sie die entsprechenden Daten ein und klicken Sie auf **Sichern**.

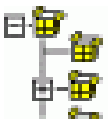
	`EINRICHTEN-BFDAT:FCTBLK=1, FUNCTION=HG3570, BGBKAN=NCHL&BKAN;`
	
	`AENDERN-BFDAT:CONFIG=WEITER, FCTBLK=1, FUNCTION=HG3570, ANZSATZ=40;`
	
	`AENDERN-BFDAT:CONFIG=OK, FCTBLK=1, ANTW=JA;`

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BFDAT	ANZBKAN	d	Anzahl der funktionsbezogenen B-Kanäle.
	BCHLCNT	e	Defines the number of b-channels related to the selected function.
	ANTW	d	JA: Block-Konfiguration abschließen
	ANSW	e	YES: Finish block configuration
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	Dedicates the block for boards with 60 and/ or 120 b-channels.
	CONFIG	d	WEITER: Weitere Block-Konfiguration möglich OK: Block-Konfiguration abschließen
	CONFIG	e	CONT: Continue block configuration OK: Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem CGW konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	FCTBLK	e	This index describes the function block which should be configured on the CGW board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNKTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die benötigte HG3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG3530, HG3540 oder HG3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion STANDBY kann nur als Einzel-Funktion konfiguriert werden.
	FUNKTION	e	This parameter defines the configuration profile of the CGW board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530, HG3540 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function STANDBY can only be configured as single function.

BCSU

Mit dem AMO BCSU wird die Baugruppe im System eingerichtet und eingeschaltet.

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Neu** klicken, Daten für (**IP-Adresse** im Abschnitt **IP-Gateway** auf der Registerkarte **STMI Baugruppendaten** eingeben und auf **Sichern** klicken.

	`EINRICHTEN-BCSU:TYP=IPGW, LTU=5, EBT=91,`
	` SACHNR=Q2316-X, FCTID=1, FCTBLK=1,`
	` IPADR=192.168.1.11, BKAN3570=40;`
	`AENDERN-BCSU:ART=HWYBDL, LTU=5, EBT=91,`
	` SACHNR=Q2316-X, HWYBDL=A;`

Wichtig: Prüfen Sie vor dem `EINRICHTEN-BCSU` die IP-Adresse, die Sie vom Netzwerkadministrator zugeteilt bekommen haben, mittels **ping** auf Erreichbarkeit. **IPADR** darf nicht erreichbar sein - sonst wird die entsprechende Adresse

bereits benutzt. **IPADR** muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
BCSU	BKAN3570	d	Anzahl der B-Kanaele fuer die IPDA (HG3570) Funktion
	BCHL3570	e	Amount of b-channels for IPDA (HG3570) function
	LTG	d	LTG-Nummer Parameter kann entfallen - oder muss auf 1 gesetzt werden.
	LTG	e	Line/Trunk Group Number Parameter can be omitted - or must be set to 1.
	LTU	d	LTU-Nummer des Rahmens, in dem die HG 3500 eingesetzt wird. Die HG 3500 darf nur in den Rahmen des OpenScape 4000 Zentralsystems (LTU 1..15) eingesetzt werden. Der Rahmen muss mit einer LTUCX Baugruppe ausgestattet sein.
	LTU	e	Line/Trunk Unit Number of the shelf where the HG 3500 is plugged. An HG 3500 may only be used in a shelf of the OpenScape 4000 central system (LTU 1..15). The shelf must be equipped with a LTUCX board.
	EBT	d	Einbauteilung des Steckplatzes der HG 3500
	SLOT	e	Slot where the HG 3500 resides.
	SACHNR	d	Sachnummer der HG 3500-Baugruppe
	PARTNO	e	Part Number of the HG 3500 Board
	FCTID	d	Function ID
	FCTID	e	Function ID
	LWVAR	d	LW Parametrisierung Wird für HG 3500 nicht benötigt. Wert sollte ausgelassen oder auf 0 gesetzt werden.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LWVAR	e	LW Parametrization Not needed for HG 3500. Parameter should be omitted or set to 0.
	IPADR	d	IP-Adresse der HG 3500 Baugruppe Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“) IPADR muss für jede Baugruppe unterschiedlich sein. Der AMO prüft nicht die Einhaltung dieser Regel.
	IPADDR	e	IP Address of the HG 3500 Board This IP address must belong to the OpenScape 4000 LAN Segment (see NETADR in AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“ auf Seite 2-670) IPADDR must be different for every board. The AMO does not check compliance with this rule.
	HWYBDL	d	Highway Bündel Die HG 3500 / STMI2/4 Baugruppe unterstützt die Wideband Technologie. Deshalb muss der Baugruppe entweder das Highway Bündel A (default) oder F zugewiesen werden.
	HWYBDL	e	Highway Bundle The HG 3500 / STMI2/4 board supports wideband technology. Thus either highway bundle A (default) or F must be assigned to this board.
	TYPE=IPGW	d	Baugruppentyp IP Gateway = Common Gateway
	MTYPE=IPGW	e	board hardware type IP gateway = common GATEWAY

10.2.4 Teilnehmersätze in Access Points

In einem über IP abgesetzten Access Point können - bis auf wenige Ausnahmen, die im Technical Upgrade Plan der OpenScape 4000 beschrieben

sind - alle Teilnehmer- und Amts-/Querverbindungsbaugruppen eingesetzt werden.

Bei Nutzung von analogen Anschlussbaugruppen, welche zusätzlich einen Rufstromgenerator benötigen, ist folgendes zu beachten:

Im 19” Access Point AP 3500 IP und der Erweiterungsbox AP 3505 IP können nur Rufstromgenerator-Module vom Typ RGM (S30807-Q6141-X bzw. S30122-K5929-X) verwendet werden, aber keine RG-Baugruppen. Die Erweiterungsbox AP 3505 IP benötigt unabhängig von der AP 3500 IP Basis-Box einen eigenen RGM, falls darin Analoganschlussbaugruppen betrieben werden.

Wichtig: Querverbindungen zwischen Access Points der selben Anlage und Querverbindungen zwischen der Zentralanlage und ihren Access Points sind nicht zulässig!

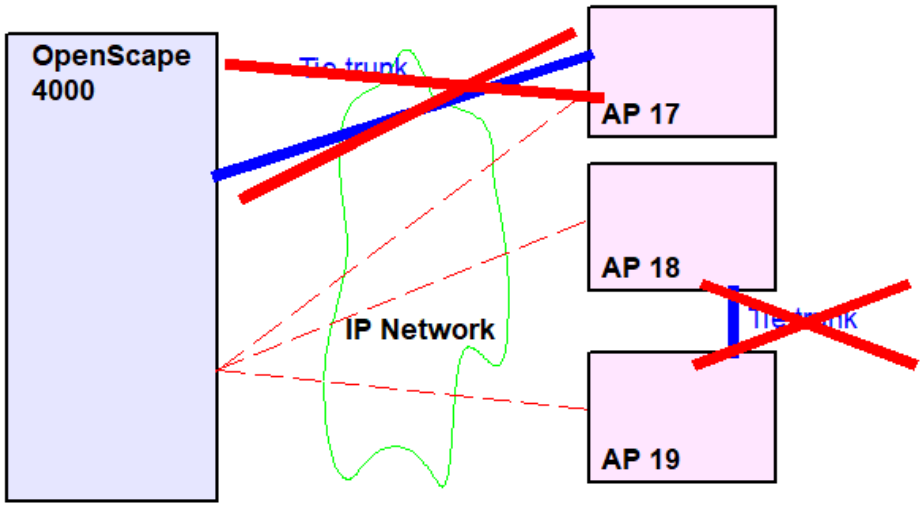


Abbildung 182: Keine Querverbindung innerhalb einer Anlage !

Mit der Konfiguration in einem über IP abgesetzten Access Point bekommen alle Sätze zusätzliche Parameter um ihre Behandlung bezüglich Voice over IP zu regeln. Diese IPDA Classmarks sind:

Tabelle 41: IPDA Classmarks

Classmark	Sprache/ Language	Beschreibung/Description
EC	d	Echo-Cancellation
EC	e	Echo-Cancellation
G711	d	Codec Typ G.711
G711	e	Codec Type G.711
G729	d	Codec Typ G.729A
G729	e	Codec Type G.729A

Classmark	Sprache/ Language	Beschreibung/Description
G729OPT	d	Codec Typ G.729A - optional
G729OPT	e	Codec Type G.729A - optional
INIT	d	stellt Default-Einstellung wieder her
INIT	e	restores default setting
KEINE	d	schaltet alle Classmarks aus
KEINER	e	turns all Classmarks off
ML	d	Multiple Listener - Ansage wird auf einer Verbindung übertragen und im Access Point an meherere Sätze geschaltet. *) nur für Ansagegeräte/MOH
ML	e	Multiple Listener - Announcement is transmitted on a single connection and switched to multiple ports in the Access Point. *) only for Announcement Devices/MOH
VAD	d	Voice Activity Detection
VAD	e	Voice Activity Detection
VIAHHS	d	Payload über Zentralsystem *) nur für Ansagegeräte/MOH
VIAHHS	e	Payload via central system *) only for Announcement Devices/MOH

Erläuterungen zu den Verfahren, welche mit den Classmarks geschaltet werden, finden Sie unter:

- Sprachkomprimierung auf Seite 64 – Abschnitt 4.2 auf Seite 4–79 im Dokument „Gateways HG 3500 und HG 3575“.
- Voice Activity Detection (VAD) auf Seite 65 – Abschnitt 4.3 auf Seite 4–81 im Dokument „Gateways HG 3500 und HG 3575“.
- Echo-Cancellation auf Seite 66– Abschnitt 4.5 auf Seite 4–82 im Dokument „Gateways HG 3500 und HG 3575“.
- Codec-Standards – Abschnitt 1.3 auf Seite 1–34 im Dokument „Gateways HG 3500 und HG 3575“.

Handhabung der Classmarks für ein Gespräch

Soll ein Gespräch zwischen Teilnehmer A und Teilnehmer B aufgebaut werden, so werden die Classmarks beider Teilnehmer, bzw. des Teilnehmers und des Amts-/Querverbindungssatzes über den der Teilnehmer erreicht wird, bewertet.

Echo Cancellation oder Voice Activity Detection werden nur dann aktiviert, wenn beide Sätze das entsprechende Classmark gesetzt haben.

Eine Ausnahme stellen Verbindungen mit Ansagegeräten dar, welche mit AMO SSC bzw. RCSU oder TSCSU eingerichtet sind. Hier wird in jedem Fall die Einstellung des Ansagegerätes übernommen.

Tabelle 42: Classmark-Behandlung bei EC oder VAD

EC bzw. VAD		Circuit B			**EC bzw. VAD**		**Ansagegerät** (RCSU)	
		NEIN	JA				NEIN	JA
Circuit A	NEIN	NEIN	NEIN		Circuit A	NEIN	NEIN	**JA**
	JA	NEIN	**JA**			JA	NEIN	**JA**

Bei den Codec-Typen wird ebenfalls nur ein Typ ausgewählt, den beide unterstützen.

Anders als in der Version 1 wird Komprimierung jetzt auch mit Ansagegeräten und bei Konferenzen unterstützt. Konferenzsätze gehen bezüglich der Codec-Classmarks entweder mit G711 (default) oder mit G711 & G729OPT in die Auswahl des Codec-Typs.

Tabelle 43: Classmark-Behandlung für Codec-Typ

Circuit A			Circuit B			Satz B
G711	G729	G729OPT	G711	G729	G729OPT	
NEIN	NEIN	NEIN	-	-	-	KEINER
NEIN	NEIN	JA	-	NEIN	JA	G.711
NEIN	JA	-	JA	NEIN	-	G.711
NEIN	JA	-	-	NEIN	JA	G.729
NEIN	JA	-	-	JA	-	G.729
JA	NEIN	NEIN	JA	-	-	G.711
JA	NEIN	JA	JA	NEIN	JA	G.711
JA	NEIN	JA	JA	JA	-	G.729
JA	NEIN	-	NEIN	JA	-	G.711
JA	JA	-	JA	NEIN	JA	G.729
JA	JA	-	JA	JA	-	G.729
JA	-	-	JA	NEIN	NEIN	G.711
-	NEIN	JA	NEIN	NEIN	JA	G.711
-	NEIN	JA	NEIN	JA	-	G.729
-	JA	-	NEIN	JA	-	G.729

Circuit A			Circuit B			Satz B
G711	G729	G729OPT	G711	G729	G729OPT	
-	-	-	NEIN	NEIN	NEIN	KEINER
- gilt unabhängig davon, ob JA oder NEIN gesetzt ist						

Generierung der Classmarks

Die Voreinstellung ist immer **EC&G711&G729OPT**.

> **Wichtig:** Die Classmark-Einstellung in den AENDERN-Zweigen der AMOs überschreibt die vor dem AMO-Aufruf vorhandene Einstellung. Soll also ein zusätzliches Classmark gesetzt werden, so muss die vorhandene Einstellung vorher abgefragt und beim AENDERN erneut mit angegeben werden.

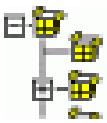
Soll eine Einstellung auf die Default-Werte zurückgeführt werden, muss der Wert INIT angegeben werden.

Sollen alle Classmarks ausgeschaltet werden, muss der Wert KEINE verwendet werden.

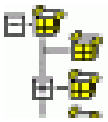
Sollen nur einzelne Classmarks ausgeschaltet werden, so müssen die zu erhaltenden Classmark beim AENDERN mit angegeben werden. Alle anderen werden automatisch gelöscht.

Beispiele:

Teilnehmer:

	**Configuration Management > Anschluss > Teilnehmeranschluss** Auf **SUCHEN** klicken und den Teilnehmer auswählen. Auf der Registerkarte **Basis 2** unter **IPDA, Merkmale für IP-Verbindungen**, die gewünschten Classmarks setzen oder löschen und auf **Speichern** klicken.
	AENDERN- SDAT:TLNNU=54321,TYP=DATEN1,CLASSMRK=KEINE; schaltet alle Classmarks aus, wie es für digitale Datenendgeräte gebraucht wird.
	AEN- SDAT:TLNNU=54321,TYP=DATEN1,CLASSMRK=EC&G711&G729; setzt die EC, G711 und G729 Classmarks. Damit wird die Verwendung des G.729-Codec erzwungen, falls der Partner G729 oder G729OPT gesetzt hat.
	AENDERN- SDAT:TLNNU=54321,TYP=DATEN1,CLASSMRK=EC&G711&G729&G729OPT&VAD schaltet die Classmarks für EC, G711, G729, G729OPT und VAD ein (also alle).

Vermittlungsplatz:

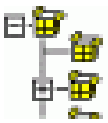
	Die Administration des Vermittlungsplatzes kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Öffnen ...**<IP> mittels AMO (siehe AMO-Befehl)
	`AENDERN-ACSU:VFNU=65432,CLASSMRK=EC&G711;` setzt die EC und G711 Classmarks. Damit werden Gespräche immer ohne Komprimierung geschaltet aber das Echo wird unterdrückt.

Ansagegeräte:

Die Voreinstellung für AMO SSC und AMO RCSU ist immer **G711&G729OPT&VIAHHS&ML**.

Die Voreinstellung für AMO TSCSU ist **EC&G711&G729OPT&VIAHHS&ML**.

Wichtig: Die Einstellmöglichkeit **G729OPT** oder gar **G729** für Ansagegeräte muss wohlüberlegt eingesetzt werden. G.729 spezifiziert ein Codec zur **Sprach**-Komprimierung. Das Codec ist zur Komprimierung von Musik völlig ungeeignet. Musik wird über G.729 extrem verzerrt wiedergegeben. Es ist in einigen Fällen erforderlich, **G729OPT** abzuschalten, insbesondere wenn Verzerrungen vermieden werden sollen und **G729** konfigurierte Sätze eingerichtet sind.

	**Configuration Management > Anschluss > Sonderteilnehmeranschluss** Auf **Suchen** klicken und den Sonderteilnehmer (**Teilnehmertyp**: **EXTANS**) auswählen. Auf der Registerkarte **Merkmale** die gewünschten Classmarks setzen oder löschen und auf **Speichern** klicken.

	`EINRICHTEN-SSC:LAGE=1-2-37-10,TYP=EXTANS, CPTON=WARTETON,CLASSMRK=G711&VIAHHS&ML;`
	oder
	`AENDERN-RCSU:LAGE=1-2-37-5,CLASSMRK=G711&VIAHHS&ML;`
	schaltet G729OPT ab und setzt dazu das G711 Classmark. Echo Cancellation wird bei Ansagegeräten nicht benötigt, da der Weg vom Teilnehmer zum Ansagegerät nicht geschaltet wird.

Wichtig: Die Classmarks **VIAHHS** und **ML** sind standardmäßig **aktiviert**. Sie dürfen nur in Ausnahmefällen ausgeschaltet werden. Vergessen Sie beim `AENDERN` nicht, die beiden Classmarks mit anzugeben, wenn sie gesetzt waren.

Wird **VIAHHS** nicht gesetzt, läuft die Verteilung von Ansagen / Music On Hold nicht mehr über das OpenScape 4000 Host System, sondern direkt von der

HG 3575, an welcher die Quelle sitzt, auf alle HG 3575, welche die Ansage benötigen.

Wird **ML** nicht gesetzt, wird für jeden Satz in einem Access Point, welcher eine Ansagen / Music On Hold benötigt, eine eigene Verbindung von der Quell-HG3575 geschaltet.

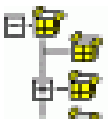
Details zum Thema Ansagen / Music-On-Hold finden Sie in Abschnitt 2.12, „Externe Music-on-Hold“.

Konferenz:

Ob komprimierte Verbindungen an Konferenzeinheiten angeschaltet werden können, wird durch einen zentralen Konfigurationsschalter systemweit einheitlich eingestellt.

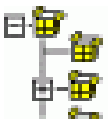
Standardmäßig werden nur unkomprimierte Verbindungen mit Konferenzeinheiten unterstützt. Das heißt, die Codec-Classmarks der Konferenzeinheiten sind auf G711 eingestellt.

Mit dem AMO ZAND kann die Einstellung auf G711 & G729OPT geändert werden.

	Die Administration der zentralen Anlagendaten kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Öffnen ...**<IP> mittels AMO (siehe AMO-Befehl)
	`AENDERN-ZAND:TYP=DATEN3,IPDAVCCF=JA;` Erlaubt komprimierte Verbindungen mit der Konferenzeinheit.

Die Änderung wird sofort, d.h. mit der nächsten Anschaltung einer IP-Verbindung an eine Konferenzeinheit wirksam.

Amts-/Querleitungen:

	**Configuration Management > Anlagendaten > Leitungssatz > Leitungssatz** Auf **Suchen** klicken und den Satz auswählen. Auf der Registerkarte **Basisdaten** die Classmarks für **IP-Verbindungen** setzen oder löschen und auf **Speichern** klicken.
	`AENDERN-TACSU:LAGE=1-1-91-1,CLASSMRK=EC&G711;` setzt die EC und G711 Classmarks. (Effektiv wurde gegenüber der Default-Einstellung G729OPT ausgeschaltet.)
	`AENDERN-TDCSU:LAGE=1-1-91-1,CLASSMRK=G711;` setzt das G711 Classmark.

Wichtig: Wird für einen ausgehenden Anruf (z. B. für Privacy Modul) die Classmark-Einstellung „**KEINE**“ temporär benötigt, so kann das über eine Kennzahl gelöst werden: AMO WABE: **NOEC**. Diese Kennzahl kann nur als Vorwahl benutzt werden.

Beispiel

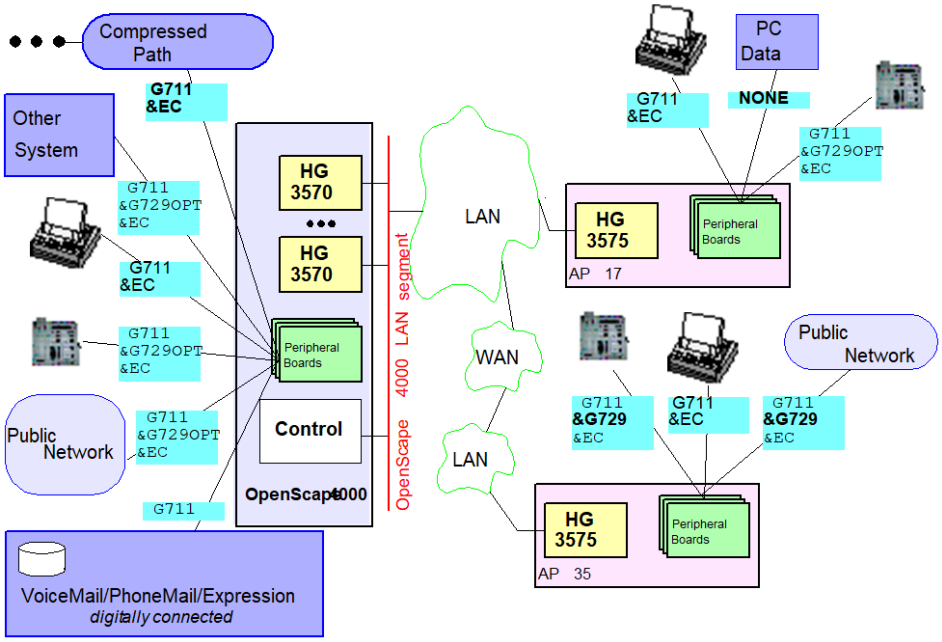


Abbildung 183: Classmarks

Das Beispiel in Abb. 20 „Classmarks“ soll die Einstellung der Classmarks für unterschiedliche Sätze illustrieren.

Standard ist G711&G729OPT&EC.

In der Zentralanlage wird davon abgewichen beim Fax, dessen Signal unkomprimiert übertragen werden muss, bei der komprimierten Querverbindungsstrecke und beim digital angeschalteten VoiceMail/ PhoneMail/Expression-Server. Werden ausschließlich STMI2/4 und NCUI2/4 Baugruppen eingesetzt, so können Faxgeräte auch mit den Standard-Classmarks eingerichtet werden. Mehrfache Kompression und Expansion in Folge soll vermieden werden. Die gewählte Einstellung G711&EC stellt im Beispiel-System sicher, dass Gespräche aus der komprimierten Querverbindungsstrecke nicht noch einmal komprimiert werden. Digital angeschlossene Ansage-/Sprachaufzeichnungsgeräte erzeugen absolut kein Echo - und sie speichern die Sprache komprimiert ab. Daher wird Kompression verhindert und EC abgeschaltet.

Das Datenendgerät auf AP 17 ist auf KEINE konfiguriert, da es weder Kompression noch Echo Cancellation bzw. Dämpfung/Verstärkung verträgt. Bei korrekter Signalisierung des ISDN-Dienstes in den Bearer Capabilities erfolgt die Übertragung unabhängig von der Classmark-Einstellung immer mit Classmarks KEINE.

AP 35 ist über WAN an die Zentrale gekoppelt. Damit ist Bandbreite ein kostbares Gut - und Voice Compression soll wann immer möglich genutzt werden. Die Einstellung G711&G729&EC für Telefone und Amtsanschluss stellt sicher, dass sowohl Gespräche mit den Telefonteilnehmern in der Zentrale und AP 17 komprimiert werden, als auch Gespräche von Telefonen in der Zentrale oder AP 17 über den lokalen Amtsanschluss in AP 35.

10.2.5 Sonderrouten

Die normal üblichen Anforderungen an das Routing zwischen Access Points und HG 3500 Baugruppen im zentralen OpenScape 4000 System sind mit der bisher beschriebenen Administration voll abgedeckt. Ein Default-Router (AMO SIPCO, parameter **DEFRT**) dient den HiPath 3500 Prozessoren als Zugang zur IP-Welt außerhalb des OpenScape 4000 LAN Segments. Je ein Default Router je LAN Segment, in dem sich Access Points befinden, dient den Access Points als Brücke in andere Netzsegmente.

Zusätzliche Anforderungen können sich aber aus der Netzarchitektur beim Kunden ergeben.

Hier sind 2 Grundszenarien zu unterscheiden:

- Verbindungen zwischen LAN Segmenten, in denen sich Access Points befinden, welche nicht über die Default-Router in den jeweiligen LAN Segmenten führen.
- Verbindungen aus dem OpenScape 4000 LAN Segment in LAN Segmente, in denen sich Access Points befinden, welche nicht über den Default-Router im OpenScape 4000 LAN Segment führen.

Der Unterschied liegt darin, dass im ersten Fall nur HG 3575 Routing Tabellen betroffen sind, während im letzten Fall zusätzlich die Routing Tabellen aller HG 3500 Baugruppen, sowie die der CC-Rechner und der OpenScape 4000 Assistant betroffen sind.

Die Routing Tabellen der HG 3500 und HG 3575 erlauben (zusätzlich zur Default-Route, welche nicht in der Routing Tabelle auftaucht) die Einrichtung von 8 Routen. Diese werden durch Angabe einer Ziel-(IP)-Adresse, der zum Zielnetz gehörigen Netzmaske sowie der IP-Adresse des von der Quell-Baugruppe anzusprechenden Router-Ports eingerichtet.

Es muss darauf geachtet werden, dass

- keine doppelten Routen eingetragen werden, z.B.

192.168.23.99	,	255.255.255.0	,	192.168.22.2
192.168.23.98	,	255.255.255.0	,	192.168.22.2

  Bereits durch den ersten Eintrag wird der Weg in das gesamte Netzsegment 192.168.23.X über den Router-Port 192.168.22.2 geführt. Der zweite Eintrag würde genau das gleiche erreichen - und muss daher unterbleiben.
- das Einrichten der Route von A nach B ohne Einfluss auf die Route von B nach A bleibt. D.h. in der Regel muss in der Ziel-Baugruppe auch eine Route zurück zur Quelle eingerichtet werden, z.B.

192.168.22.43	,	255.255.255.0	,	192.168.23.2

10.2.5.1 Sonderrouten zwischen Access Points

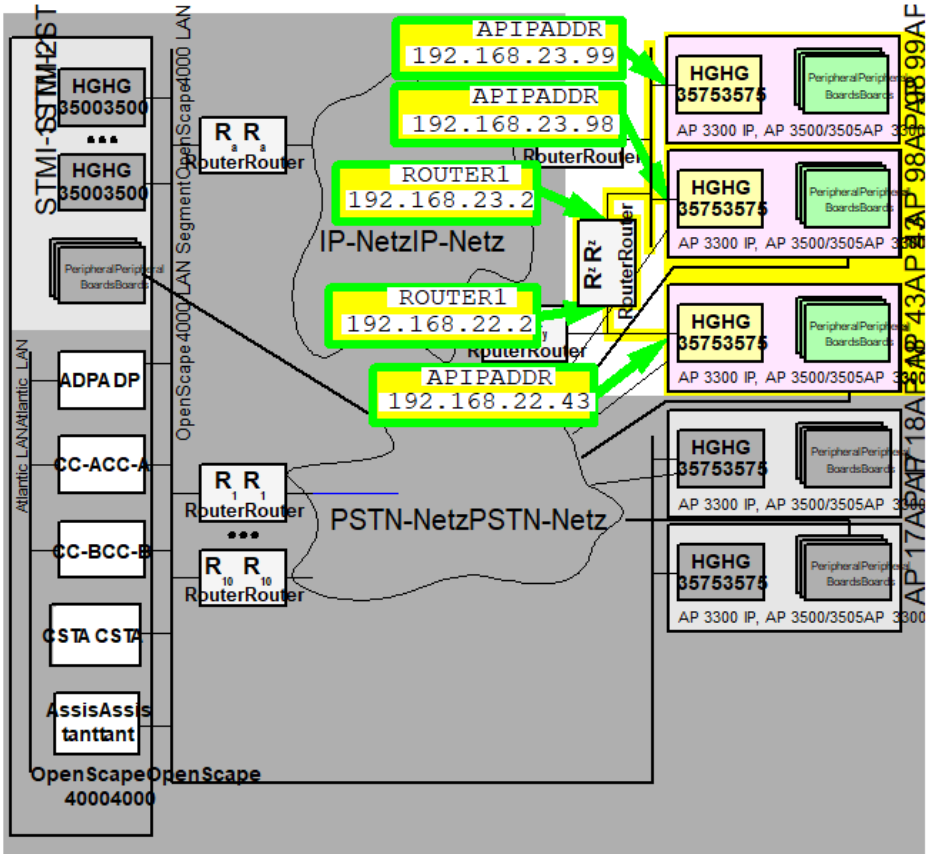
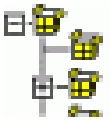


Abbildung 184: Sonderrouten zwischen Access Points

Generierung

Die Einrichtung von Sonderrouten in HG 3575 (NCUI2/4S) erfolgt mit dem AMO APRT im Zweig **ROUTTBL**.

Einrichten des in Bild 12 „Sonderrouten zwischen Access Points“ gezeigten Szenarios:

	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches Routing** Auf **Neu** klicken, wenn noch keine Einträge vorhanden sind. **LTU** eintragen. IP-Adressen der Ziele und Router sowie die Netzmasken in die Routingtabelle eingeben und auf **Sichern** klicken.

	`AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=99, DSTADR1=192.168.22.43, DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`
	Setzt den Weg von AP99 nach AP43 über Router Rz.
	`AENDERN-APRT:TYP=ROUTTBL,MTYP=NCUI,LTU=98, DSTADR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`
	Setzt den Weg von AP98 nach AP43 über Router Rz.
	`AENDERN-APRT:TYP=ROUTTBL,MTYP=NCUI,LTU=43, DSTADR1=192.168.23.99,DSTMSK1=255.255.255.0, ROUTER1=192.168.22.2;`
	Setzt den Weg von AP43 nach AP99 - **und AP98** - über Router Rz.

In diesem Beispiel wurde in allen 3 Baugruppen der erste der 8 Routing Table Einträge verwendet. Das setzt natürlich voraus, dass diese noch nicht genutzt sind.

Wären im AP43 schon die ersten 2 Einträge genutzt, wäre folgendes zu tun:

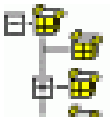
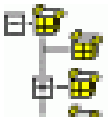
	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches Routing** Auf **Suchen** klicken und **LTU** auswählen. IP-Adressen in die Routingtabelle in Zeile 3 eingeben und auf **Sichern** klicken.
	`AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=43, DSTADR3=192.168.23.99, DSTMSK3=255.255.255.0, ROUTER3=192.168.22.2;`

Tabelle 28 „Parameter des AMO APRT im AENDERN-Zweig unter TYP=ROUTTBL“ liefert eine genaue Beschreibung der Parameter.

Soll ein **ROUTTBL**-Eintrag gelöscht werden, (z.B. der zweite Eintrag in AP43) so geschieht dies folgendermaßen:

	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches Routing** Auf **Suchen** klicken und **LTU** auswählen. IP-Adressen in der zweiten Zeile der Routingtabelle löschen und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`LOESCHEN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=43, INDEX=2;` Damit diese Änderungen im betroffenen Access Point wirksam werden, muss dieser mit `EXEC-USSU:MODE=UPDATAP, LTU=xx;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt. Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

10.2.5.2 Sonderrouten zwischen Access Point und OpenScape 4000 LAN Segment

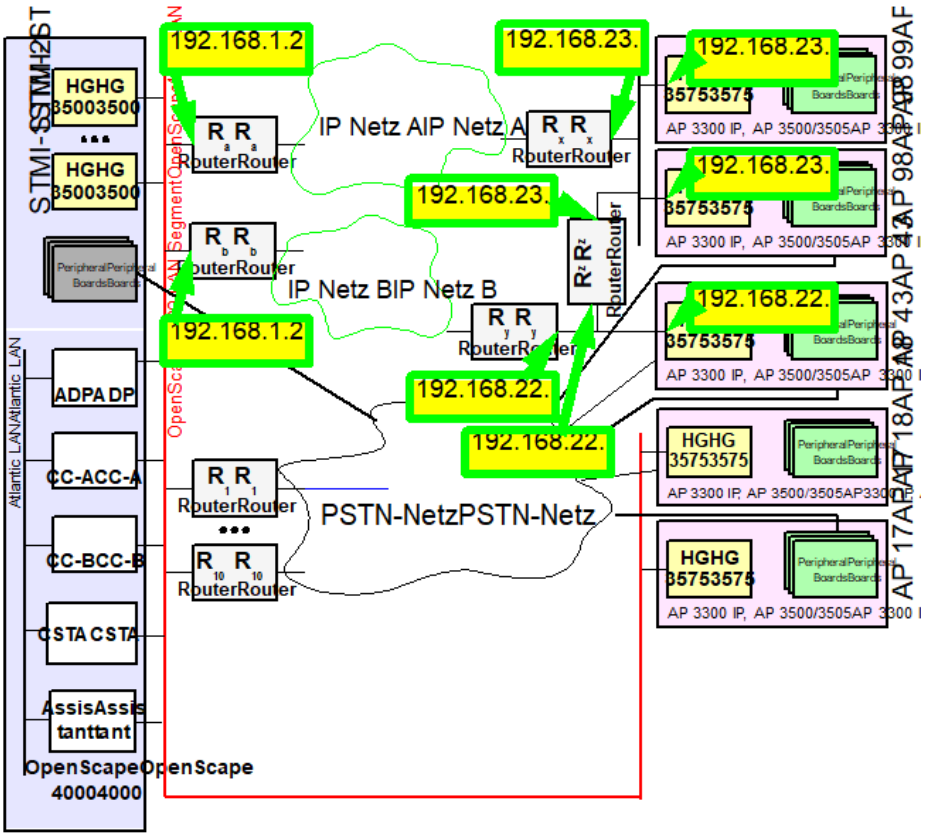


Abbildung 185: Sonderrouten zwischen Access Point und OpenScape 4000 LAN Segment

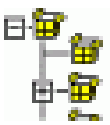
Dieser komplizierte Fall baut auf dem einfachen Fall der Sonderroute zwischen 2 Access Points auf. Zusätzlich zerfällt das IP-Netz des Kunden in diesem Fall in zwei Teilnetze, die nicht, bzw. nur über das OpenScape 4000 LAN Segment miteinander gekoppelt sind.

Dieses Szenario geht von der Annahme aus, dass die Router a, x und y die Default-Router (für OpenScape 4000 Komponenten) in den jeweiligen Netzen sind.

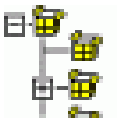
Ohne zusätzliche Routen erreichen weder die HG 3500 noch die „direct link“ Access Points AP17 und AP18 den Access Point AP 43.

Die Einrichtung des Gesamt-Szenarios läuft in folgenden Schritten ab:

- Einrichten von Router Ra als Default-Router für alle HG 3500

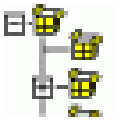
	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und Standard-Router-Adresse eingeben, dann auf **Sichern** klicken.
	`EINRICHTEN-SIPCO: ... DEFRT=192.168.1.254 ...;`

- Einrichten von Router Ra als Default-Router für AP17 und AP18

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle (DL)** Router Adresse eingeben und dann auf **Sichern** klicken.

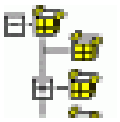
	`EINRICHTEN-UCSU:ART=AP, LTU=17, ...`
	`APRTADR=192.168.1.254 ...;`
	und
	`EINRICHTEN-UCSU:ART=AP, LTU=18, ...`
	`APRTADR=192.168.1.254 ...;`

- Einrichten von Router Rx als Default-Router für AP98 und AP99 und Festlegen von Router Ra als Weg für die Signalisierungsmeldungen des CC-A bzw. CC-B

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle (NW)** die Router-Adressen eingeben und dann auf **Sichern** klicken.

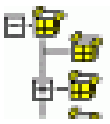
	`EINRICHTEN-UCSU:ART=AP, LTU=98, ...`
	`LSRTADR=192.168.1.254, APRTADR=192.168.23.1 ...;`
	und
	`EINRICHTEN-UCSU:ART=AP, LTU=99, ...`
	`LSRTADR=192.168.1.254, APRTADR=192.168.23.1 ...;`

- Einrichten Router Ry als Default-Router für AP43 und Festlegen von Router Rb als Weg für die Signalisierungsmeldungen des CC-A bzw. CC-B

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle (NW)** die Router-Adressen eingeben und dann auf **Sichern** klicken.
	`EINRICHTEN-UCSU:ART=AP, LTU=43, ...` `LSRTADR=192.168.1.253, APRTADR=192.168.22.1 ...;`

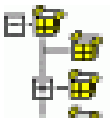
Die Payload zwischen AP43 und AP98/AP99 würde jetzt über Router Ry -> Router Rb -> Router Ra -> Router Rx gehen. Die Abkürzung über Router Rz wird, wie im vorigen Beispiel, eingerichtet durch:

- Setzen der Wege von AP43 nach AP98/AP99 über Router Rz

	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches** **Routing** Auf **Suchen** klicken, den Access Point auswählen und IP-Adressen eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=43, DSTADR1=192.168.23.99, DSTMSK1=255.255.255.0, ROUTER1=192.168.22.2;`

Für den Weg der Payload von AP98/AP99 nach AP43 müssen ebenfalls Sonderrouten eingerichtet werden:

- Setzen der Wege von AP98/AP99 nach AP43 über Router Rz

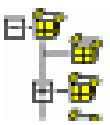
	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches** **Routing** Auf **Suchen** klicken, den Access Point auswählen und IP-Adressen eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=98, DSTADR1=192.168.22.43, DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;` `AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI, LTU=99, DSTADR1=192.168.22.43, DSTMSK1=255.255.255.0, ROUTER1=192.168.23.2;`

Die Payload von den HG 3500 zu AP98/AP99 führt über den Default-Router Ra. Der Weg ist bereits mit dem EINRICHTEN-SIPCO festgelegt.

Die Payload von AP98/AP99 zu den HG 3500 führt über den Default-Router Rx. Der Weg ist bereits mit dem EINRICHTEN-UCSU festgelegt.

Für den Payload-Transport von den HG 3500 nach AP43 fehlt jedoch die Route noch. Hier muss eine Sonderroute für alle HG 3500 (STMI2/4) über Router Rb eingerichtet werden:

- Setzen des Weges aus den HG 3500 nach AP43 über Router Rb

	**Configuration Management > Anlagendaten > IPDA > HG3570 zusätzliches** **Routing** Auf **Suchen** klicken und Netzmaske, Ziel- und Router-Adressen eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-APRT:TYP=ROUTTBL, MTYP=STMI, DSTADR1=192.168.22.43,DSTMSK1=255.255.255.0, ROUTER1=192.168.1.253;`

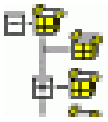
Die Payload von AP43 zu den HG 3500 führt über den Default-Router Ry. Der Weg ist bereits mit dem EINRICHTEN-UCSU festgelegt.

Die Payload zwischen den HG 3500 und den „direct link“ Access Points AP17/AP18 und zurück bleibt innerhalb des OpenScape 4000 LAN Segments und benötigt keine zusätzlichen Routen.

Die Payload zwischen den „direct link“ Access Points AP17/AP18 und AP98/AP99 und zurück führt über die mit EINRICHTEN-UCSU festgelegten Wege. (Ra, Rx)

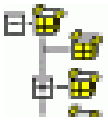
Für den Payload-Transport von den „direct link“ Access Points AP17/AP18 und AP43 fehlt jedoch die Route noch. Hier müssen Sonderrouten über Router Rb eingerichtet werden:

- Setzen der Wege aus AP17/AP18 nach AP43 über Router Rb

	**Configuration Management > Anlagendaten > IPDA > HG3575 zusätzliches** **Routing** Auf **Suchen** klicken, den Access Point auswählen und Netzmaske, Ziel- und Router-Adressen eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI.LTU=17, DSTADR1=192.168.22.43, DSTMSK1=255.255.255.0, ROUTER1=192.168.1.253;` `AENDERN-APRT:TYP=ROUTTBL, MTYP=NCUI.LTU=18, DSTADR1=192.168.22.43, DSTMSK1=255.255.255.0, ROUTER1=192.168.1.253;`

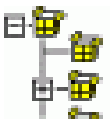
Die Payload von AP43 nach AP17/AP18 findet ihren Weg über den Default-Router Ry, es muss keine zusätzliche Route eingerichtet werden.

Damit diese Änderungen in den betroffenen Access Points wirksam werden, müssen diese neu geladen werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`EXEC-USSU:MODE=UPDATAP,LTU=xx;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt. Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

Damit diese Änderungen in den HG 3500 wirksam werden, müssen **alle** HG 3500 neu geladen werden.

	**Configuration Management > Anlagendaten > Wartung > BG-Wartung** Auf **Suchen** klicken und **STMI** auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.
	`RESTART-BSSU:ADDRTYPE=PARTNO, PARTNO=Q2316-X, FCTID=1;`

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt.

Um in diesen etwas komplexeren Szenarien den Überblick zu behalten, empfiehlt sich das Anlegen einer Kommunikationsmatrix:

Tabelle 44: Kommunikationsmatrix: Sonderrouten AP - OpenScape 4000 LAN Segmentâ

nach von	CC-A	CC-B	HG 3500	AP 17	AP 18	AP 43	AP 98	AP 99
CC-A	-	-	-	direkt	direkt	Rb	Ra	Ra
CC-B	-	-	-	direkt	direkt	Rb	Ra	Ra
HG 3500	-	-	-	direkt	direkt	Rb	Ra	Ra
AP 17	direkt	direkt	direkt	-	direkt	Rb	Ra	Ra
AP 18	direkt	direkt	direkt	direkt	-	Rb	Ra	Ra
AP 43	Ry	Ry	Ry	Ry	Ry	-	Rz	Rz
AP 98	Rx	Rx	Rx	Rx	Rx	Rz	-	direkt
AP 99	Rx	Rx	Rx	Rx	Rx	Rz	direkt	-

Tabelle 45: Parameter des AMO APRT im AENDERN-Zweig unter TYP=ROUTTBL

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	MTYP	d	Modul Typ Hier wird zwischen STMI2/4 (HG 3500) und NCUI2/4 (HG 3575) unterschieden. MTYP=STMI: Diese Routing Table gilt für alle STMI2/4 im System gleichermaßen. DSTADRx darf nicht zum OpenScape 4000 LAN Segment gehören. ROUTERx muss zum OpenScape 4000 LAN Segment gehören. (siehe NETADR im AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“) MTYP=NCUI: Diese Routing Tabelle gilt nur für die durch LTU angegebene NCUI2/4. Bei Routen zwischen 2 NCUI2/4 müssen bei beiden NCUI2/4 die entsprechenden Einträge gemacht werden!
	MTYPE	e	Modul Type This is to distinguish between STMI2/4 (HG 3500) and NCUI2/4 (HG 3575). MTYPE=STMI: This routing table is common to all the STMIs in the system. DSTADRx must not belong to the OpenScape 4000 LAN Segment. ROUTERx must belong to the OpenScape 4000 LAN Segment. (see NETADR in AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“) MTYPE=NCUI: This routing table is valid only for the NCUI2/4 assigned by LTU. For routes between 2 NCUI2/4 entries must be made for both NCUI2/4 respectively!

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DSTADR1	d	Zieladresse der 1. Route. Legt die Adresse fest, die über die im 1. Eintrag spezifizierte Route erreicht werden soll. Das kann eine Host- oder auch eine Netzadresse sein. Die DSTMSK1 erlaubt die Interpretation.
	DSTADDR1	e	Destination Address for the 1st Route. Assigns the address to be reached using the route defined in the 1. entry. It may be a host or a network address. DSTMSK1 allows the interpretation.
	DSTMSK1	d	Netzmaske des Netzes, dem DSTADR1 angehört
	DSTMSK1	e	Netmask of the network which DSTADDR1 is part of
	ROUTER1	d	IP-Adresse des Routers, über den Pakete an DSTADR1 gesendet werden sollen. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe NETADR im AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“)
	ROUTER1	e	IP Address of the Router via which Packets to DSTADDR1 are to be sent. This IP address must belong to the OpenScape 4000 LAN Segment (see NETADR in AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“)
	DSTADR2	d	Zieladresse der 2. Route.
	DSTADDR2	e	Destination Address for the 2nd Route.
	DSTMSK2	d	Netzmaske des Netzes, dem DSTADR2 angehört
	DSTMSK2	e	Netmask of the network which DSTADDR2 is part of
	ROUTER2	d	IP-Adresse des Routers, über den Pakete an DSTADR2 gesendet werden sollen.
	ROUTER2	e	IP Address of the Router via which Packets to DSTADDR2 are to be sent.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DSTADR3	d	Zieladresse der 3. Route.
	DSTADDR3	e	Destination Address for the 3rd Route.
	DSTMSK3	d	Netzmaske des Netzes, dem DSTADR3 angehört
	DSTMSK3	e	Netmask of the network which DSTADDR3 is part of
	ROUTER3	d	IP-Adresse des Routers, über den Pakete an DSTADR3 gesendet werden sollen.
	ROUTER3	e	IP Address of the Router via which Packets to DSTADDR3 are to be sent.
	DSTADR4	d	Zieladresse der 4. Route.
	DSTADDR4	e	Destination Address for the 4th Route.
	DSTMSK4	d	Netzmaske des Netzes, dem DSTADR4 angehört
	DSTMSK4	e	Netmask of the network which DSTADDR4 is part of
	ROUTER4	d	IP-Adresse des Routers, über den Pakete an DSTADR4 gesendet werden sollen.
	ROUTER4	e	IP Address of the Router via which Packets to DSTADDR4 are to be sent.
	DSTADR5	d	Zieladresse der 5. Route.
	DSTADDR5	e	Destination Address for the 5th Route.
	DSTMSK5	d	Netzmaske des Netzes, dem DSTADR5 angehört
	DSTMSK5	e	Netmask of the network which DSTADDR5 is part of
	ROUTER5	d	IP-Adresse des Routers, über den Pakete an DSTADR5 gesendet werden sollen.
	ROUTER5	e	IP Address of the Router via which Packets to DSTADDR5 are to be sent.
	DSTADR6	d	Zieladresse der 6. Route.
	DSTADDR6	e	Destination Address for the 6thRoute.
	DSTMSK6	d	Netzmaske des Netzes, dem DSTADR6 angehört

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	DSTMSK6	e	Netmask of the network which DSTADDR6 is part of
	ROUTER6	d	IP-Adresse des Routers, über den Pakete an DSTADR6 gesendet werden sollen.
	ROUTER6	e	IP Address of the Router via which Packets to DSTADDR6 are to be sent.
	DSTADR7	d	Zieladresse der 7. Route.
	DSTADDR7	e	Destination Address for the 7th Route.
	DSTMSK7	d	Netzmaske des Netzes, dem DSTADR7 angehört
	DSTMSK7	e	Netmask of the network which DSTADDR7 is part of
	ROUTER7	d	IP-Adresse des Routers, über den Pakete an DSTADR7 gesendet werden sollen.
	ROUTER7	e	IP Address of the Router via which Packets to DSTADDR7 are to be sent.
	DSTADR8	d	Zieladresse der 8. Route.
	DSTADDR8	e	Destination Address for the 8th Route.
	DSTMSK8	d	Netzmaske des Netzes, dem DSTADR8 angehört
	DSTMSK8	e	Netmask of the network which DSTADDR8 is part of
	ROUTER8	d	IP-Adresse des Routers, über den Pakete an DSTADR8 gesendet werden sollen.
	ROUTER8	e	IP Address of the Router via which Packets to DSTADDR8 are to be sent.

10.2.6 Signaling Survivability

Signaling Survivability wurde in einen eigenen Abschnitt innerhalb der IP-Lösungen verschoben:

Signaling Survivability

10.2.7 Qualitätsüberwachung für die Signalisierungsverbindung über IP

Wie im Abschnitt Signaling Survivability beschrieben, ist die einwandfreie Funktion der Signalisierungsverbindung unbedingte Voraussetzung für den Betrieb eines Access Points.

Das Konzept zur Überwachung der Signalisierungsverbindung prüft durch die zusätzliche Überwachungsverbindung, ob prinzipiell eine Kommunikation zwischen CC und Access Point möglich ist. Das hat den großen Vorteil, dass bei komplettem Ausfall der IP-Verbindung zwischen CC und Access Point sehr schnell reagiert und die Signaling Survivability aktiviert werden kann.

Manchmal ist aber die IP-Verbindung zwischen CC und Access Point nicht komplett unterbrochen, sondern „nur“ stark eingeschränkt. Das kann die Signalisierungsfunktion extrem beeinträchtigen, ohne dass diese Störung von der separaten Überwachungsverbindung erkannt wird.

Um diese Einschränkung aufzuheben, wird nun zusätzlich zum beschriebenen Mechanismus mit der separaten Überwachungsverbindung die Überwachungsmöglichkeit der eigentlichen Signalisierungsverbindung eingeführt.

Diese zusätzliche Funktionalität gliedert sich in fünf Komponenten:

- Begrenzung der nutzbaren Signalisierungsbandbreite (Traffic Shaping)
- Überwachung der Umlaufzeit von Signalisierungsmeldungen (Round Trip Delay)
- Überwachung des Meldungsdurchsatzes
- Erweiterte Kriterien für Signaling Survivability
- Ausgabe von statistischen Informationen zur Signalisierungsverbindung

10.2.7.1 Begrenzung der nutzbaren Signalisierungsbandbreite (Traffic Shaping)

Die Signalisierungsbandbreite zur Steuerung eines Access Points ist nicht besonders groß und sie schwankt extrem stark. Pauschal werden 64 kBit/s für die Signalisierungsverbindung gefordert. In manchen Konfigurationen reicht auch ein kleinerer Wert für die Bandbreite (z.B. 32 kBit/s) für normale Betriebsszeiten (z.B. zur Steuerung des Call Processing/Access Points) aus.

Werden aus einer vermittlungstechnischen Aktion heraus viele parallele Folgeaktionen in der Peripherie veranlasst, steigt kurzzeitig der Bandbreitebedarf stark an. Es kann sein, dass mehrere große Pakete mit Signalisierungsinformation in sehr kurzem Abstand an einen Access Point gesendet werden.

Während des Startup/der Installation eines Access Points wird ebenfalls mehr Bandbreite benötigt (z.B. für den FTP-Loadware-Transfer für die NCUI-Baugruppe und anderer periperer baugruppen). Daraus resultierend muss mindestens eine Banbreite von 64 kBit/s für TCP-Signalisierung zur Verfügung stehen/garantiert sein (die selbe Bandbreite ist über ISDN-Modem verfügbar, z.B. Signaling Survivability).

Für einen WAN-Router mit einer sehr geringen verfügbaren Bandbreite für diese Signalisierungsverbindung (z.B. 64 kBit/s) bedeutet das, dass während der Übertragung des ersten Pakets aus diesem „Burst“ bereits weitere ankommen. Es kann sein, dass im Router nicht genügend Puffer zum Zwischenspeichern der Pakete bereitsteht. Die Folge ist, dass Pakete aus

diesem „Burst“ von Router verworfen werden und später vom CC wiederholt werden müssen.

Die Begrenzung der Signalisierungsbandbreite zu einem Access Point im CC bewirkt, dass ein Burst von unmittelbar aufeinander folgenden Paketen vom CC vermieden wird. Dazu werden die Pakete verzögert gesendet und dabei in einen Abstand gebracht, der einen Pufferüberlauf im Router verhindert.

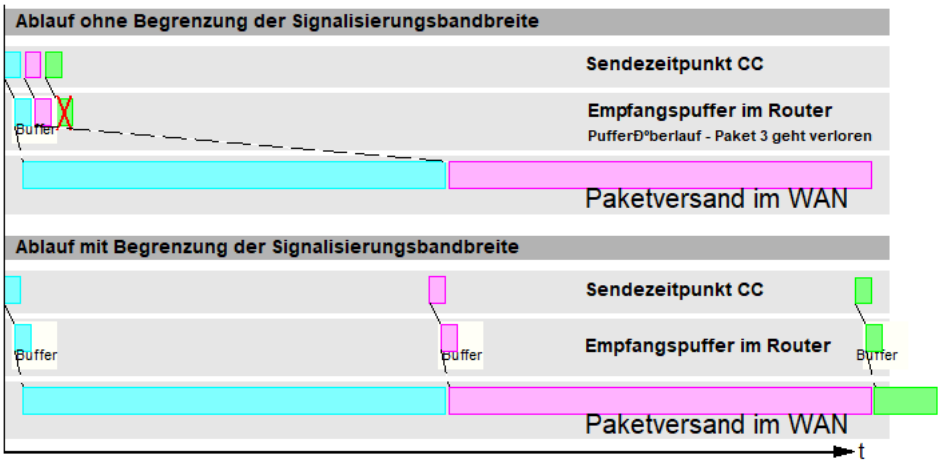


Abbildung 186: Signalisierungsverbindung ohne/mit Begrenzung der Bandbreite

---

Wichtig: Steht für die Signalisierung zu einem Access Point im IP Netz nur eine Bandbreite zwischen 64 und 250 kBit/s zur Verfügung, so muss die Begrenzung der Signalisierungsbandbreite im CC aktiviert (AMO STMIB, Parameter **SIGQOS**) und auf den im Netz verfügbaren Wert eingestellt werden.

Durch die Begrenzung der Signalisierungsbandbreite werden im CC Signalisierungsmeldungen verzögert und als Folge manchmal auch mehrere Meldungen hintereinander gestaut. Hält ein derartiger Meldungsstau über mehrere Sekunden an, so ist die konfigurierte Signalisierungsbandbreite zu gering. Das System setzt die Fehlermeldung F8292 ab (siehe Tabelle 28 „F8292 - Bandbreitebedarf übersteigt Grenzwert“), die den Beginn der Stausituation markiert. Zusätzlich kann das Auftreten eines Meldungsstaus als Kriterium für die Umschaltung des Signalisierungspfades auf den Signaling Survivability Pfad genutzt werden (siehe Abschnitt 2.7.4, „Erweiterte Kriterien für Signaling Survivability“).

Hat sich der Stau wieder aufgelöst, wird dies durch die Meldung F8293 angezeigt (siehe Abschnitt 2.7.6.5, „F8293 - Bandbreitebedarf wieder unter Grenzwert“).

Die Begrenzung der Signalisierungsbandbreite wirkt ausschließlich auf dem Signalisierungspfad über LAN. Die Modemverbindung im Falle von Signaling Survivability ist davon nicht betroffen.

Wichtig: Die krasse Unterdimensionierung der Signalisierungsbandbreite kann zu einem Meldungspuffermangel führen, der ein Rücksetzen des Access

Points zur Folge hat. Dabei werden alle Verbindungen getrennt. Sobald eine Unterdimensionierung im laufenden Betrieb festgestellt wird, gibt das System die Fehlermeldung F8292 aus (siehe Abschnitt 2.7.6.4, „F8292 - Bandbreitebedarf übersteigt Grenzwert“). Auf diese Meldung hin **muss** die aktuell im Kundennetzwerk zur Verfügung stehende Signalisierungsbandbreite erhöht werden. Werden diese Frühwarnsignale nicht beachtet, kann es zum beschriebenen Rücksetzen des Access Points oder anderen schwerwiegenden Folgen kommen. Außerdem kann eine Begrenzung der Bandbreite im TCP Verzögerungen beim Laden der Loadware und Einrichten des Rahmens/Systems verursachen!

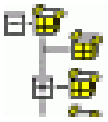
Ablauf

Zu Beginn jeder Sekunde wird ein Übertragungsguthaben in Höhe der konfigurierten Signalisierungsbandbreite zum Verbrauch bereitgestellt. Aus einer Einstellung von z.B. 64 kBit/s folgt, dass in jeder Sekunde 8000 Bytes übertragen werden dürfen. Für jedes zu sendende Paket wird nun die Paketgröße vom Guthaben abgebucht. Reicht das Guthaben nicht aus, wird das Paket so lange verzögert, bis wieder ausreichend Guthaben vorhanden ist.

Mit Ablauf der Sekunde wird das restliche Übertragungsguthaben getilgt. Die nächste Sekunde startet dann wieder mit einem neuen Guthaben in Höhe der konfigurierten Signalisierungsbandbreite, z.B. 8000 Byte. Zurückgestellte Pakete können jetzt gesendet werden.

Die Begrenzung der Übertragungsbandbreite erfolgt auf „Applikationsebene“, d.h. über dem TCP/IP-Stack.

Generierung

	**Configuration Management > Anlagendaten > IPDA > Access Point** Auf **Suchen** klicken, auf der Registerkarte **Quality of Service** im Bereich **Signaling Quality of Service** die Bandbreite eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2, TYP=SIGQOS, LTU=99, BANDW=64;`

Die Signalisierungsbandbreite wird in kBit/s angegeben. Der Wert `BANDW=0` schaltet die Begrenzung der Signalisierungsbandbreite aus (Standardkonfiguration). Die Einstellung wird sofort wirksam.

10.2.7.2 Überwachung der Umlaufzeit von Signalisierungsmeldungen (Round Trip Delay)

Ist das IP-Netzwerk gestört, so sinkt die effektiv nutzbare Bandbreite und die Zeit zwischen dem Abschicken einer Meldung und der Empfangsquittung steigt.

Für die Signalisierungsverbindung jedes Access Points kann eine maximal zulässige Meldungsumlaufzeit festgelegt werden. Diese Umlaufzeit umfasst

die gesamte Zeit vom Senden der Meldung bis zum Empfang der Quittung, also das „Round Trip Delay“. Die Auswertung der Umlaufzeit erfolgt mit jeder Signalisierungsmeldung. Die Messung ist damit unabhängig von der Signalisierungslast.

Überschreitet die Umlaufzeit den eingestellten Grenzwert, so gibt das System die Fehlermeldung F8290 aus (siehe Abschnitt 2.7.6.2, „F8290 - Beginn Netzwerkschwäche“). Zusätzlich kann die Überschreitung der maximalen Meldungsumlaufzeit als Kriterium für die Umschaltung des Signalisierungspfades auf den Signaling Survivability Pfad genutzt werden (siehe Abschnitt 2.7.4, „Erweiterte Kriterien für Signaling Survivability“).

Hat die Umlaufzeit wieder zulässige Werte angenommen, wird dies durch die Meldung F8291 angezeigt (siehe Abschnitt 2.7.6.3, „F8291 - Ende Netzwerkschwäche“).

Die Überwachung der maximalen Meldungsumlaufzeit ist ausschließlich auf dem Signalisierungspfad über LAN aktiv. Die Modemverbindung im Falle von Signaling Survivability ist davon nicht betroffen.

Ablauf

Alle drei Sekunden wird ein Mittelwert der Laufzeit aller in diesem Intervall quittierten Meldungen errechnet und gespeichert.

Aus den Drei-Sekunden-Mittelwerten werden gleitend weitere Mittelwerte über eine kurze (15 Sekunden, SHORT) und eine lange Beobachtungsdauer (60 Sekunden, LONG) gebildet.

Überschreitet einer der beiden Werte (SHORT/LONG) den konfigurierten Grenzwert, wird die Fehlermeldung erzeugt.

Eingestellt wird der Grenzwert für die lange Beobachtungsdauer (LONG). Der Grenzwert für die kurze (SHORT) wird auf den 2 fachen Wert gesetzt.

Das SHORT-Intervall mit höherem Grenzwert macht Sinn, weil so bei sprunghafter Veränderung der Netzwerkqualität schneller, d.h. bereits nach 15 Sekunden reagiert werden kann. Für eine exakte Messung kann erst nach 60 Sekunden reagiert werden.

Die Messung erfolgt auf „Applikationsebene“, d.h. über dem TCP/IP-Stack. Auf Grund der Eigendynamik im Stack können die gemessenen Werte nicht unmittelbar mit Werten in Vergleich gesetzt werden, welche direkt auf dem Netzwerk gemessen werden.

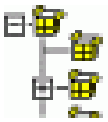
In die Laufzeit gehen ein:

- Sender eines Pakets ab TCP Ebene im OpenScape 4000 Zentralsystem
- Übertragung des Pakets im Netz
- Empfangen des Pakets auf der HG 3575 bis TCP
- Erzeugen und Senden des Acknowledge auf der HG 3575
- Übertragung des Acknowledge im Netz
- Empfangen des Acknowledge im OpenScape 4000 Zentralsystem

Da TCP die Möglichkeit hat, den Acknowledge eines Pakets zu verzögern um ihn mit dem Acknowledge eines weiteren empfangenen Pakets zu kombinieren, sind Werte unter 400 ms nicht sehr aussagekräftig.

Keep-Alive-Pakete gehen nicht in die Messung ein. Wurden innerhalb eines 3 Sekunden Intervalls keine Pakete versendet und acknowledged, wird ein vom TCP geführter langfristiger Mittelwert eingesetzt.

Generierung

	**Configuration Management > Anlagendaten > IPDA > Access Point** Auf **Suchen** klicken, auf der Registerkarte **Quality of Service** im Bereich **Signaling Quality of Service** maximale Umlaufzeit eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-STMIB:MTYP=NCUI2, TYP=SIGQOS, LTU=99, MAXRTD=500;`

Die Meldungsumlaufzeit wird dabei in ms angegeben. Der Wert `MAXRTD=0` schaltet die Überwachung der Meldungsumlaufzeit aus. Die Einstellung wird sofort wirksam.

Wichtig: Die Messung erfolgt in 10 Millisekunden-Granularität. Es macht daher nur Sinn, ohne Rest durch 10 teilbare Werte einzustellen, also z.B. 400, 410, 420 ...

10.2.7.3 Überwachung des Meldungsdurchsatzes

Für die Signalisierungsverbindung jedes Access Points kann ein minimal erforderlicher Meldungsdurchsatz festgelegt werden. Die Durchsatz-Messung umfasst das Volumen aller aus dem CC gesendeten Meldungen.

Die Unterschreitung des minimal geforderten Meldungsdurchsatzes berücksichtigt nur die Zeiten, in denen mindestens die spezifizierte Last genutzt wird. Ein Unterschreiten des minimalen Meldungsdurchsatzes, weil nicht genügend Meldungen zur Übertragung anstehen, wird ignoriert.

Unterschreitet der Durchsatz den eingestellten Grenzwert, so gibt das System die Fehlermeldung F8290 aus (siehe Abschnitt 2.7.6.2, „Meldungsdurchsatz unterschritten“). Zusätzlich kann die Unterschreitung des minimalen Meldungsdurchsatzes als Kriterium für die Umschaltung des Signalisierungspfades auf den Signaling Survivability Pfad genutzt werden (siehe Abschnitt 2.7.4, „Erweiterte Kriterien für Signaling Survivability“).

Hat der Meldungsdurchsatz wieder zulässige Werte angenommen, wird dies durch die Meldung F8291 angezeigt (siehe Abschnitt 2.7.6.3, „F8291 - Ende Netzwerkschwäche“).

Die Überwachung des minimalen Meldungsdurchsatzes ist ausschließlich auf dem Signalisierungspfad über LAN aktiv. Die Modemverbindung im Falle von Signaling Survivability ist davon nicht betroffen.

Ablauf

Alle drei Sekunden wird bilanziert, wie viele Bytes in diesem Intervall gesendet wurden. Daraus wird der Durchsatz in kBit/s errechnet. *(Gesendete Bytes * 8 / 3)*

Aus den Drei-Sekunden-Werten werden gleitend Mittelwerte über eine kurze (15 Sekunden, SHORT) und eine lange Beobachtungsdauer (60 Sekunden, LONG) gebildet.

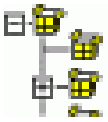
Überschreitet einer der beiden Werte (SHORT/LONG) den konfigurierten Grenzwert, wird die Fehlermeldung erzeugt.

Eingestellt wird der Grenzwert für die lange Beobachtungsdauer (LONG). Der Grenzwert für die kurze (SHORT) wird auf den 2/3 des LONG-Wert gesetzt.

Das SHORT-Intervall mit niedrigerem Grenzwert macht Sinn, weil so bei sprunghafter Veränderung der Netzwerkqualität schneller, d.h. bereits nach 15 Sekunden reagiert werden kann. Für eine exakte Messung kann erst nach 60 Sekunden reagiert werden.

Die Messung erfolgt auf „Applikationsebene“, d.h. über dem TCP/IP-Stack. Auf Grund der Eigendynamik im Stack können die gemessenen Werte nicht unmittelbar mit Werten in Vergleich gesetzt werden, welche direkt auf dem Netzwerk gemessen werden.

Generierung

	**Configuration Management > Anlagendaten > IPDA > Access Point** Auf **Suchen** klicken, auf der Registerkarte **Quality of Service** im Bereich **Signaling Quality of Service** den minimalen Meldungsdurchsatz eintragen oder ändern, dann auf **Sichern** klicken.
	AEN- `STMIB:MTYP=NCUI2,TYP=SIGQOS,LTU=99,MINTHRPT=32;`

Der minimale Meldungsdurchsatz wird dabei in kBit/s angegeben. Der Wert `MINTHRPT=0` schaltet die Überwachung des Meldungsdurchsatzes aus. Die Einstellung wird sofort wirksam.

10.2.7.4 Erweiterte Kriterien für Signaling Survivability

Die Begrenzungs- und Überwachungsfunktionen aus Abschnitt 2.7.1, „Begrenzung der nutzbaren Signalisierungsbandbreite (Traffic Shaping)“ bis Abschnitt 2.7.3, „Überwachung des Meldungsdurchsatzes“ können die Umschaltung des Signalisierungspfades von LAN auf Modem auslösen.

Welche Ereignisse zur Aktivierung der Signaling Survivability führen sollen, wird je Access Point durch Konfiguration festgelegt.

Folgende Möglichkeiten bestehen:

- Umschaltung des Signalisierungspfades auf Modem bei Verlust der Überwachungsverbindung - [STD] Im STanDard Modus wird der Signalisierungspfad auf LAN zurückgeschaltet, sobald die Überwachungsverbindung wieder stabil ist.
- Umschaltung des Signalisierungspfades auf Modem bei Verlust der Überwachungsverbindung oder bei Verletzung der Kriterien aus der Qualitätsüberwachung der Signalisierungsverbindung - [EXTENDED] Im EXTENDED Modus wird der Signalisierungspfad auf LAN zurückgeschaltet, sobald die Überwachungsverbindung wieder stabil ist und die Qualitätskriterien erfüllt werden. Zur Messung der Qualitätskriterien wird periodisch eine Last auf der Überwachungsverbindung erzeugt, welche

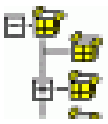
die Signalisierungsverbindung nach Rückschaltung auf LAN mindestens transportieren können muss.

Wichtig: Bei Nutzung des EXTENDED Modus muss die verfügbare Bandbreite auf dem Signalisierungspfad über Modem berücksichtigt werden. Es macht keinen Sinn auf eine 28,8 kBit/s Modemverbindung zu schalten, weil der minimale Durchsatz der LAN-Verbindung 64 kBit/s unterschreitet.

- Ausschließliche Nutzung des Signalisierungspfades auf Modem - [SURVONLY] Der SURVONLY Modus erlaubt die administrative Umschaltung des Signalisierungspfades auf Modem unabhängig von den Verhältnissen auf der LAN-Verbindung. Damit kann bei geplanten Wartungsarbeiten im LAN/WAN-Umfeld für die Zeit der Wartungsarbeit stabil umgeschaltet werden. Die Rückschaltung erfolgt dann in den STanDard- oder EXTENDED-Modus

Wichtig: Auch bei administrativer Aktivierung der Signaling Survivability für einen Access Point wird damit der Aufbau neuer Payload-Verbindungen in die OpenScape 4000 Zentrale (zu allen HG 3500) blockiert.

Generierung

	**Configuration Management > Anlagendaten > IPDA > Access Point** Auf **Suchen** klicken, auf der Registerkarte **Quality of Service** im Bereich **Signaling Quality of Service** den Umschaltemodus für Signaling Survivability auswählen, dann auf **Sichern** klicken.
	AENDERN- STMIB:MTYP=NCUI2,TYP=SIGQOS,LTU=99,SIGPTHSW=EXTENDED;

Die Einstellung wird sofort wirksam.

10.2.7.5 Ausgabe von statistischen Informationen zur Signalisierungsverbindung

Ist die Überwachung der Meldungsumlaufzeit oder des Meldungsdurchsatzes aktiv, so informiert das System nur bei Verletzung der Grenzwerte über das Ergebnis der Messungen.

Es lässt sich also nur schwer sagen, ob die konfigurierten Grenzwerte sehr knapp, oder vielleicht auch viel zu großzügig eingestellt sind.

Daher kann die zyklische Ausgabe der Messdaten auf das Betriebsterminal eingerichtet werden.

Je Access Point kann eingestellt werden, ob für diesen Access Point zyklisch Messdaten ausgegeben werden sollen, oder nicht.

Die Ausgabe der Daten erfolgt aber nur, wenn

- die Überwachung der Meldungsumlaufzeit oder des Meldungsdurchsatzes aktiviert ist
- die Ausgabe generell freigeschaltet ist (AMO-DIAGS, CC/HSR-Schalter S00)

Die Messdaten werden mit der Meldung F8289 ausgegeben

Wichtig: Die zyklische Abfrage und Ausgabe der Messdaten erzeugt eine hohe Last im System. Zudem besteht die Gefahr, dass wichtige Fehlermeldungen in der Flut der Messdaten übersehen werden. Die Ausgabe der Messdaten darf daher nur selektiv für wenige Access Points gleichzeitig genutzt werden. Die Freischaltung der Ausgabe soll nur für einen überschaubaren Zeitraum genutzt werden.

Mehr Informationen (z.B. zur Generierung) finden Sie in **Gateways HG 3500 und HG 3575 >** Abschnitt 11.11, „TYP SIGQOS - Qualitätsüberwachung für die Signalisierungsverbindung über IP“**.**

10.2.7.6 Fehlermeldungen aus der Qualitätsüberwachung für die Signalisierungsverbindung über IP

10.2.7.6.1 F8289 - Ausgabe der Statistikdaten

Wichtig: Die dargestellten Werte sind dezimal Angaben in kBit/s. Das Ziel ist es hohe Werte zu haben: dargestellter Wert >= Short Wert => gut dargestellter Wert < Short Wert => schlecht

Meldungsumlaufzeit

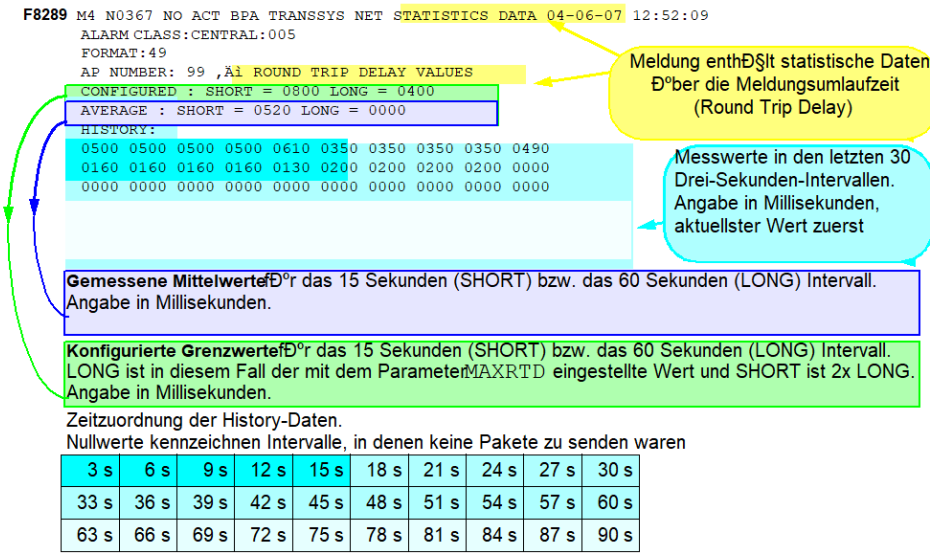


Abbildung 187: F8289 - Ausgabe der Statistikdaten über die Meldungsumlaufzeit (Round Trip Delay)

Meldungsdurchsatz

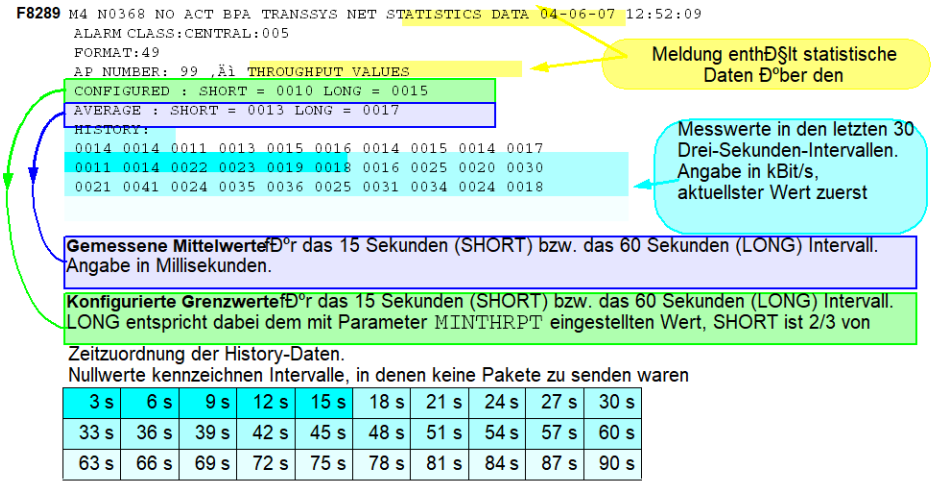


Abbildung 188: F8289 - Ausgabe der Statistikdaten über den Meldungsdurchsatz

10.2.7.6.2 F8290 - Beginn Netzwerkschwäche

Wichtig: Die dargestellten Werte sind dezimal Angaben in kBit/s. Das Ziel ist es hohe Werte zu haben: dargestellter Wert >= Short Wert => gut dargestellter Wert < Short Wert => schlecht

---

Meldungsdurchsatz überschritten

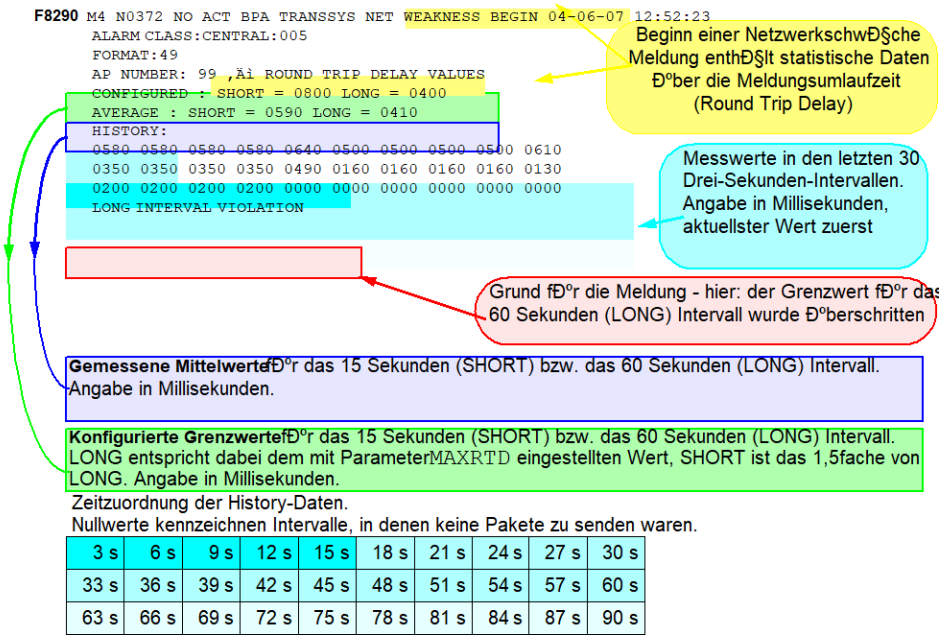


Abbildung 189: F8290 - Beginn Netzwerkschwäche (statistische Daten über die Meldungsumlaufzeit (Round Trip Delay))

Meldungsdurchsatz unterschritten

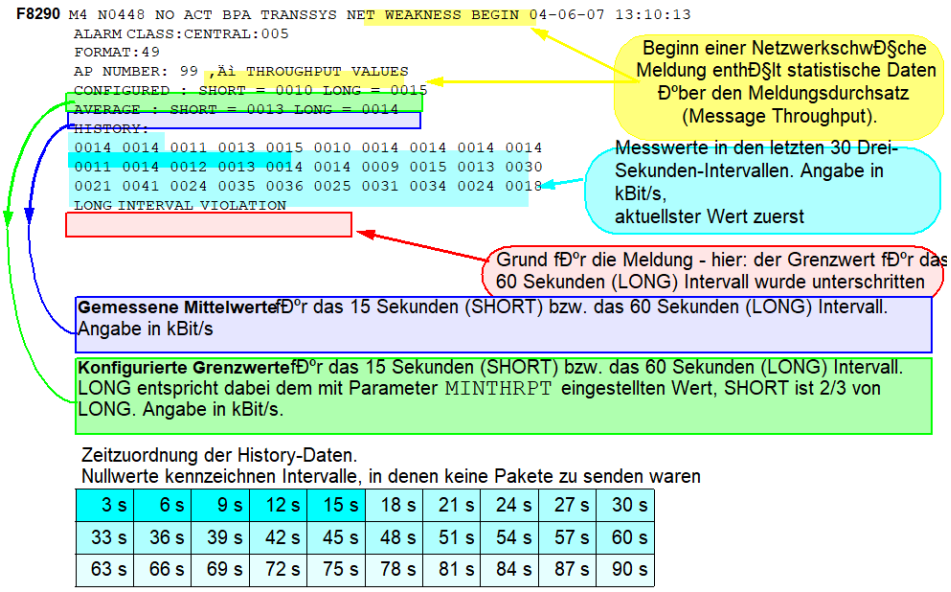
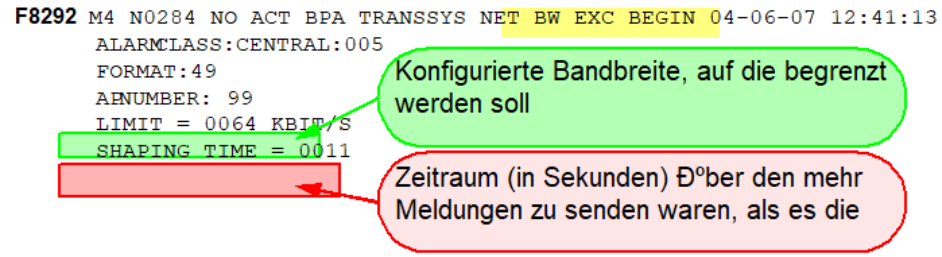


Abbildung 190: F8290 - Beginn Netzwerkschwäche (statistische Daten über den Meldungsdurchsatz)

10.2.7.6.3 F8291 - Ende Netzwerkschwäche

```
F8291 M4 N0380 NO ACT BPA TRANSSYS NET WEAKNESS END 04-06-07 13:04:05
      ALARMCLASS:CENTRAL:005
      FORMAT:49
      AP NUMBER: 99
```

10.2.7.6.4 F8292 - Bandbreitebedarf übersteigt Grenzwert



10.2.7.6.5 F8293 - Bandbreitebedarf wieder unter Grenzwert

```
F8293 M4 N0366 NO ACT BPA TRANSSYS NET BW EXC END 04-06-07 12:49:45
      ALARM CLASS:CENTRAL:005
      FORMAT:49
      AP NUMBER: 99
```

10.2.8 Source Dependent Routing

Mit IP Distributed Architecture ist es möglich, Teile eines OpenScape 4000 Systems in unterschiedlichen Ortsnetzen zu platzieren. So könnte die

OpenScape 4000 Zentrale in München stehen, Access Points davon aber in Berlin und Frankfurt.

Würde jetzt immer ein einheitliches Routing für alle Gespräche erfolgen, dann würden Gespräche aus dem Frankfurter Access Point in das Frankfurter Ortsnetz - mit LCR aus Sicht der Zentrale in München - über IP nach München und von dort als Ferngespräch nach Frankfurt geroutet. Das wäre nicht sehr kostengünstig.

Würde ein Teilnehmer am Access Point in Berlin die Feuerwehr rufen, käme er bei der Münchner Feuerwehr heraus.

Die Lösung der Probleme liegt darin, den Access Points in Berlin und Frankfurt einen Anschluss zum jeweiligen Ortsamt zu geben und dann abhängig vom Teilnehmer zu routen.

Diese „Ortsabhängigkeit“ gilt immer für mehrere Teilnehmer-, Amts- oder Querverbindungssätze. Zur Identifikation einer Gruppe, die gleiches Routing-Verhalten benötigt, wird die Source Group ID eingeführt. Jeder Access Point muss einer Source Group zugewiesen werden. Sind die Teilnehmer-, Amts- oder Querverbindungssätze mit Source Group ID „0“ eingerichtet (Default-Wert), so übernehmen sie die Einstellung des Access Points. Im Bedarfsfall kann auch eine vom Access Point abweichende Source Group ID an einzelne Teilnehmer-, Amts- oder Querverbindungssätze zugewiesen werden.

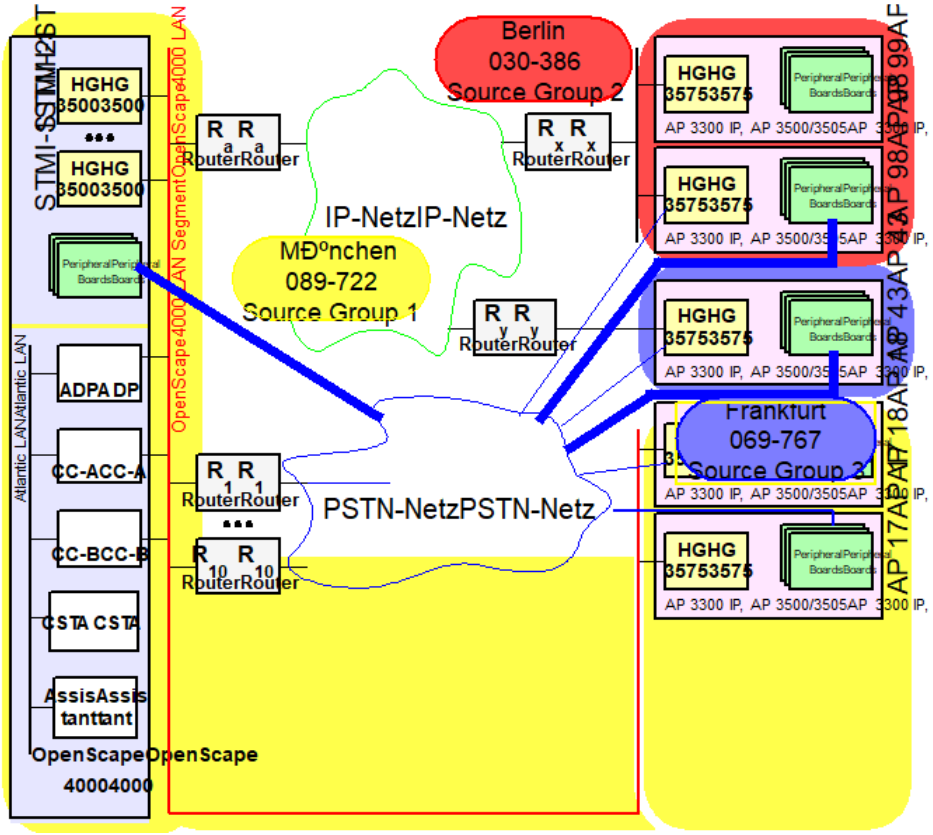


Abbildung 191: Source Dependent Routing

Im Beispiel wurden die Access Points AP 17 und AP 18 in München der Source Group 1 zugewiesen, die immer auch für alle LTUs (1..15) des zentralen OpenScape 4000 Systems voreingestellt ist. Die beiden Access Points in Berlin

(AP 98 und AP 99) wurden der Source Group 2 zugeordnet. Der Frankfurter Access Point AP 43 hat Source Group 3.

Die Nummer der Source Group wird beim EINRICHTEN-UCSU (siehe Parameter SRCGRP in Tabelle 18 „APNW: Parameter des AMO UCSU im EINRICHTEN-Zweig unter ART=AP“) als Source Group Index angegeben.

Um Source Dependent Routing realisieren zu können, musste LCR erweitert werden.

Werden im Wählmusterplan bisher mit dem AMO LDPLN für ein Wählmuster unter Berücksichtigung von WABE-Gruppen, Berechtigung etc. Richtungsnummern (LRTG) zugewiesen, so muss bei Source Dependent Routing statt der LRTG der Index eines LCR-Profils (PROFIDX) angegeben werden. In dem LCR-Profil kann dann abhängig vom Source Group Index auf eine LRTG verzweigt werden. LCR-Profile werden mit dem AMO LPROF eingerichtet.

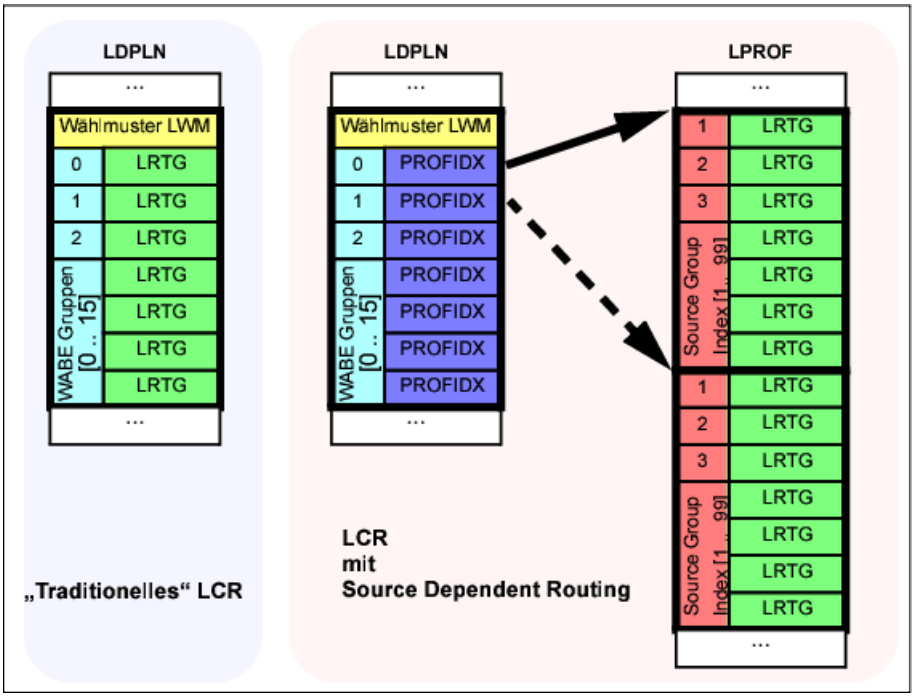
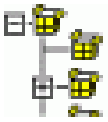


Abbildung 192: Zusammenspiel LDPLN und LPROF

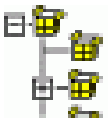
Da PROFIDX im Wählmusterplan auf ein LCR-Profil zeigt, muss dieses zuerst eingerichtet werden.

Es soll ein LCR-Profil für Notrufe zur Feuerwehr erstellt werden. In München führt LRTG 722 ins Amt, in Berlin LRTG 386 und in Frankfurt LRTG 767.

	**Configuration Management > Least Cost Routing > LCR Profile** Auf **Neu** klicken, **Profilname**, **Source Group** und **LCR-Richtung** eintragen und auf **Sichern** klicken. Der Profilindex wird ermittelt und zurückgegeben

	`EINRICHTEN-LPROF:PROFNAME=FEUERWEHR, SRCGRP=1, LRTG=722;`
	Der AMO gibt den Profil-Index zurück, angenommen er ist 12.
	Weitere Source Groups können ergänzt werden mit:
	`AENDERN-LPROF:PROFIDX=12, SRCGRP=2, LRTG=386;`
	
	`AENDERN-LPROF:PROFIDX=12, SRCGRP=3, LRTG=767;`

Als nächster Schritt kann ein Eintrag im Wählmusterplan für Notrufe zur Feuerwehr gemacht werden, der auf das eben eingerichtete LCR-Profil Nummer 12 zeigt.

	**Configuration Management > Least Cost Routing > Wählmuster** Auf **Neu** klicken, bei **Wählmuster** die Nummer**112** eintragen. Auf der Registerkarte **Daten** unter Profilindex die oben eingerichtete **LCR-Profil Nummer** eintragen und auf Sichern klicken.
	`EINRICHTEN-LDPLN:LWM=112, PROFIDX=12, ...;`

Weitere Funktionen des AMO LPROF:

	`LOESCHEN-LPROF:PROFIDX=12, SRCGRP=3;`

Löscht den Eintrag für eine Source Group aus dem angegebenen LCR-Profil. Wird keine Source Group angegeben, wird das gesamte Profil gelöscht.

	`ABFRAGEN-LPROF:PROFIDX=1&&33, INFOMUS=FEUER, FORMAT=K;`

Alle Parameter sind optional. Für **PROFIDX** kann ein bestimmter Index oder ein Bereich angegeben werden. Mit **INFOMUS** kann ein Suchmuster angegeben werden. Wird es in einem Profilnamen gefunden, wird das Profil ausgegeben. Mittels **FORMAT** kann ein gekürztes oder das lange Ausgabeformat gewählt werden.

Hinweise

- Jedem Teilnehmer-, Amts- oder Querverbindungssatz wird beim Einrichten automatisch der Source Group Index 0 zugewiesen. Das bedeutet, dass

der Source Group Index der LTU verwendet wird. Er kann aber individuell geändert werden. Es stehen maximal 99 Source Groups zur Verfügung.

- Beim Abfragen des AMOs SDAT wird der für einen Teilnehmer verwendete Source Group Index ausgegeben. Die Ausgabe `SRCGRP =(1)`besagt, dass der Teilnehmer den Source Group Index der LTU verwendet. Der Teilnehmer ist also mit `SRCGRP=0` konfiguriert. Zieht der Teilnehmer in eine LTU um, die einer anderen Source Group zugeordnet ist, wird er genau dieser Source Group zugeordnet.
- Die Ausgabe `SRCGRP = 1` besagt, dass der Teilnehmer unabhängig vom Source Group Index der LTU den Wert 1 verwendet. Der Teilnehmer ist also mit `SRCGRP=1` konfiguriert. Damit bleibt die teilnehmerspezifisch gesetzte Source Group bei einem Umzug in eine andere LTU erhalten. Es muss geprüft werden, ob diese Zuordnung noch sinnvoll ist.

Tabelle 46: Parameter des AMO LPROF

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
LPROF	FORMAT	d	Abhängig vom Parameter Format werden die Profile in einem gekürzten Format angezeigt (nur die Service Information) oder in einem langen Format (alle für LCR Profile relevanten Informationen) K - Ausgabe LCR Profile, Service Information - Kurz L - Ausgabe LCR Profile Einträge - Lang.
	FORMAT	e	According to the parameter format, the profiles are displayed in a short format (only the Service Information) or a long format (all LCR profile releated info). S - Display LCR Profile, Service information - Short L - Display of LCR Profile related info - Long
	INFOMUS	d	Bestimmt das Muster nach dem das Profil angezeigt wird. Wenn das im Parameter INFOMUS angegebene Muster im Profil Namen gefunden wird, wird das folgende Profil angezeigt.
	INFOPAT	e	Specifies the pattern according to which profiles will be displayed.If the pattern given in the INFOPAT parameter is found in the profile name, the following profile is displayed.
	LRTG	d	LCR Richtung
	LRTE	e	LCR route
	PROFIDX	d	LCR Profil-Index

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	PROFIDX	e	LCR profile index
	PROFNAMD	d	LCR Profilname
	PROFNAME	e	LCR profile name
	SRCGRP	d	Source Group Index
	SRCGRP	e	Source Group Index

10.2.9 Payload Survivability

Die IP Distributed Architecture ist prinzipbedingt von der Verfügbarkeit des IP-Netzes abhängig. Fällt die IP-Verbindung zwischen zwei Access Points oder zwischen dem zentralen OpenScape 4000 System und einem Access Point aus, so sind keine Payload-Verbindungen über IP mehr möglich.

Darüber hinaus benötigen Kunden in folgendem Szenario sehr häufig eine Trennung von Signalisierungs- und Payload-Strömen:

- Signalisierung von der Außenstelle zum Hauptsitz sollte über das IP-Netzwerk des Kunden (WAN) laufen
- Payload sollte über das herkömmliche PSTN (mit ISDN-Flatrate) laufen

Der Signalisierungsaspekt zwischen Zentrale und Access Point wird im Abschnitt 2.6, „Signaling Survivability“ behandelt.

Ist die Steuerung des Access Points durch Signaling Survivability sichergestellt, können in jedem Fall Gespräche innerhalb des Access Points geführt werden. Externe Gespräche über Amtsleitungen oder Querverbindungen in andere Anlagen sind möglich, wenn sich die entsprechenden Anschlussbaugruppen in diesem Access Point befinden.

Payload Survivability nutzt vorhandene Amtsleitungen, um unabhängig vom IP-Netz Payload-Verbindungen mit anderen Access Points oder mit der OpenScape 4000 Zentrale herzustellen. Die Anlage ruft sich hierzu über Amt selber an.

Bei Payload Survivability zwischen einem lokalen Teilnehmer und einem Amts-/Querverbindungssatz wird richtungsabhängig unterschiedlich verfahren.

Kommt der Call über den Amts-/Querverbindungssatz, so wird eine Amtsverbindung aufgebaut zwischen der Source Group, in welcher der Call hereinkommt und der Source Group, zu welcher der Teilnehmer gehört.

Baut dagegen der OpenScape 4000 Teilnehmer den Call auf, so wird dieser mittels LCR direkt über Amt aus der Anlage herausgeführt. Eine ab der Zentralanlage verfügbare Amts-/Querverbindung kann dafür nicht genutzt werden.

Die Payload Survivability ist zielorientiert und auf ein OpenScape 4000 System beschränkt. D. h., die Hardware-Gateways NCUI und STMI2/STMI4 sowie vNCUI (für SoftGate und Enterprise GW) und STMIX-Boards sind betroffen. Sind an der OpenScape 4000 weitere Anlagen angeschaltet, so muss das Networking LCR erweitert werden. Details finden sich in Abschnitt 2.9.3, „Payload Survivability in OpenScape 4000 Netzen“.

10.2.9.1 Wann wird Payload Survivability genutzt?

Es gibt folgende Gründe, Verbindungen zu Access Points statt über IP über Amtsverkehr abzuwickeln:

Die Qualität bestehender Verbindungen im IP-Netz ist schlecht

Die Kapazität der IP-Anbindung ist erschöpft

Teilnehmer bestimmt über Kennzahl, dass er nicht über IP gehen will

Payload Survivability bei aktiver Signaling Survivability

Wenn im AMO UCSU der Parameter ANZBKAN auf „0“ gesetzt wird.

Die Qualität bestehender Verbindungen im IP-Netz ist schlecht

Die Qualität der aktiven Payload-Verbindungen über das IP-Netz wird permanent überwacht.

Überschreitet die Paketverzögerung oder die Paketverlustrate voreingestellte obere Grenzwerte, wird die Verbindung als „Bad Quality“ gekennzeichnet. Unterschreiten diese Größen die ebenfalls voreingestellten unteren Grenzwerte, so wird die Verbindung wieder als „Good Quality“ gekennzeichnet. Die Grenzwerte werden im Zweig **PLQUAL** im AMO SIPCO eingestellt (siehe Abschnitt 2.1, „Payload Qualität (PLQUAL)“).

Bild 21 „Sperren der IP-Verbindung für Payload wegen „Bad Quality““ zeigt die Abläufe:

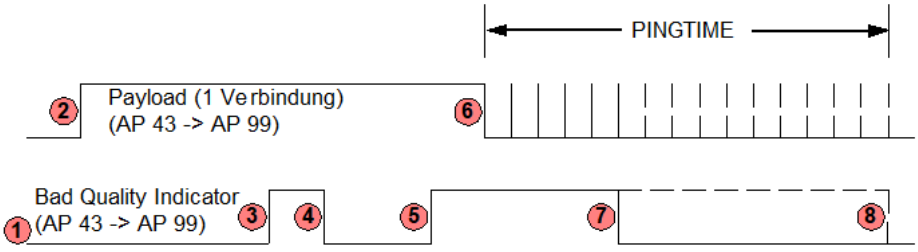


Abbildung 193: Sperren der IP-Verbindung für Payload wegen „Bad Quality“

	Zum Startpunkt der Betrachtung ist die IP-Verbindungsqualität von AP 43 nach AP 99 als gut gekennzeichnet.
	Eine Payload-Verbindung wird über IP aufgebaut.
	Die ständige Überprüfung der Verbindungsqualität meldet „Bad Quality“ Von diesem Zeitpunkt an werden keine weiteren Payload-Verbindungen zwischen AP 43 und AP 99 mehr über IP aufgebaut. Falls verfügbar, wird ein alternativer Weg über Payload- Survivability genutzt. Andernfalls wird der Verbindungswunsch abgewiesen. Die bestehende Payload-Verbindung wird trotz „Bad Quality“ nicht getrennt.

	Die ständige Überprüfung der Verbindungsqualität meldet wieder „Good Quality“ Von diesem Zeitpunkt an werden weitere Payload-Verbindungen zwischen AP 43 und AP 99 wieder über IP aufgebaut.
	wie 3
	Der Teilnehmer beendet die Payload-Verbindung Zu diesem Zeitpunkt ist „Bad Quality“ gesetzt. In Folge der vorangegangenen Payload-Verbindung werden nun alle 5 Sekunden „UDP-Ping“-Meldungen geschickt, um das Verhalten der IP-Verbindung weiter zu beobachten.
	Der Test mit „UDP-Ping“-Meldungen ergibt, dass die Verbindungsqualität wieder gut ist. Der „Bad Quality Indikator“ wird zurückgesetzt. Von diesem Zeitpunkt an werden wieder Payload-Verbindungen zwischen AP 43 und AP 99 über IP aufgebaut.
	Falls die Tests mit „UDP-Ping“-Meldungen erfolglos blieben, wird nach Ablauf der Zeitdauer **PINGTIME** der „Bad Quality Indikator“ zurückgesetzt. **PINGTIME** wird im Zweig TIMING des AMO SIPCO eingestellt. Der Wertebereich liegt zwischen 0 und 3600 Sekunden. Wichtig • Es wird empfohlen den Parameter **PINGTIME** im AMP SIPCO auf den Maximalwert 3600 (Standard: 60) zu ändern. • Die aktuelle Payload-Matrix kann mit Hilfe vom AMO SIPCO mit dem Kommando `ABFRAGEN-SIPCO:PLMATRIX;` abgefragt werden. • Die Fehlermeldungen F5915/F5750 können ebenfalls mit Hilfe des DIAGS-Schalters `AENDERN-DIAGS:,NCM;,,EIN;` aktiviert werden. REASON:01H IP GOOD QUALITY REASON:02H IP QUALITY TEST TIMER EXPIRED

Laufen mehrere Payload-Verbindungen parallel zwischen zwei Access Points bzw. zwischen Access Point und HG 3500, so können diese unterschiedliche Qualitätsaussagen liefern. Es setzt sich in jedem Fall der „Bad Quality“ Status einer Verbindung gegen beliebig viele „Good Quality“ Verbindungen durch.

Melden also 10 Verbindungen „Good Quality“ und 1 „Bad Quality“, so werden so lange keine weiteren IP-Verbindungen mehr aufgebaut, bis der Status der „Bad Quality“-Verbindung wieder „Good Quality“ wird. Möglicher Ablauf siehe Bild 21 „Sperren der IP-Verbindung für Payload wegen „Bad Quality““.

Alle Payload-Wege zwischen Zentrale (alle HG 3500 Baugruppen) und einem Access Point werden zusätzlich zum oben beschriebenen Verfahren auf „Bad Quality“ Status gesetzt, sobald für den Access Point Signaling Survivability aktiviert wird. Es wird davon ausgegangen, dass eine Störung, welche den Weg der Signalisierung zwischen Zentrale und Access Point betrifft, gleichermassen die Payload-Verbindungen beeinflußt.

Soll verhindert werden, dass wegen schlechter IP-Verbindungen („Bad Quality“) die Erreichbarkeit von Teilnehmern in einem Access Point ohne Payload Survivability gesperrt wird, so kann für den Access Point das Payload Quality Handling im AMO UCSU mit dem Parameter **PLCHECK** ausgeschaltet werden. Damit wird unabhängig von der Qualität der IP-Verbindung jedes Gespräch durchgeschaltet. Das kann im schlimmsten Fall dazu führen, dass das Gespräch signalisiert wird, die Sprachverbindung aber tot bleibt, weil keine Pakete mit Payload ankommen.

Die Kapazität der IP-Anbindung ist erschöpft

Die Transportkapazität für Payload-Verbindungen zwischen einem Access Point und dem IP-Netz ist begrenzt durch die Zahl der maximal gleichzeitig möglichen Verbindungen (HW-abhängig 30/60/120 Verbindungen) und die im Resource Manager konfigurierte maximale Bandbreite. Ist die Transportkapazität ausgeschöpft, wird für weitere Gespräche innerhalb des OpenScape 4000 Systems automatisch der Payload-Survivability-Weg genommen. Die Wegesuche unterscheidet nicht, ob kein Weg über IP verfügbar ist, weil das IP-Netz gestört ist, oder weil alle verfügbaren Wege aus dem Access Point bereits belegt sind.

Wegen der Einschränkungen bei Payload Survivability muss das System so ausgelegt werden, dass dieser Überlauf möglichst nicht, d.h. nur in seltenen Überlast-Fällen zum Einsatz kommt.

Teilnehmer bestimmt über Kennzahl, dass er nicht über IP gehen will

Im OpenScape 4000 System kann eine Kennzahl (AMO WABE: **ALTROUTE**) eingerichtet werden, mittels derer ein Teilnehmer den Survivability-Weg erzwingen kann. Die Kennzahl für **ALTROUTE** ist für jedermann nutzbar und unterliegt keiner Class Of Service! Für diese Gespräche gelten die bekannten Einschränkungen von Payload Survivability.

Payload Survivability bei aktiver Signaling Survivability

Wenn ein OpenScape 4000 SoftGate im Signaling Survivability-Modus arbeitet, werden die Verbindungen zu allen anderen APs in einer anderen Source Group als der des angegebenen OpenScape 4000 SoftGate über den alternativen Weg hergestellt.

Die Verbindung zu allen APs in derselben Source Group wie das angegebene OpenScape 4000 SoftGate wird nach Möglichkeit über LAN hergestellt. Wenn dies nicht möglich ist, kann keine Verbindung hergestellt werden.

Wie bei herkömmlichen IPDA-Rahmen wird die Funktionalität durch den Parameter **NPLMSURV** in AMO ZANDE > **DATENALL** gesteuert. Wenn dieser Parameter auf **NEIN** gesetzt ist, entspricht das der Funktionalität in Versionen vor HiPath 4000 V5. Das bedeutet: Alle Payload-Wege zwischen dem Hostsystem (alle HG 3500 Baugruppen) und einem Access Point werden zusätzlich zum oben beschriebenen Verfahren auf „Bad Quality“ Status gesetzt, sobald für den Access Point Signaling Survivability aktiviert wird. Bei alternativem Routing (aktive Signaling Survivability) wird die Payload-Matrix zwischen HHS und dem entsprechenden AP gesperrt. Alle verfügbaren Wege vom HHS zum AP sind als BAD IP gekennzeichnet.

Wenn **NPLMSURV** auf **JA** gesetzt ist, weisen die herkömmlichen IPDA-Rahmen ein erweitertes Verhalten auf, ähnlich dem des oben erwähnten Verhaltens des OpenScape 4000 SoftGate.

Dies bedeutet, dass ein IPDA-Rahmen im Signaling Survivablility-Modus eine Verbindung zum OpenScape 4000 Host System herstellt. Bei allen anderen APs, die einer anderen Source Group angehören, wird die Verbindung über den alternativen Weg hergestellt.

Andererseits wird die Verbindung zu allen APs in derselben Source Group wie das angegebene OpenScape 4000 SoftGate nach Möglichkeit über LAN hergestellt; wenn dies nicht möglich ist, kann keine Verbindung hergestellt werden.

Wichtig: Der Parameter **NPLMSURV** hat keine Auswirkung auf ein OpenScape 4000 SoftGate im Signaling Survivability-Modus. Das OpenScape 4000 SoftGate weist immer das erweiterte Verhalten auf.

Wichtig: Der Parameter **PLMSGSRV** in AMO ZANDE > **DATENALL** hat keine Auswirkung.

10.2.9.2 Wie wird Payload Survivability eingerichtet?

10.2.9.2.1 Überblick

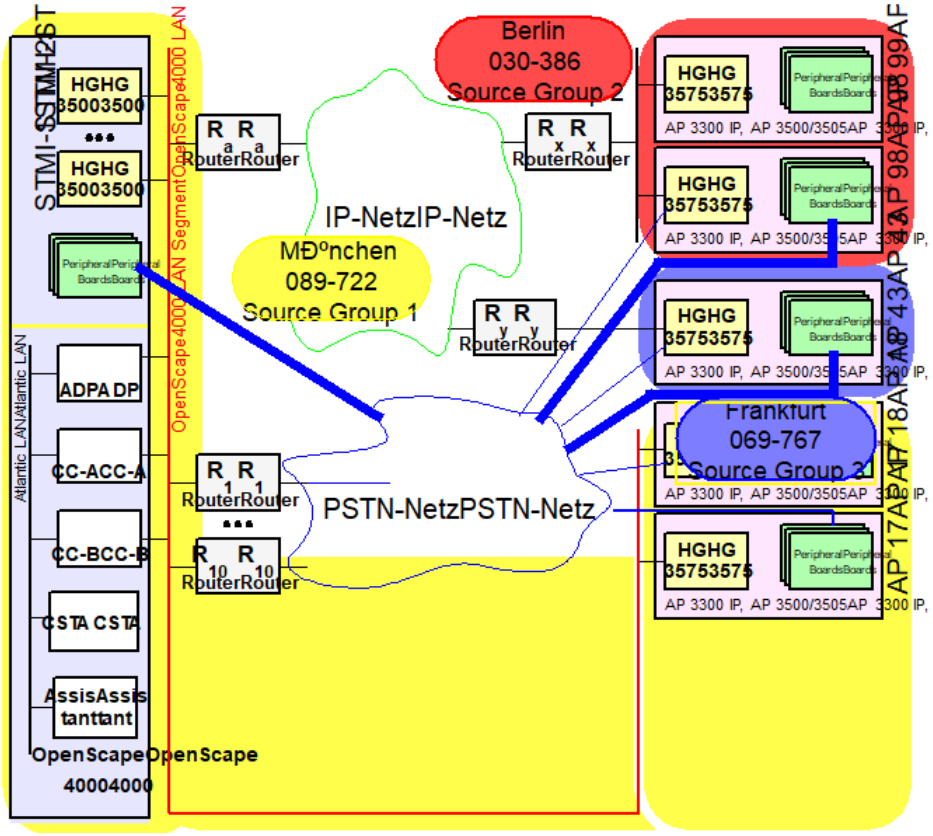


Abbildung 194: Payload Survivability - ursprungsabhängige („source-dependent“) Routing-Konfiguration

Payload Survivability braucht Amtsanschlüsse an Access Points, um Alternativwege zu schalten. Fällt in dem Beispiel in Bild 22 „Payload Survivability - ursprungsabhängige („source-dependent“) Routing-Konfiguration“ die IP-Verbindung zwischen Berlin und Frankfurt aus, so werden alle bestehenden Gespräche gestört. Neue Gespräche können erst wieder aufgebaut werden, wenn wieder „Good Quality“ festgestellt wird.

Da sowohl ein Access Point in Berlin, als auch der Access Point in Frankfurt einen lokalen Amtsanschluss haben, können Gespräche zwischen Teilnehmern in Berlin und Frankfurt alternativ über Amt geschaltet werden. Das besondere ist hier, dass sich bei IPDA jetzt eine OpenScape 4000 Anlage über Amt selber anruft, um ihre eigenen Teilnehmer zu verbinden.

Die Alternativwege werden in Abhängigkeit von der Source Group definiert. Damit ist es im Beispiel für AP 99 nicht erforderlich, einen eigenen Amtszugang zu haben. Er kann über den Amtszugang seiner Source Group in AP 98 erreicht werden.

10.2.9.2.2 Varianten der Payload Survivability

Es gibt 3 Varianten von Payload Survivability, die von der Art der Amtsanschaltung abhängen und unterschiedliche Vor- bzw. Nachteile haben. Als Standard sollte ALR verwendet werden.

ALR mit Einzelnummern	Funktioniert mit jeder Form der Amtsanschaltung, auch analog. • Jedem Kanal der Amtsanschaltung muss eine eigene Rufnummer zugewiesen werden. • Braucht dadurch viele Einzelrufnummern, viele Einträge in der **ALTROUT**-Tabelle • A-Teilnehmer sieht bei Nutzung des Payload Survivability Wegs zusätzlich zur gewählten internen Nummer auch die für den Call genutzte „Alternate Routing Number“. • B-Teilnehmer hört bei Nutzung des Payload Survivability Wegs „Amtsklingeln“ trotz des internen Calls, sieht aber die interne Rufnummer von Teilnehmer A.

ALR über mehrkanaligen Amtssatz unter einer Rufnummer	Funktioniert nur mit mehrkanaligen ISDN-Amtsanschlüssen. • Nur eine Rufnummer für alle Kanäle eines Satzes • Nur ein Eintrag in der **ALTROUT**-Tabelle je Satz • Nutzung der „Artificial Calling Number“ erfordert Vereinbarung mit dem PSTN-Netzbetreiber, dass die mitgegebene Calling Party Number nicht geprüft wird, da sie nicht der tatsächlichen Rufnummer des Satzes entspricht (USER PROVIDED SCREENED). Dies muss für alle Source Groups gleich vereinbart werden. Die Source Group, für welche ALR mit **ARTCNR** konfiguriert ist, muss von allen anderen Source Groups auf diesem Weg erreichbar sein. • Das gesamte Carrier-Netz muss die Artificial Calling Number aus allen Source Groups heraus garantiert unverfälscht transportieren. (Keine Modifizierung der Rufnummer) • Gesprächsgebühren für die Nutzung des Payload Survivability Wegs sind nicht dem Rufenden zuordenbar. • A-Teilnehmer sieht bei Nutzung des Payload Survivability Wegs zusätzlich zur gewählten internen Nummer auch die für den Call genutzte „Alternate Routing Number“. • B-Teilnehmer hört bei Nutzung des Payload Survivability Wegs „Amtsklingeln“ trotz des internen Calls, sieht aber die interne Rufnummer von Teilnehmer A.
PUBDID	Sind bereits **PUBDID**-Nummern für Teilnehmer eines Access Points konfiguriert, so können diese auch für Payload Survivability genutzt werden. • Relativ hoher Administrationsaufwand, da jedem Teilnehmer individuell die **PUBDID**-Nummer eingerichtet werden muss. • 1 Eintrag in der **ALTROUT**-Tabelle für die ganze Source Group • Die **PUBDID**-Nummer bleibt beim Umzug erhalten. • Beim Gesprächspartner wird im Falle Payload Survivability die **PUBDID**-Nummer angezeigt. • Gesprächsgebühren für die Nutzung des Payload Survivability Wegs sind dem Rufenden eindeutig zuordenbar.

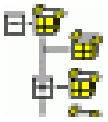
ALR mit Einzelnummern

Am Amtsanschluss, der (auch) für Payload Survivability einer Source Group genutzt werden soll, sind bestimmte Rufnummern für Payload Survivability eingerichtet.

Angenommen, in Frankfurt wären die Nummern 069-767-97, 069-767-98 und 069-767-99 für Payload Survivability reserviert. Es können dann bis zu 3 Gespräche gleichzeitig auf Alternativwegen in die Source Group 3 gelangen.

Für jeden Access Code muss in WABE der Kennzahlpunkt ALTRTKOM eingerichtet werden.

Eingerichtet wird das durch

	**Configuration Management > Anlagendaten > IPDA -- > IPDA Payload Survivability** Auf **Neu** klicken, auf der Registerkarte **Basisdaten Index**, **Routing Position**, **Rufnummer** und **Access Code** eintragen und auf **Sichern** klicken. **Configuration Management > Tabellen > Wählplan > Wählcodes** Auf **Neu** klicken und im Pulldownmenü **Bearbeiten** den Punkt **Maske löschen** auswählen. Den **Wählcode** und den **Codetyp** eintragen und auf **Sichern** klicken.

	`EINRICHTEN-APRT:TYP=ALTROUT,SRCGRP=3,POS=1,ALRTYP=ALR,ALTRTNR=006976797,ACCODE=97;`
	
	`EINRICHTEN-WABE:RNR=97,KZP=ALTRTKOM;`
	`EINRICHTEN-APRT:TYP=ALTROUT,SRCGRP=3,POS=2,ALRTYP=ALR,ALTRTNR=006976798,ACCODE=98;`
	
	`EINRICHTEN-WABE:RNR=98,KZP=ALTRTKOM;`
	`EINRICHTEN-APRT:TYP=ALTROUT,SRCGRP=3,POS=3,ALRTYP=ALR,ALTRTNR=006976799,ACCODE=99;`
	
	`EINRICHTEN-WABE:RNR=99,KZP=ALTRTKOM;`
	Durch diese Einfügereihenfolge steht der ACCODE 97 vorne in der Liste und wird zuerst belegt.

Hinweis zu ALTRTNR

Für die Alternate Routing Number **ALTRTNR** müssen bestimmte Regeln beachtet werden:

- **ALTRTNR** muss die Kennzahl für den Amtsausstieg beinhalten.
- Sind die Source Groups über unterschiedliche Ortsnetze verteilt, so muss auch die Ortsnetzkennzahl mit angegeben werden (siehe Beispiel).
- Die Kennzahl für den Amtsausstieg muss in allen Source Groups identisch eingestellt sein. Die Zielnummer muss aus allen anderen Source Groups gleichermaßen erreichbar sein!
- **ALTRTNR** darf durch LCR im gesamten Netz nicht modifiziert werden (kein REROUTE-INTERN).
- **ALTRTNR** muss in jeder Source Group „source-dependent“ geroutet werden.

Hinweis zu AMO-Parameter POS (AMO APRT:ALTROUT)

Der AMO-Parameter POS ist optional. Ohne Angabe des Parameters wird hinten angefügt. Die Tabelle wird immer kompakt ab POS = 1 gehalten. Bei Angabe eines bestimmten POS-Wertes wird der Tabelleneintrag immer nur dann auf dieser Position gemacht, wenn die Position bereits belegt oder die erste freie ist. In allen anderen Fällen wird in der Liste hinten angefügt. In allen anderen Fällen wird in der Liste hinten angefügt. Wird ein Eintrag gelöscht,

rücken alle folgenden eine Position vor. Von Bedeutung ist POS, wenn für eine Source Group mehrere Einträge gemacht werden. Die Belegung der angegebenen Alternativwege erfolgt linear steigend nach dem POS-Wert.

ALR über mehrkanaligen Amtssatz unter einer Rufnummer

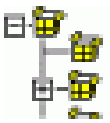
Am Amtsanschluss stehen z.B. 30 Kanäle für Payload Survivability einer Source Group zur Verfügung, die alle unter der gleichen Rufnummer erreicht werden. Das könnte z.B. in München die Nummer 089-722-9000 sein.

Für den Access Code 9000 muss in WABE der Kennzahlpunkt ALTRTKOM eingerichtet werden.

Hierüber können dann z.B. bis zu 30 Gespräche gleichzeitig auf Alternativwegen in die Source Group 1 gelangen. Da aber alle Gespräche an die gleiche Rufnummer gehen (ACCODE, AMO APRT:ALTROUT), bekommt das Call Processing das Problem, die Alternativwegsgespräche richtig zuzuordnen. Hierzu muss mit jedem Gespräch eine Identifikationszahl übertragen werden. Man ersetzt dazu die Rufnummer des Rufenden, die Calling Party Number. Welche Nummern dazu zur Verfügung stehen wird durch die Parameter ARTCNR (Artificial Calling Number) und ARTCNRG (Artificial Calling Number Bereich) eingerichtet.

Die Artificial Calling Number wird zielabhängig mit den Angaben zu einer bestimmten Source Group eingerichtet. Benutzt wird diese Nummer aber an der Quelle, d.h. am Amtszugang, der auf den Alternativweg hinausgeht. Der Wert wird schließlich als Calling Party Number eingesetzt. Da Carrier nicht beliebige, frei wählbare Calling Party Nummern erlauben, muss mit dem Carrier eine Vereinbarung über die Nutzung der Artificial Calling Numbers getroffen werden. Der Carrier muss die Überprüfung der Anrufernummer abschalten (CLIPNOSCREEN).

Einrichtebeispiel:

	**Configuration Management > Anlagendaten > IPDA -- > IPDA Payload Survivability** Auf **Neu** klicken, auf der Registerkarte **Basisdaten** alle Felder für Alternativ-Routing ausfüllen und auf **Sichern** klicken. **Configuration Management > Tabellen > Wählplan > Wählcodes** Auf **Neu** klicken und im Pulldownmenü **Bearbeiten** den Punkt **Maske löschen** auswählen. Den **Wählcode** und den **Codetyp** eintragen und auf **Sichern** klicken.
	`EINRICHTEN-APRT:TYP=ALTROUT,SRCGRP=1,ALRTYP=ALR, ALTRTNR=00897229000,ACCODE=9000,ARTCNR=1000, ARTCNRNG=30;` `EINRICHTEN-WABE:RNR=9000,KZP=ALTRTKOM;`

Hinweis zu ARTCNR

Für die Artificial Calling Number ARTCNR müssen bestimmte Regeln beachtet werden:

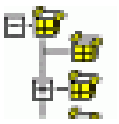
- Die ARTCNR-Bereiche für unterschiedliche Sätze und Source Groups dürfen sich nicht überlappen.

- Die Bereiche müssen groß genug sein um die gewünschte maximale Zahl von Calls über den Payload Survivability Weg an einem Satz zu ermöglichen.
- Dieser ARTCNR-Bereich muss **nicht** in der WABE reserviert werden.
- Das gesamte Carrier-Netz muss den ARTCNR-Bereich aus allen Source Groups heraus garantiert unverfälscht transportieren. (Keine Modifizierung der Rufnummer)

PUBDID

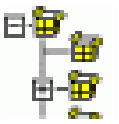
Teilnehmer einer Source Group haben eine Public DID Nummer im Ortsamt. Berliner Teilnehmer sind direkt sowohl über die Münchner Einwahl des zentralen OpenScape 4000 Systems zu erreichen, als auch über ihre Berliner Einwahlnummer. Zum Beispiel könnte ein Teilnehmer dann sowohl unter 089-722-**12345**, als auch unter 030-386-**789** erreichbar sein.

Einstellen der PUBDID-Nummer: *[TON: Type Of Number - NPI: Numbering Plan Identifier]*

	**Configuration Management > Anschluss > Teilnehmeranschluss** Auf **Suchen** klicken und zum Teilnehmer blättern. Auf der Registerkarte **Basis 3** unter **Primärmultiplexanschluss** die **Rufnummer**, **NPI** und **TON** eintragen und auf **Sichern** klicken.
	`AENDERN-SDAT:TLNNU=12345,TYP=DATEN1,PUBNUM=30386789,TON=NATIONAL,NPI=ISDN;`

Weitere Einstellungen mit den AMOs DNIT und DIDCR sind erforderlich.

Soll dieser Mechanismus für Payload Survivability genutzt werden, so wird dies eingeschaltet durch:

	**Configuration Management > Anlagendaten > IPDA -- > IPDA Payload Survivability** Auf **Neu** klicken, auf der Registerkarte **Basisdaten**, **Position** und **Art des Routings** eintragen und auf **Sichern** klicken.
	`EINR-APRT:TYP=ALTROUT,SRCGRP=2,POS=1,ALRTYP=PUBDID;`

Es kann für Source Groups mit PUBDID aber auch eines der ALR-Verfahren für Payload Survivability eingerichtet werden.

Tabelle 47: Parameter des AMO APRT im EINRICHTEN-Zweig unter TYP=ALTROUT

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
APRT	SRCGRP	d	Source Group Index Zuordnung des Access Points in eine Source Group. Die Access Points einer Source Group sind für Payload Survivability über einen bestimmten Amtsanschluss erreichbar.
	SRCGRP	e	Source Group Index Assignment of the Access Point to a Source Group. The Access Points of one Source Group are reachable via a distinct CO trunk for Payload Survivability.
	POS	d	Position Index des Eintrags in der Alternate Routing Tabelle. [1 .. 500] Siehe auch: Abschnitt 2.9.2.2, „**Hinweis zu AMO-Parameter POS (AMO APRT:ALTROUT)**“
	POS	e	Position Index of the entry in the Alternate Routing Table. [1 .. 500] See also: Abschnitt 2.9.2.2, „**Hinweis zu AMO-Parameter POS (AMO APRT:ALTROUT)**“
	ALRTYP	d	Alternate Routing Typ des Eintrags. 3 Typen sind möglich: ALR: Alternate Routing über eine DID, DIT oder PRI Nummer. NOALR: Kein Alternate Routing Pfad PUBDID: Alternate Routing über Public DID Nummer, d.h. Teilnehmer haben eine zweite Nummer, unter der sie über den Amtsanschluss für die angegebene Source Group aus dem öffentlichen Netz erreichbar sind.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ALRTYPE	e	Alternate Routing Type of the Entry 3 types are possible: ALR: Alternate Routing via a DID, DIT or PRI number. NOALR: No Alternate Routing PUBDID: Alternate Routing using a public DID number. Subscribers are reachable by a second number via the CO access for the specified Source Group.
	ALTRTNR	d	Rufnummer für Alternate Routing Vollständige Rufnummer des Alternate Routing Anschlusses Siehe auch: Abschnitt 2.9.2.2, „Hinweis zu ALTRTNR“
	ALTRTNR	e	Alternate Routing Number. Complete number of the Alternate Routing access See also: Abschnitt 2.9.2.2, „Hinweis zu ALTRTNR“
	ACCODE	d	Access Code Nebenstellennummer des Alternate Routing Anschlusses, d.h. ALTRTNR ohne Vorwahl und Amtsnummer. Maximal 6-stellig.
	ACCODE	e	Access Code Extension Number of the ALternate Routing Access. ALTRTNR without Area and Office Code. Maximum 6 digits.
	ARTCNR	d	Artificial Calling Number Maximal 6-stellige Nummer, welche zur Identifikation des Rufes als „Nummer des Rufenden“ übertragen wird. Diese Nummer ist die erste eines Bereichs (siehe ARTCNRNG), der für diese Zwecke genutzt wird. Siehe auch: Abschnitt 2.9.2.2, „Hinweis zu ARTCNR“

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	ARTCNR	e	Artificial Calling Number. A number with a maximum of 6 digits. Is given als „Calling Party Number“ to identify the call. This number is the first of a range (see ARTCNRNG) used for that purpose. See also: Abschnitt 2.9.2.2, „Hinweis zu ARTCNR“
	ARTCNRNG	d	Artificial Calling Number Bereich Gibt an, wieviele Artificial Calling Numbers einschließlich ARTCNR zur Verfügung stehen [1 .. 99999].
	ARTCNRNG	e	Artificial Calling Number Range Specifies, how many Artificial Calling Numbers including ARTCNR are available [1 .. 99999].

10.2.9.3 Payload Survivability in OpenScape 4000 Netzen

Die Payload Survivability ist zielorientiert und auf **ein** OpenScape 4000 System beschränkt. Sind an der OpenScape 4000 weitere Anlagen über ECMAV2-Querverbindungen angeschaltet (verdeckte Nummerierung), so muss das Networking LCR (NWLCR) erweitert werden. Andernfalls können AP-Teilnehmer die entsprechenden Netzteilnehmer bei aktiver Payload Survivability nicht erreichen.

Bei Payload Survivability zwischen einem lokalen Teilnehmer und einem Amts-/Querverbindungssatz wird richtungsabhängig unterschiedlich verfahren.

Kommt der Call über den Amts-/Querverbindungssatz, so wird eine Amtsverbindung aufgebaut zwischen der Source Group, in welcher der Call hereinkommt und der Source Group, zu welcher der Teilnehmer gehört.

Baut dagegen der OpenScape 4000 Teilnehmer den Call auf, so wird dieser mittels LCR direkt über Amt aus der Anlage herausgeführt. Eine ab der Zentralanlage verfügbare Querverbindung kann dafür nicht genutzt werden.

Bild 23 „Payload-Survivability und Vernetzung - Normalweg A ruft B oder B ruft A“, Bild 24 „Payload-Survivability und Vernetzung - Survivability-Weg A ruft B“ und Bild 25 „Payload-Survivability und Vernetzung - Survivability-Weg B ruft A“ zeigen die unterschiedlichen Wege.

Zur Behandlung des Rufes A -> B bei Payload Survivability (Bild 24 „Payload-Survivability und Vernetzung - Survivability-Weg A ruft B“) muss im NWLCR der Anlage 1 für die Richtung zur ZLNR 2 eine Erweiterung gemacht werden. Diese Erweiterung beinhaltet einen Überlaufeintrag ins lokale Amt des AP 17 (Bündel 17), der das Routing zur Zielanlage 2 über Amt bei Payload Survivability sicherstellt.

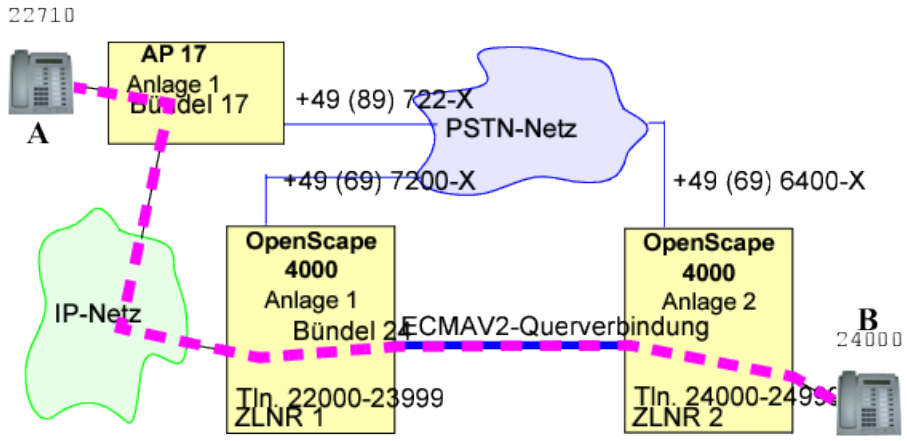


Abbildung 195: Payload-Survivability und Vernetzung - Normalweg A ruft B oder B ruft A

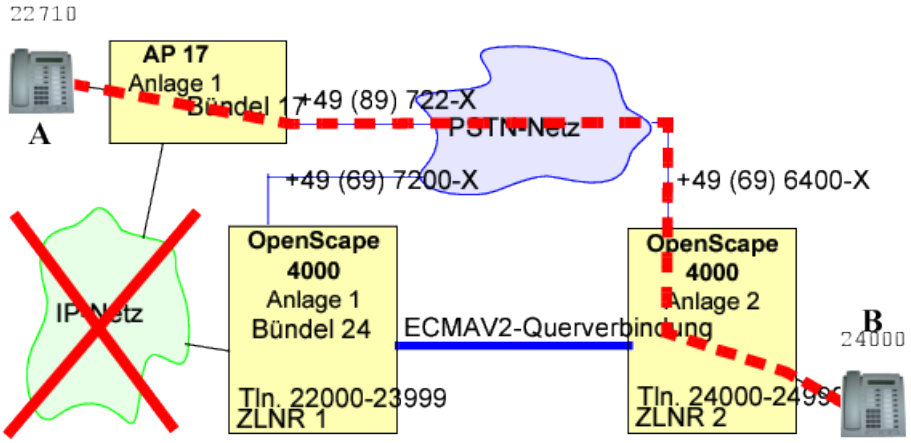


Abbildung 196: Payload-Survivability und Vernetzung - Survivability-Weg A ruft B

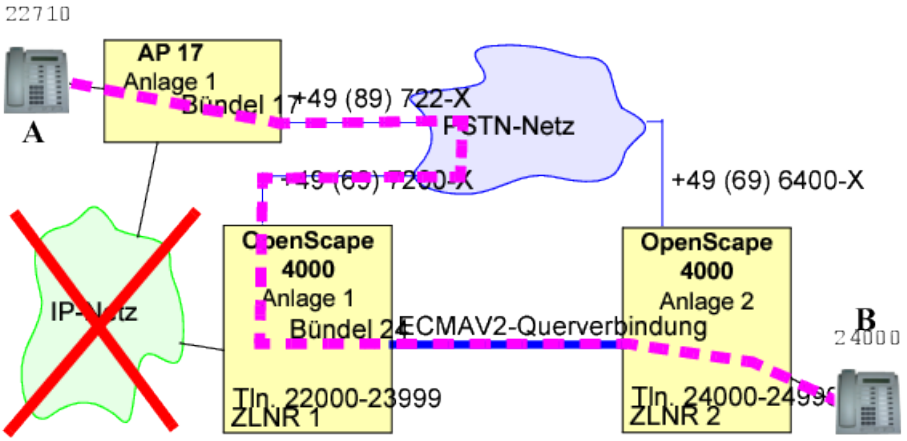


Abbildung 197: Payload-Survivability und Vernetzung - Survivability-Weg B ruft A

NWLCR-Erweiterung für AP 17 zu Anlage 2 bei Payload Survivability
(Bild 24 „Payload-Survivability und Vernetzung - Survivability-Weg A ruft B“)

```
+-------------------------------------------------------------------------+
| LRTG = 124              NAME = ANLAGE 2                  DIENST = ALLE  |
| TYP = NWLCR                                 ZKNNR-RICHTUNG = 1 -2 -400  |
| SERVICE INFO =                                                          |
+-------+-----+-----+-----+------+----------+------------+----------+------+
|       |     |     |     |      | ZEITBAND | CARRIER    |          |      |
|LRTGEL |LWERT|BUNUM|  LWR| LBER | ABCDEFGH |       ZONE |    LATTR | LDSRT|
+-------+-----+-----+-----+------+----------+------------+----------+------+
|     1 |    1|   24|    1|    1 | ******** | 1     LEER |    KEINE |      |
|    2  |  1| 17| 17|   17|      |********  | 1     LEER |    KEINE |      |
+-------+-----+-----+-----+------+----------+------------+----------+------+
+-------------------------------------------------------+
|  LWR     LWRELPOS  LWREL       PARAMETER              |
+--------+----------------------------------------------+
|   1    |      1    ECHOFELD    1                      |
|        |      2    END                                |
+--------+----------------------------------------------+
|INFO:STANDARD-NWLCR ZUR ANLAGE 2                       |
+-------------------------------------------------------+
+-------------------------------------------------------+
|  LWR     LWRELPOS  LWREL       PARAMETER              |
+--------+----------------------------------------------+
|   17   |      1    OUTPULSE    696400                 |
|   2    |      1    ECHO    1                          |
|        |      3    NPI         ISDN                   |
|        |      4    TON         NATIONAL               |
|        |      5    END                                |
+--------+----------------------------------------------+
|INFO:UEBERLAUF AMT FUER ANLAGE 2 (SURVIVABILITY)       |
+--------+----------------------------------------------+
```

10.2.9.4 Einschränkungen

Display-Probleme auf VNR-Systemen, wenn Payload Survivability aktiviert ist

Bitte beachten Sie, dass im Falle eine VNR-Systems, für Rufe über die Payload-Survivability-Route im Display die Rufnummern angezeigt werden, die für das Routing über das öffentliche Netz verwendet werden.

10.2.10 Signaling und Payload Separation (SPS)

Wichtig: Signaling und Payload Separation (SPS) wird nur für Einzelanlagen bereitgestellt! In einer Netzwerkumgebung ist eine projektspezifische Freigabe (PSF) erforderlich und es ist nur Basic Call möglich!

Mithilfe des Leistungsmerkmales Signaling und Payload Separation kann die OpenScape 4000 in einer IPDA-Umgebung den Pfad des Netzwerkverkehrs wie folgt aufteilen:

1) Signalisierung vom Hostsystem (Verbindungssteuerung) an den Access Point wird über das IP-Netzwerk des Kunden (Enterprise WAN) geroutet.

- Payload wird mithilfe von Payload Survivability-Verbindungen über das PSTN Network (ein Anruf vom Hostsystem an einen Access Point beispielsweise automatisch über AMT) geroutet.

Wichtig: SPS Connectivity und Leistungsmerkmale werden nur von IP Access Points und Host Shelves (LTUs) unterstützt, die vom zentralen Kommunikationsserver (Host System) gesteuert werden. Wenn ein IP Access Point in den AP-Emergency-Mode wechselt, dann werden SPS-Connectivity und Leistungsmerkmale nicht mehr unterstützt. Für IP Access Points im AP-Emergency-Mode werden alle Rufe zu anderen IP Access Points und Host Shelves über das Amt basierend auf der AP-Emergeny-LCR-Routing Konfiguration mit Basic Call Funktionalität geroutet.

Da Signaling und Payload Separation auf der vorhandenen Survivability-Lösung basiert, wird die Signalisierung auf dieselbe Weise geroutet wie bisher.

Signaling und Payload Separation kann auf verschiedene Weisen konfiguriert werden:

- Payload-Trennung ist immer aktiv (statische Signaling und Payload Separation).
- Payload-Trennung wird bei eingeschränkter vom Resource Manager verwalteter WAN-Bandbreite oder in Überlauf-Szenarien verwendet, wenn die maximale Bandbreite erreicht ist (Payload-Überlauf).
- Payload-Trennung wird im Falle einer Netzwerkstörung verwendet (Emergency-Routing).
- Teilnehmer bestimmt über Kennzahl, dass er nicht über IP gehen will. In diesem Fall kann die Payload-Trennung mit allen in verschiedenen Source Groups konfigurierten Access Points verwendet werden.

In diesem Fall müssen alle Access Points in unterschiedlichen Source Groups zugewiesen werden, wobei für alle Access Points Amtszugriff obligatorisch ist.

Alle Verbindungen zwischen Access Points sowie zwischen Access Points und dem Hostsystem werden über ISDN-Leitungen hergestellt.

10.2.10.1 Auswirkungen auf Leistungsmerkmale mit SPS

- Für die Payload-Trennung ohne Abwurfparameter müssen SPS-Leitungsbündel konfiguriert sein.
- Belegtübergabe ist über SPS nicht möglich.
- Eine Wegeoptimierung ist nicht möglich.
- Ein direkter Zugriff auf eine Querverbindung ist nicht möglich, wenn sich die Amtsleitung auf einem anderen Rahmen befindet. Umgehungslösung:

Verwenden Sie AMO TWABE, oder aktivieren Sie das Leistungsmerkmal Blockwahl.

- Vermittlungsplatz-Szenarien werden nicht unterstützt.
- Es werden lediglich ComAssistant-Basisszenarien unterstützt. Andere Applikationen mit BL (durch CAP/CA4000) werden nicht unterstützt.
- Payload Survivability ALR mit Einzelnummern und PUBDID werden nicht unterstützt.
- Virtueller Rufnummernplan (VNR) wird nicht unterstützt.
- US-spezifische Szenarien werden nicht unterstützt.
- Direktanruf (DSS)
- Aufschalten
- Anklopfen
- Nur lokale Ansagen werden unterstützt; Ansagen werden nicht über ISDN geroutet (aufgrund der AMT-Ressourcennutzung).
- MLPP wird nicht unterstützt - MLPP-Anrufe über Payload-Trennung sind nicht möglich.
- CHESE - Sekretär und Chef müssen derselben Zweigstelle angehören.
- Broadcast, Direktansprechen - Simplex - Alle Teilnehmer müssen sich auf derselben Zweigstelle befinden.
- ACD-Agenten müssen sich alle auf derselben Zweigstelle befinden.
- PARKEN - Darf nicht auf unterschiedlichen Zweigstellen verwendet werden
- SIP-Telefone werden nicht unterstützt
- Sammelanschluss-Master, der UC-Mitglied ist, ist über den ALR-Pfad nicht erreichbar
- ISDN, ANATE - es werden nur Basisanrufe unterstützt
- UC- und Circuit-Anwendungen werden mit SPS nicht unterstützt

10.2.10.2 Auswirkungen auf Leistungsmerkmale mit SPS

- Basic Call
  - Direktanrufe von einem Rahmen an einen anderen werden über das Amt (Anrufe vom Hostsystem an einen Access Point beispielsweise über AMT) geroutet.
  - Namens- und Nummernanzeige: Ankommende und abgehende Anrufe - bei Verwendung der Payload Survivability-Route:
    - Auf dem Display des Anrufers werden bei einem Basisanruf in der ersten Zeile die Rufnummer und der Name des angerufenen Teilnehmers angezeigt.
    - Auf dem Display des gerufenen Teilnehmers werden bei einem Basisanruf in der ersten Zeile die Rufnummer und der Name des Anrufers angezeigt.
  - Bei Verwendung der Payload Survivability-Route hört der gerufene Teilnehmer „Amtsklingeln“, obwohl es sich um einen internen Anruf handelt.
  - Wenn eine AMT-Verbindung in einer Verbindung zwischen verschiedenen Rahmen abbricht, weist die Verbindung keine Payload auf und wird nach 90 Sekunden getrennt.
  - In QUER-Verbindungen wird der Name nicht angezeigt.

Wichtig: Signaling und Payload Separation (SPS) wird nur für Einzelanlagen bereitgestellt! In einer Netzwerkumgebung ist eine projektspezifische Freigabe (PSF) erforderlich und es ist nur Basic Call möglich!

- Sammelanschluss
  - Paralleler Sammelanschluss wird nicht unterstützt.
  - Sammelanschlussfunktionen sind abgedeckt - linear/zyklisch, Master/Pilot, Sammelanschluss aktivieren/deaktivieren, Überlauf.
  - Sammelanschlussmitglieder müssen sich auf demselben Zweig befinden.
  - Sammelanschlussteilnehmer werden über LAN verbunden, wenn der Anrufer und das Sammelanschlussmitglied demselben Rahmen angehören. Falls der Anrufer und das Sammelanschlussmitglied verschiedenen Rahmen angehören, werden Sammelanschlussteilnehmer über das Amt verbunden.
  - Vergebührung:

  Dem Anrufer werden Gebühren berechnet, wenn ein Sammelanschlussteilnehmer auf einem anderen Rahmen den Anruf entgegennimmt. Bei externen Anrufen (AMT) ist der zahlende Teilnehmer ein Standard-Ziel mit virtueller Richtungskennziffer und das Ziel eine ALR-Rufnummer.

  - Beim Sammelanschluss ankommende Anrufe - bei Verwendung der Payload Survivability-Route:
    - Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des Sammelanschlusses und in der zweiten Zeile die Rufnummer und der Name des anrufenden Sammelanschlussmitglieds angezeigt.

  - Auf dem Display des verbundenen Teilnehmers werden in der ersten Zeile der Name und die Rufnummer des Sammelanschlussmitglieds angezeigt.
  - Auf dem Display des angerufenen Sammelanschlussmitglieds werden in der ersten Zeile die Rufnummer und der Name des Anrufers und in der zweiten Zeile der Name und die Rufnummer des Sammelanschlusses angezeigt.
  - Auf dem Display des verbundenen Sammelanschlussmitglieds werden in der ersten Zeile die Rufnummer und der Name des verbundenen Teilnehmers angezeigt.

  Überlauf-Szenario:
- Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des Sammelanschlusses und in der zweiten Zeile der Name und die Rufnummer des letzten anrufenden Sammelanschlussmitglieds angezeigt.
- Auf dem Display des verbundenen Teilnehmers werden in der ersten Zeile der Name und die Rufnummer des Sammelanschlussmitglieds angezeigt.
- Weiterleitung für Sammelanschlussmitglieder wird nicht unterstützt (**VERLNEXT =N**)*
- Ansage bei Anrufordner - Sammelanschluss wird aufgrund von Einschränkungen der AMT-Ressource nicht unterstützt.
- Die Ausführung des **EXECCFW**-Parameters für die Anrufumleitung vom Sammelanschluss wird ignoriert, wenn sich der Anrufer und der Sammelanschlussteilnehmer mit aktivierter Anrufumleitung auf verschiedenen Rahmen befinden.

• Anrufübernahme

  - Übernahmefunktionen sind abgedeckt (Anzeige des anrufenden Teilnehmers **ANZANR**), Aufmerksamkeitsruf nach Zeit **AUFMRUF**).
  - Anrufübernahmemitglieder müssen sich auf demselben Zweig befinden.
  - Ein Teilnehmeranschluss/Benutzer kann bei der Anrufübernahmegruppe eingehende Anrufe übernehmen.

  Bei Rufszenarien, bei denen sich der Anrufer auf einem anderen Rahmen befindet als der gerufene Teilnehmer und der Teilnehmer, der den Anruf entgegennimmt, wird die AMT-Route verwendet. Dem Anrufer werden Gebühren berechnet.

  Bei externen Anrufen (AMT) ist der zahlende Teilnehmer ein Standard-Ziel mit virtueller Richtungskennziffer und das Ziel eine ALR-Rufnummer.

  - Anzeige Auf dem Display des Teilnehmers, der den Anruf entgegennimmt, werden der Name und die Rufnummer des Anrufers angezeigt.
  - Bei Verwendung der Payload Survivability-Route hört der gerufene Teilnehmer „Amtsklingeln“, obwohl es sich um einen internen Anruf handelt.
  - Gezielte Anrufübernahme wird nicht unterstützt.
  - Netzweite Anrufübernahmegruppen werden nicht unterstützt.

- Rückruf

  Der Benutzer eines Teilnehmeranschlusses kann eine Rückrufanforderung an einen Teilnehmer auf einem anderen Rahmen einrichten.

  – Rückruf bei besetzt/Nichtmelden/frei/Mailbox ist möglich für Anrufe zwischen verschiedenen Zweigen über AMT.
  – Wenn der Rückruf eingeleitet wird (der Anschluss des gerufenen Teilnehmers wird frei), hört der Anrufer den „Anrufton für Intern“, obwohl es sich um einen internen Anruf handelt.
  – Wenn der Rückruf ausgeführt wird, hört der gerufene Teilnehmer „Amtsklingeln“, obwohl es sich um einen internen Anruf handelt.
  – Rückruf vom/zum Netzpartner ist nicht möglich - Menü „Rückruf“ wird nicht angezeigt.
- Anrufumleitung

  Der Benutzer kann Anrufe an einen Teilnehmer auf einem anderen Rahmen umleiten.

  – Anrufumleitung bei besetzt/Nichtmelden ist auf demselben System möglich. An Teilnehmer auf einem anderen Zweigen wird der Anruf über AMT geroutet.
  – Anrufumleitung an Xpressions ist unabhängig vom Rahmenstandort möglich, wenn eine QUER-Verbindung zu Xpressions konfiguriert ist.
  – In Anrufumleitungs-Szenarien werden keine AMT-Ressourcen verwendet, wenn sich der Anrufer und das Anrufumleitungsziel auf demselben Rahmen befinden.
  – Vergebührung

  Dem Anrufer werden Gebühren berechnet, wenn sich das Umleitungsziel auf einem anderen Zweig befindet.

  – Anzeige

  Anrufumleitung unbedingt/bei besetzt - Das Umleitungsziel befindet sich auf einem anderen Zweig als der Anrufer.

  – Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des gerufenen Teilnehmers angezeigt.
  – Auf dem Display des Umleitungsziels werden in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt.

  Anrufumleitung bei Nichtmelden - Wenn sich das Umleitungsziel auf einem anderen Zweig befindet als der Anrufer:

  – Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des gerufenen Teilnehmers und in der zweiten Zeile der Name und die Rufnummer des Umleitungsziels angezeigt.
  – Auf dem Display des Umleitungsziels werden in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt.
  – Die Anrufumleitung wird auf dem Display des Umleitungsziels nicht angezeigt.

- Übergabe und Makeln
  - Der Benutzer kann Anrufe an einen Teilnehmer auf einem anderen Rahmen übergeben.

  Ankommende und abgehende externe Anrufe können an Teilnehmer auf einem anderen Rahmen übergeben werden. In diesem Fall wird der Anruf über AMT geroutet.

  - Anzeige

  Nach der Übergabe werden auf dem Display des Anrufers der Name und die Rufnummer des gerufenen Teilnehmers und auf dem Display des Übergabeziels in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt.

  - Ruf

  Wenn sich der Anrufer und das Übergabeziel auf verschiedenen Rahmen befinden, hört der Anrufer unabhängig von seinem Standort (lokal, Netzwerk) das „Amtsklingeln“.
- Konferenz
  - Der Benutzer kann eine Konferenz einleiten oder an einer Konferenz teilnehmen.
  - Anzeige

  Wenn sich alle Konferenzteilnehmer auf demselben Zweig befinden wie der Teilnehmer, der die Konferenz eingerichtet hat, werden auf dem Display die korrekten Informationen angezeigt.

  - Auf dem Display von Konferenzeilnehmern, die sich auf einem anderen Zweig befinden als der Teilnehmer, der die Konferenz eingerichtet hat, wird nur die Verbindung mit diesem Teilnehmer angezeigt.
  - Auf dem Display von Konferenzteilnehmern, die sich auf einem anderen Zweig befinden als der Teilnehmer, der die Konferenz eingerichtet hat, wird anstelle des Teilnehmernamens der Name der ALR-Route angezeigt.
- Keyset
  - Alle Keysets sind über die Hauptrufnummer erreichbar und können Anrufe über die Primärleitung einleiten.
  - Primärleitung, Sekundärleitung und Phantomline müssen derselben Source Group angehören.
- Namens- und Nummernanzeige

- One Number Service (ONS)
  - Ein ONS-Gruppenteilnehmer kann bei der ONS-Gruppe eingehende Anrufe übernehmen.
  - ONS-Gruppenteilnehmer müssen sich auf demselben Zweig befinden.
  - Bei Rufszenarien, bei denen sich der Anrufer auf demselben Rahmen befindet wie der gerufene ONS-Master und der Teilnehmer, der den Anruf entgegennimmt, wird keine AMT-Route verwendet.
  - Bei Rufszenarien, bei denen sich der Anrufer auf einem anderen Rahmen befindet als der ONS-Master und der ONS-Slave, wird die AMT-Route verwendet und der Anrufer mit den Gebühren belastet.
  - Töne
    - Den ONS-Gruppenteilnehmern ist derselbe RUFTYP zugewiesen wie dem ONS-Master.
    - Bei Verwendung der Payload Survivability-Route hört der gerufene Teilnehmer „Amtsklingeln“, obwohl es sich um einen internen Anruf handelt.
- Fax-Modem
- Anklopfen
- Anrufprotokoll
- OpenScape Xpression-Basisszenarien
- ComAssistant-Basisszenarien

10.2.10.3 Konfiguration

Allgemeine Aktivierung des SPS-Leistungsmerkmals:
`AENDERN-ZANDE:TYP=DATENALL,SPS=JA;`

Weitere Informationen zur Konfiguration finden Sie in Abschnitt 2.9.2, „Wie wird Payload Survivability eingerichtet?“.

Konfigurationsbeispiel

- Erreichbarkeit von Source Group 1 mit alternativer Routing-Tabelle beschreiben
  ```
  EINRICHTEN-
  APRT:TYP=ALTROUT,SRCGRP=1,ALRTYP=ALR,ALTRTNR=00897229000,
  ACCODE=9000,ARTCNR=1000,ARTCNRNG=30;
  ```
- Erreichbarkeit von Source Group 19 mit alternativer Routing-Tabelle beschreiben
  ```
  EINRICHTEN-
  APRT:TYP=ALTROUT,SRCGRP=19,ALRTYP=ALR,ALTRTNR=00897229000,
  ACCODE=9000,ARTCNR=1000,ARTCNRNG=30;
  ```
- Kennzahl für ankommende alternative Route definieren
  `EINRICHTEN-WABE:RNR=9000,KZP=ALTRTKOM;`
- Source Group muss für alle betroffenen externen Leitungen in AMO TDCSU konfiguriert werden
  ```
  AENDERN-TDCSU:LAGE=x-x-x-x,SRCGRP=1;
  AENDERN-TDCSU:LAGE=x-x-x-x,SRCGRP=19;
  ```

- AMO TWABE wird für Direktanruf an Xpression-Zugangsnummern verwendet
  `EINRICHTEN-TWABE:RNR=64,LAE=5;`

  ..hierbei ist 64 (QUER-Kennzahl für EBX, max. 3), 5 die zulässige Länge der gesamten Nummer (QUER-Kennzahl + Länge der Direktzugangsnummer).

  Es ist zu beachten, das TWABE keine WABE-Gruppen aufweist. Anstelle von AMO TWABE könnte auch die Blockwahlfunktion verwendet werden.
- Kennzahl für das Erzwingen der alternativen Route konfigurieren
  `EINRICHTEN-WABE:xxx,,,ALTROUTE,N,,,,,,,;`
- Teilnehmerautorisierung konfigurieren

  TIn COSSU benötigt UENW (UEBERGABE NETZWEIT)-Autorisierung für die Übergabe über SPS.
  `AENDERN-COSSU:TYP=COS, COS=xx, ESBER=UENW;`

Wichtig: Der Carrier muss die Überprüfung der Anrufernummer abschalten (**CLIPNOSCREEN**).

10.2.11 Anrufumlenkung im Survivability-Modus zu einem anderen Access Point

Wenn SingleStepTransfer für ein DIGITE oder ein ANATE im Gesprächszustand aufgerufen wird und kein Pfad zwischen Quelle und Ziel verfügbar ist, wird der alternative Pfad für Payload-Survivability verwendet, sofern er ordnungsgemäß konfiguriert ist.

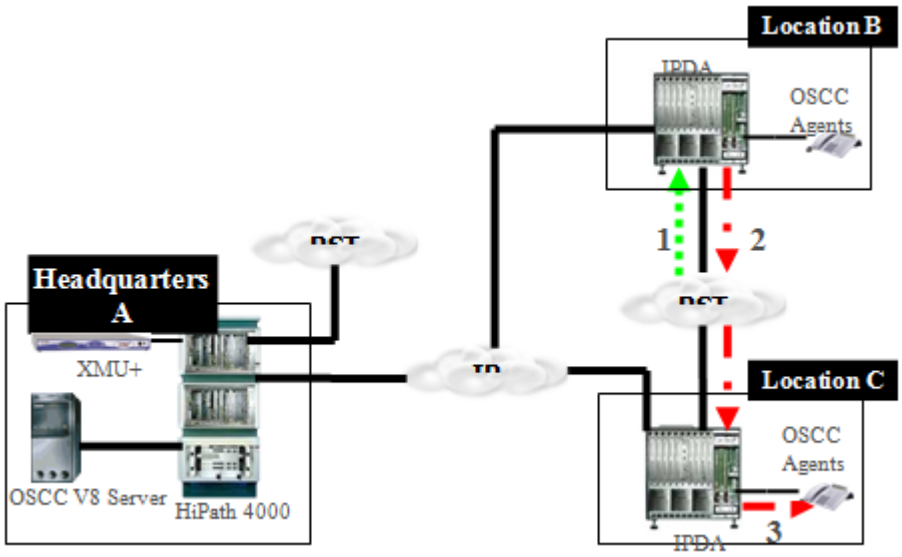
10.2.11.1 Voraussetzungen

- Jeder Access Point benötigt Zugang zum PSTN über den CO-Trunk, und entsprechende alternative Routen und Nummern müssen konfiguriert sein.
- Payload-Survivability oder Signalisierungs- und Payload-Separation (siehe Abschnitt 2.10, „Signaling und Payload Separation (SPS)“) muss konfiguriert sein.
- OpenScape Contact Center (OSCC) ab V8.

10.2.11.2 Benutzerszenarien

Szenario 1

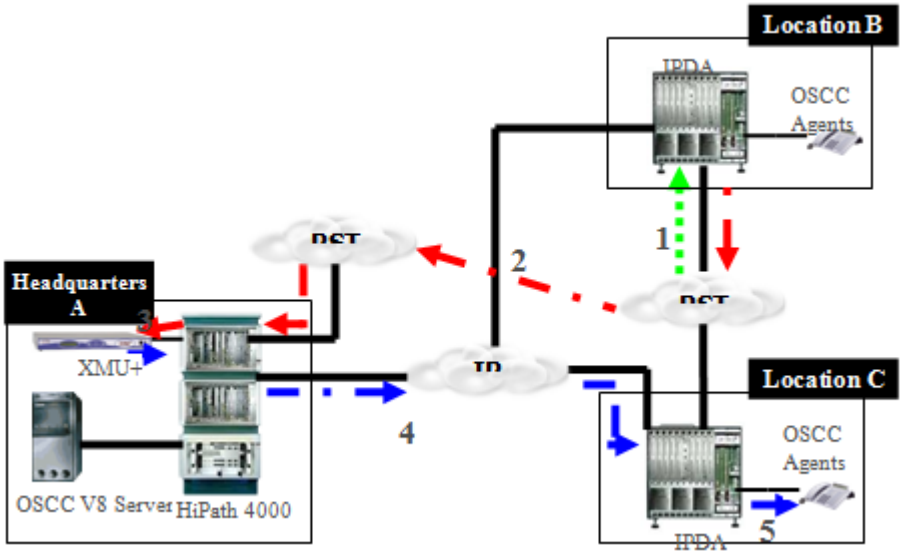
Anruf kommt auf einem Trunk auf dem IPDA an **Standort B** an (in unten stehender Abbildung mit #1 gekennzeichnet). OpenScape Contact Center setzt voraus, dass der Anruf an eine Agent-Nebenstelle auf dem IPDA an **Standort C** geroutet wird, die aufgrund der Payload-Survivability über PSTN routet (gekennzeichnet mit #2 und #3).



Anrufumlenkung im Survivability-Modus - Benutzerszenario 1

Szenario 2

Anruf kommt auf einem Trunk auf dem IPDA an **Standort B** an (in unten stehender Abbildung mit #1 gekennzeichnet). Der Anruf wird aufgrund der Payload-Survivability für die Wiedergabe einer Call Director-Nachricht über PSTN an die OpenScape 4000-Hauptanlage in **Hauptsitz A** geroutet (gekennzeichnet mit #2 und #3). Anschließend kann dieser Anruf entweder über Payload-Survivability oder über das WAN an eine Agent-Nebenstelle auf dem IPDA an **Standort C** geroutet werden (gekennzeichnet mit #4 und #5).

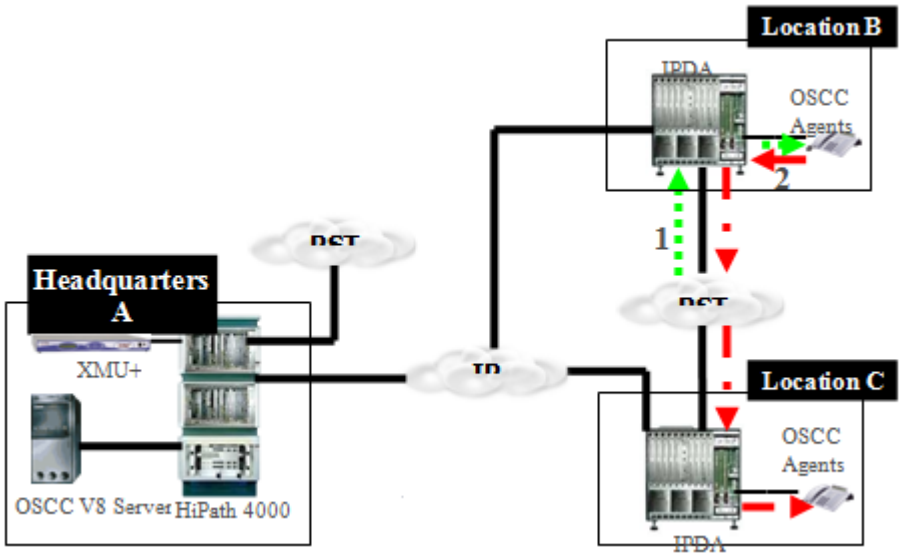


Anrufumlenkung im Survivability-Modus - Benutzerszenario 2

Szenario 3

Anruf kommt auf dem IPDA an **Standort B** an und wird an eine Agent-Nebenstelle geroutet (gekennzeichnet mit #1). Dieser Agent tätigt eine Rückfrage, startet eine Konferenz oder übergibt den Anruf an einen Agenten

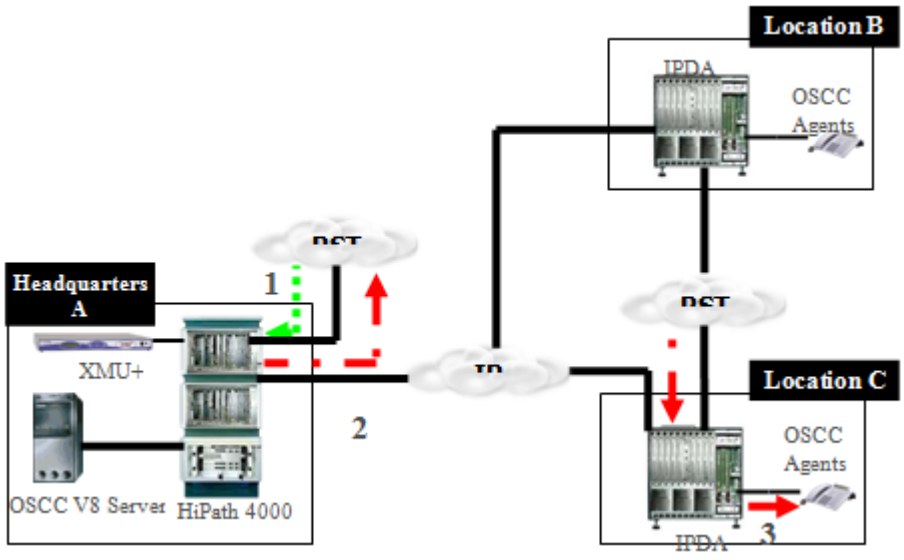
auf dem IPDA an **Standort C** (gekennzeichnet mit #2), der aufgrund der Payload-Survivability über PSTN routet.



Anrufumlenkung im Survivability-Modus - Benutzerszenario 3

Szenario 4

Anruf kommt auf einem Trunk bei der OpenScape 4000-Hauptanlage in **Hauptsitz A** (gekennzeichnet mit #1) an und wird aufgrund der Payload-Survivability über PSTN an eine Agent-Nebenstelle auf einem IPDA an **Standort C** (gekennzeichnet mit #2 und #3) geroutet.



Anrufumlenkung im Survivability-Modus - Benutzerszenario 4

10.2.11.3 Anwendungsfälle

1) Basic Call

2) • Ankommender ACD-Anruf an AP x wird direkt an einen Agenten an AP y geroutet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anrufer in ACD-Warteschlange eingereiht
  • Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten an AP y

• Ankommender ACD-Anruf am OpenScape 4000-Hostsystem wird direkt an einen Agenten an AP x geroutet.

Details:

a) Ankommender Anruf auf CO-Trunk auf dem OpenScape 4000-Hostsystem

b) • Anrufer in ACD-Warteschlange eingereiht
  • Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten an AP x

• Ankommender ACD-Anruf an AP x wird direkt an einen Agenten auf dem OpenScape 4000-Hostsystem geroutet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anrufer in ACD-Warteschlange eingereiht
  • Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten auf dem OpenScape 4000-Hostsystem

3) **Szenarien mit XMU (AMO:RCSU)-Ports**

4) • Ankommender ACD-Anruf an AP x wird an XMU (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP x weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anruf wird in die ACD-Warteschlange eingereiht und mit dem ACD Musik-/Ansageport verbunden (siehe Hinweis 2)
  • Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten an AP x

• Ankommender ACD-Anruf an AP x wird an XMU (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP y weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anruf wird in die ACD-Warteschlange eingereiht und mit dem ACD Musik-/Ansageport verbunden (siehe Hinweis 2)

- Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten an AP y

- Ankommender ACD-Anruf an AP x wird an XMU (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten auf dem OpenScape 4000-Hostsystem weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b)
- Anruf wird in die ACD-Warteschlange eingereiht und mit dem ACD Musik-/Ansageport verbunden (siehe Hinweis 2)
- Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten auf dem OpenScape 4000-Hostsystem

- Ankommender ACD-Anruf am OpenScape 4000-Hostsystem wird an XMU (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP x weitergeleitet

Details:

a) Ankommender Anruf auf CO-Trunk auf dem OpenScape 4000-Hostsystem

b)
- Anruf wird in die ACD-Warteschlange eingereiht und mit dem ACD Musik-/Ansageport verbunden (siehe Hinweis 2)
- Agent ist verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an einen Agenten an AP x

---

Anmerkung: Wenn während der Ansage kein Agent verfügbar wird, wird der ACD-Anruf mit CSTA_DEFLECT_CALL_REQUEST an RCG/DNIT zurückgegeben und ein neuer Agent gesucht. Anwendungsfall 2 gilt also für 2 Fälle: a. Während der Ansage wird ein Agent verfügbar. b. Während der Ansage wird kein Agent verfügbar und eine neue Suche beginnt.

Anmerkung: Wenn ACD-Musik/Ansagen (XMU als RCSU-Ports konfiguriert) verwendet werden, wechselt ACD nur Pfade und verbindet Anrufer-TLS mit XMU-TLS. Wenn keine Payload möglich ist, steht kein Mechanismus für die Verwendung eines alternativen Pfads zur Überwachung dieser Ports zur Verfügung. Der Anruf verbleibt in der ACD-Warteschlange und kann mit CSTA_DEFLECT_CALL_REQUEST jederzeit wie in Hinweis 1 beschrieben an einen beliebigen Agenten geroutet werden. Als Alternative zu RCSU-Ports können auch Call Directors verwendet werden (siehe Anwendungsfall **Szenarien mit Call Director (AMO SCSU)-Ports (analoges Gerät)**).

---

5) Szenarien mit Call Director (AMO SCSU)-Ports (analoges Gerät)

6) • Ankommender ACD-Anruf an AP x wird an Call Director (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP x weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anrufer in ACD-Warteschlange eingereiht
- OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an Call Director auf dem OpenScape 4000-Hostsystem und der Anrufer wird mit Call Director verbunden
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST wieder an die ACD-Warteschlange, ein Agent wird verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an den Agenten an AP x oder
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST an einen Agenten an AP x

• Ankommender ACD-Anruf an AP x wird an Call Director (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP y weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anrufer in ACD-Warteschlange eingereiht
- OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an Call Director auf dem OpenScape 4000-Hostsystem und der Anrufer wird mit Call Director verbunden
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST wieder an die ACD-Warteschlange, ein Agent wird verfügbar und OSCC routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an den Agenten an AP y oder
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST an einen Agenten an AP y

• Ankommender ACD-Anruf an AP x wird an Call Director (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten auf dem OpenScape 4000-Hostsystem weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk an AP x

b) • Anrufer in ACD-Warteschlange eingereiht
- OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an Call Director auf dem OpenScape 4000-Hostsystem und der Anrufer wird mit Call Director verbunden
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST wieder an die ACD-Warteschlange, ein Agent wird verfügbar und OpenScape Contact Center routet den Anruf mit

CSTA_DEFLECT_CALL_REQUEST an den Agenten auf dem OpenScape 4000-Hostsystem oder

- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST an einen Agenten auf dem OpenScape 4000-Hostsystem

- Ankommender ACD-Anruf am OpenScape 4000-Hostsystem wird an Call Director (OpenScape 4000-Hostsystem) geroutet und dann an einen Agenten an AP x weitergeleitet.

Details:

a) Ankommender Anruf auf CO-Trunk auf dem OpenScape 4000-Hostsystem

b)
- Anrufer in ACD-Warteschlange eingereiht
- OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an Call Director auf dem OpenScape 4000-Hostsystem und der Anrufer wird mit Call Director verbunden
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST wieder an die ACD-Warteschlange, ein Agent wird verfügbar und OpenScape Contact Center routet den Anruf mit CSTA_DEFLECT_CALL_REQUEST an den Agenten an AP x oder
- OpenScape Contact Center routet den Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST an einen Agenten an AP x

---

Anmerkung: Wenn während der Ansage kein Agent verfügbar wird, wird der ACD-Anruf mit CSTA_SINGLE_STEP_XFER_CALL_REQUEST an RCG/DNIT zurückgegeben und ein neuer Agent gesucht. Anwendungsfall 3 gilt also für 2 Fälle: a. Während der Ansage wird ein Agent verfügbar. b. Während der Ansage wird kein Agent verfügbar und eine neue Suche beginnt.

Anmerkung: Dieser Anwendungsfall funktioniert, wenn sich Call Director an AP x befindet.

Anmerkung: Dieser Anwendungsfall funktioniert, wenn Call Director durch ein DIGITE ersetzt wird.

---

7) Rückfrage, Anrufübergabeszenarien

8) Im Prinzip könnte es vorkommen, dass ein Agent einen Anruf an einen anderen Agenten übergeben möchte, der sich am selben oder an einem anderen Standort befindet, an dem möglicherweise keine IP-Ressourcen verfügbar sind. Die Anrufübergabe kann nach jedem der oben beschriebenen Szenarien erfolgen.

Anmerkung: Die Nummern können bei Übergabe durch alternatives Routing auf dem Telefondisplay nicht aktualisiert werden.

---

9) **Rufsignal Nichtmelden - kann nach jedem der oben beschriebenen Szenarien erfolgen**
10) Der ACD-Anruf läutet bereits, d. h. der Ziel-Agent ist bereits zugeteilt, nimmt den Anruf aber nicht an. Nach Ablauf eines Timers nimmt OpenScape Contact Center/ACD den Anruf zurück, routet ihn mit CSTA_DEFLECT_CALL_REQUEST wieder an RCG/DNIT und sucht anschließend einen neuen Agenten. Dieses Szenario funktioniert unabhängig vom Standort des Ursprungs-Trunk (OpenScape 4000-Hostsystem/AP x oder AP y) oder des alten/neuen Agenten.

10.2.11.4 Generierung

Es ist keine spezielle AMO-Konfiguration erforderlich.

Payload-Survivability muss ordnungsgemäß konfiguriert sein. Die einzige unterstützte Konfiguration ist ALR über mehrkanaligen Amtssatz unter einer Rufnummer.

Der Wert des OpenScape Contact Center-Timers für âring no answerâ (Rufsignal Nichtmelden) muss kleiner sein als der Wert des âno call transferâ-Parameters **NOCALLTR** (Keine Anrufübergabe) in OpenScape 4000.

Beide Timer (in OpenScape 4000 und OpenScape Contact Center) weisen einen Standardwert von 30 auf. Dies bewirkt das folgende Verhalten: Wenn der Aufruf von ISDN zurückkommt, wird er an die Vermittlungskonsole übergeben und nicht an Call Director geroutet.

Der Parameter kann mit dem folgenden AMO-Befehl in OpenScape 4000 geändert werden:

z. B. `CHANGE-CTIME:TYPESWU=TRK,NOCALLTR=35;`

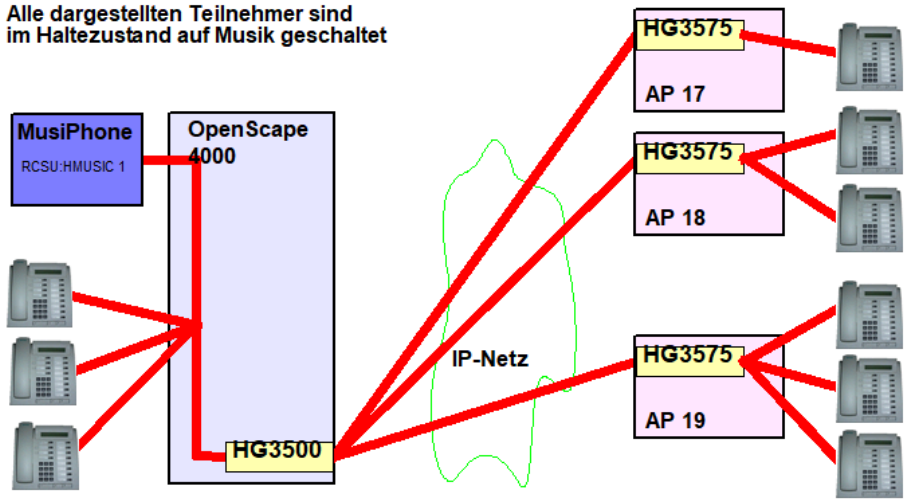
Eine Anleitung zum Ändern des Timers in OpenScape Contact Center finden Sie im Handbuch **OpenScape Contact Center Enterprise V8 R2, Manager Administration Guide, Administrator Documentation > Abschnitt 8.3.2**.

10.2.12 Externe Music-On-Hold

Wird eine interne Tonart (SIU) durch eine externe Tonquelle ersetzt (z.B. Music-On-Hold), dann ist dieser neue Tontyp systemweit gültig.

Im nachfolgenden Beispiel (Bild 30 „Wege für Music-On-Hold: Einspeisung in Zentralsystem“) ist ein externes Musiphone in der Zentrale konfiguriert, wie es am häufigsten praktiziert wird.

Für alle Sätze in IPDA Access Points, welche auf externe MOH geschaltet werden, sind dann IP Payload-Verbindungen in das Zentralsystem nötig. Sind in einem Access Point mehrere Sätze/Teilnehmer auf die selbe MOH geschaltet, wird nur eine Payload-Verbindung (B-Kanal) für die Musikübertragung zwischen Zentrale und Access Point geschaltet, auf die sich alle betroffenen Sätze des AP aufschalten.

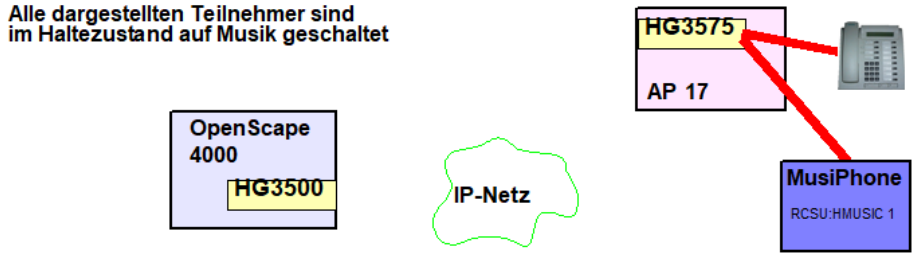


Wege für Music-On-Hold: Einspeisung in Zentralsystem

Wichtig: Wird ein Satz z.B. durch Rückfrage auf MOH geschaltet, wird die ursprüngliche Payload-Verbindung weiter gehalten. D.h. die Anschaltung der MOH belegt eine zusätzliche Payload-Verbindung!

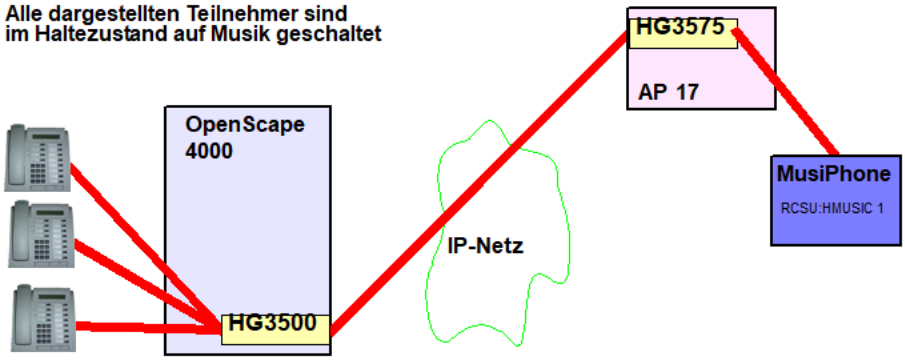
Wird die externe MOH nicht im Zentralsystem, sondern in einem Access Point eingespeist, so werden die Verbindungen dorthin wie folgt gehandhabt.

Sätze innerhalb des Access Point, in dem die MOH eingespeist wird, werden über das AP-interne Koppelfeld auf MOH geschaltet. D.h. es werden keine zusätzlichen Payload-Verbindungen über IP benötigt.



Wege für Music-On-Hold: Einspeisung in Access Point 17 - lokale Teilnehmer

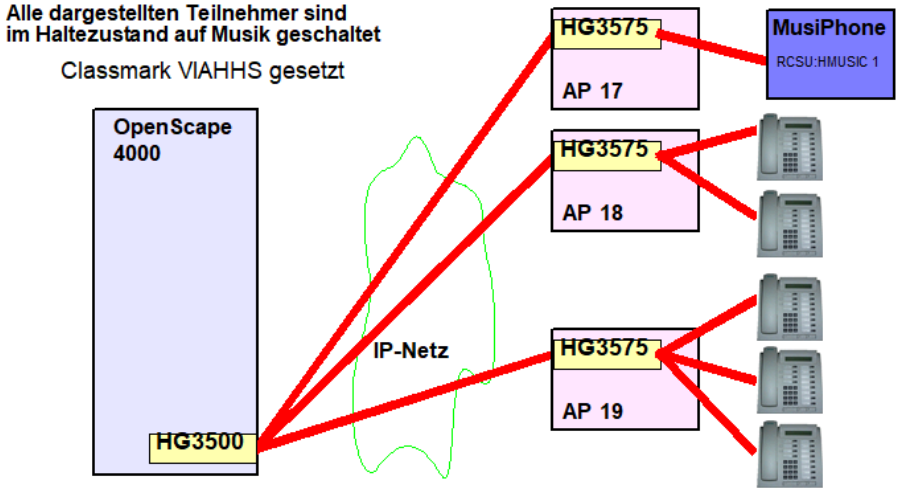
Werden Sätze im Zentralsystem auf MOH geschaltet, so wird eine Payload-Verbindung zwischen dem Access Point mit der MOH-Quelle und der Zentrale geschaltet, aus der dann alle Sätze des Zentralsystems bedient werden.



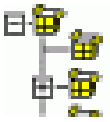
Wege für Music-On-Hold: Einspeisung in Access Point 17 - zentrale Teilnehmer

Werden Sätze anderer Access Points auf MOH geschaltet, so wird für diese Access Points jeweils eine Payload-Verbindung in das Zentralsystem geschaltet, welches über eine zweite Payload-Verbindung zu dem Access Point mit der MOH-Quelle verbunden ist. MOH-Verbindungen zwischen Access Points werden also immer über die Zentrale geschaltet.

Es gibt kein „alternatives Routing“ durch Acess Point <-> Access Point Verbindungen, falls für den Weg über das Zentralsystem keine/nicht genügen Ressourcen vorhanden sind.

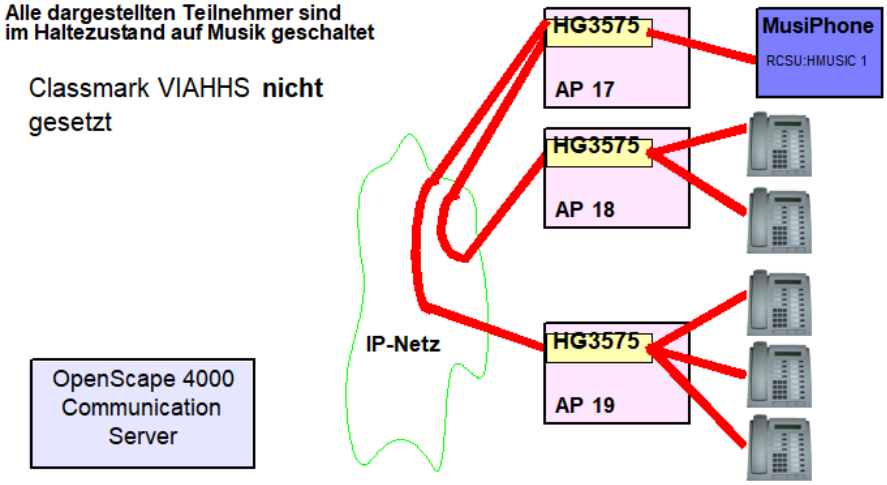


Wege für Music-On-Hold: Einspeisung in Access Point 17 - Teilnehmer in anderen AP

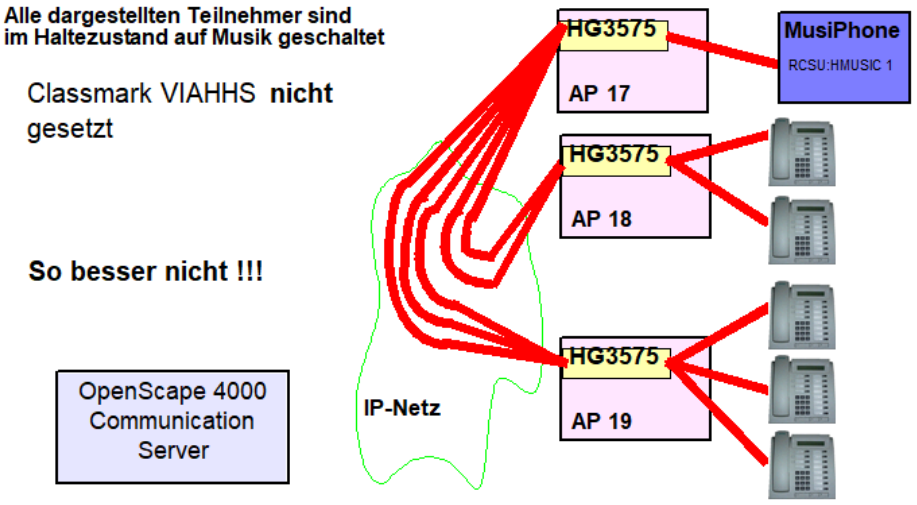
	**Configuration Management > Anschluss > Sonderteilnehmeranschluss** Auf **Suchen** klicken und den Sonderteilnehmer (**Teilnehmertyp EXTANS**) auswählen. Auf der Registerkarte **Merkmale** die gewünschten Classmarks setzen oder löschen und auf **Sichern** klicken.

	`EINRICHTEN-SSC:LAGE=1-2-37-10,TYP=EXTANS,CPTON=WARTETON,CLASSMRK=G711&ML;`
	oder
	`AENDERN-RCSU:LAGE=1-2-37-5,CLASSMRK=G711&&ML;`

Wichtig: Beachten Sie bei dem `AENDERN` der Classmarks, dass Sie alle Classmarks angeben müssen, die gesetzt sein sollen. Es werden keine Classmarks aus der vorherigen Einstellung übernommen. Geben Sie Classmark **ML** immer mit an, da sonst für jeden Satz auf einer HG 3575, der eine Musikanschaltung aktiv benötigt, eine eigene Payload-Verbindung zur Quell-HG3575 aufgebaut wird, was Bandbreite und B-Kanal-Ressourcen frisst.



Wege für Music-On-Hold: Einspeisung in Access Point 17 - Teilnehmer in anderen AP



Wege für Music-On-Hold: Einspeisung in Access Point 17 - Teilnehmer in anderen AP

Multiple Music-On Hold

Gerade bei IPDA-basierten Filialkonzepten besteht die Anforderung, unterschiedlichen Filialen unterschiedliche Music-On-Hold einzustellen.

Mit Hilfe von Flexrouting können dann bis zu 150 unterschiedliche Ansagen im System verwendet werden. Die Zuordnung der Ansagen erfolgt auf Teilnehmerbasis.

Wenn allen Teilnehmern eines Access Points die selbe MOH zugeordnet wird und diese MOH lokal im Access Point eingespielt wird, werden für MOH keine Payload-Verbindungen über IP benötigt. Ist einem Teilnehmer aber eine MOH zugeordnet, welche in einem anderen Access Point eingespielt wird, so werden 2 Payload-Verbindungen über IP geschaltet - von der MOH-Quelle zur Zentrale sowie von der Zentrale zum AP des Teilnehmers.

10.2.13 Hinweise zu CMI

Siehe Projektierungsleitfaden von OpenScape Cordless E in TI - Online:

https://ti-online.global-intra.net/produktiv/de/z3-hp4-70a.pdf

Homepage TI - Online:

https://ti-online.global-intra.net/index.html

10.2.14 IP-Adressänderungen

Leider ist es mit der korrekten Einstellung der IP-Adressen aller IPDA Komponenten zum Installationszeitpunkt nicht getan. Umstrukturierungen im IP-Netz des Kunden, welche auch die Adressierung der IPDA Komponenten betreffen, gehören zum Tagesgeschäft.

Wann immer IP-Adressen geändert werden müssen, führt an einer zumindest kurzfristigen Betriebsstörung kein Weg vorbei. Um die Auswirkungen für die

Benutzer der OpenScape 4000 Anlage zu minimieren, muss das Vorgehen bei Adressumstellungen sorgfältig geplant werden.

Bei den folgenden Szenarien wird immer unterstellt, dass es sich um Änderungen handelt, die das ganze LAN Segment betreffen, an dem IPDA Komponenten angeschlossen sind, nicht um die Adresse einer einzelnen Komponente.

3 Fälle sind dabei zu unterscheiden:

- Adressänderung in einem Netz Segment, in dem Access Points angeschlossen sind
- Änderung der Adresse des Survivability-Netzes
- Änderungen im OpenScape 4000 LAN Segment

10.2.14.1 Adressänderung in einem Netz Segment, in dem Access Points angeschlossen sind

Nehmen wir als Beispiel die Konfiguration des Access Points AP99:

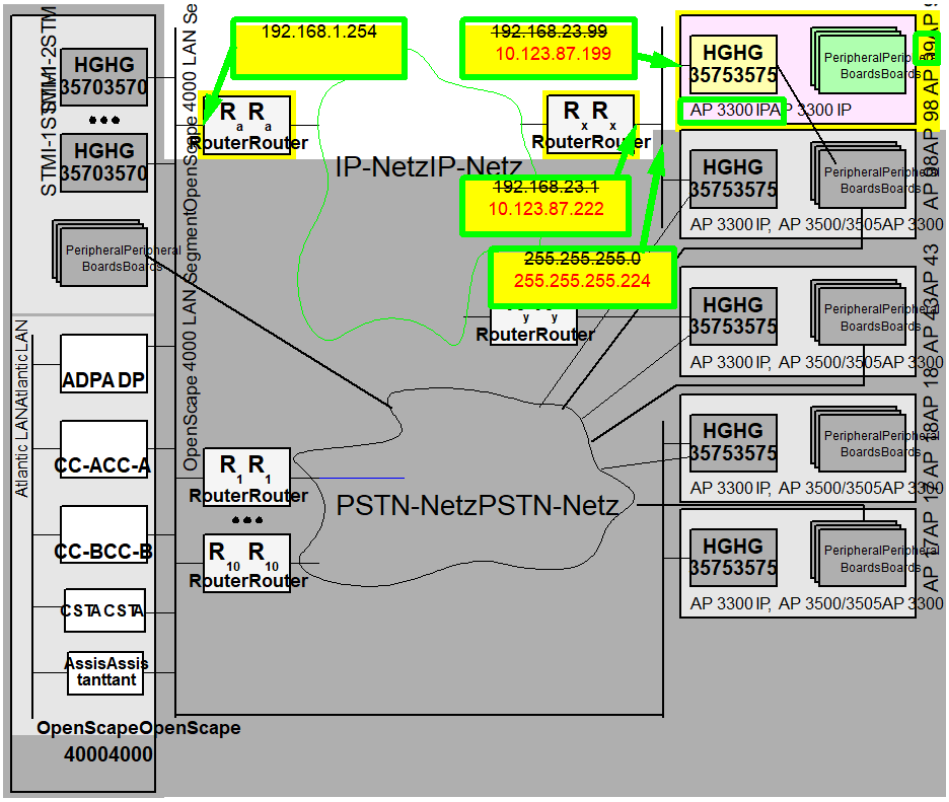
- Er soll aus dem OpenScape 4000 LAN Segment über Router Ra erreicht werden (192.168.1.254).
- Er soll andere Netze über Router Rx (192.168.23.1) erreichen.
- Seine eigene IP-Adresse ist 192.168.23.99.
- Die IP-Adresse für den TAP ist 192.168.23.199.
- Die Netzmaske des Netzes, in dem sich der Access Point befindet ist 255.255.255.0

Da es sich um die Umstellung des gesamten Netzsegments handelt ist auch AP 98 betroffen mit **APIPADR=192.168.23.98**.

Vom Netzwerkadministrator des Kunden bekommen wir diese Infos:

Tabelle 48: Adressänderung bei „networked“ Access Points

Name	Adresse NEU	Adresse ALT
Netzmaske	255.255.255.224	255.255.255.0
Router Rx	10.123.87.222	192.168.23.1
AP 98 APIPADR	10.123.87.198	192.168.23.98
AP 99 APIPADR	10.123.87.199	192.168.23.99



Adressänderung bei „networked“ Access Points

Kritisch bei der Umstellung ist der Zeitpunkt der Adressänderung in den Access Points.

Falls im Kundennetz kein Parallelbetrieb der beiden Netzadressierungen während einer Übergangszeit eingerichtet wird, muss sich die Adressänderung am Umstellzeitpunkt des Routers Rx und der Änderung des Routings im Kundennetz orientieren.

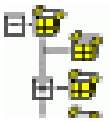
Die Adressänderung muss noch vor der Neukonfiguration des Routers Rx durchgeführt und mittels EXEC-USSU:UPDATAP auf den Access Point geladen werden. Bestehende Verbindungen werden dadurch getrennt. Nach der Neukonfiguration des Routers würden wir den Access Point ja bereits nicht mehr erreichen und könnten die Adressänderung nur noch vor Ort am Access Point durchführen.

Wichtig: Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden. Andernfalls wären nach einem Reload der Anlage die Daten auf dem System und auf der HG 3575 unterschiedlich und könnten nur durch `EXEC-USSU:UPDATAP`, LTU-Nummer, `UL` wieder synchronisiert werden.

Sobald der Access Point mit der neuen Adresse hochgelaufen ist, kann er von der OpenScape 4000 Zentrale nicht mehr bzw. nur mehr über den Signaling Survivability Weg (falls eingerichtet) erreicht werden. Und das solange, bis das Routing im Kundennetz ebenfalls geändert ist.

Wichtig: Werden in der Konfiguration des IPDA Systems Sonderrouten verwendet (in Access Points oder für HG 3500), so sind diese alle zu überprüfen und müssen gegebenenfalls angepasst werden. (`AENDERN-APRT:TYP=ROUTTBL ...`)

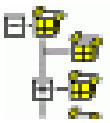
Generierung

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle** die Adressen ändern und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.

	`AENDERN-`
	`APRT:TYP=APNET,LTU=98,APIPADR=10.123.87.198,`
	`NETMASK=255.255.255.224;`
	`EXEC-USSU:ART=UPDATAP,LTU=98;`
	`AENDERN-`
	`APRT:TYP=APNET,LTU=99,APIPADR=10.123.87.199,`
	`NETMASK=255.255.255.224;`
	`EXEC-USSU:ART=UPDATAP,LTU=99;`

10.2.14.2 Änderung der Adresse des Survivability-Netzes

Dieser Fall ist eher unwahrscheinlich, dafür aber im OpenScape 4000 System einfach durchzuführen. Alle Adressen im Survivability-Netz sind fest von der Netzadresse abgeleitet.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf der Registerkarte **Anlagendaten** die Survivability-Netzwerk-Adresse ändern, dann auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`AENDERN-SIPCO:TYP=LSNET,SURVNET=192.168.123.0;` Die Änderung innerhalb der Access Points wird wirksam nach `EXEC-USSU:MODE=UPDATAP,LTU=xx;` für alle betroffenen Access Points.

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt. Vor dem `EXEC-USSU:UPDATAP`muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

Wichtig: Da auch Ports der Survivability-Router von der Adressänderung betroffen sind, müssen die Router ebenfalls neu konfiguriert werden. Dies darf aber erst nach dem Umstellen der Access Points erfolgen!

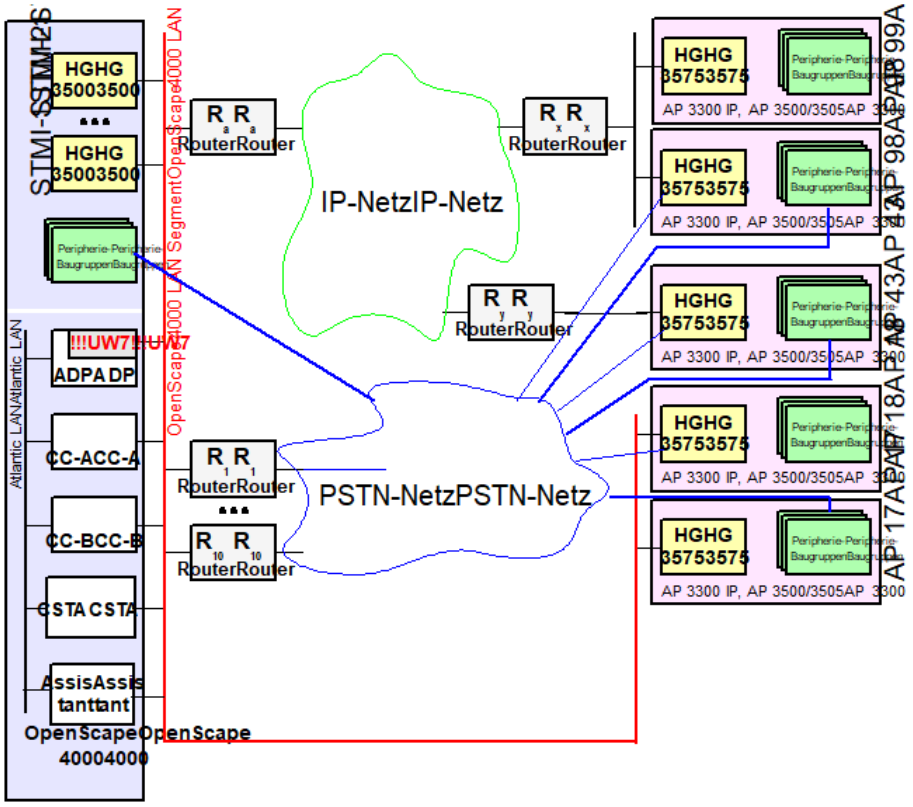
10.2.14.3 Änderungen im OpenScape 4000 LAN Segment

Diese Änderung ist die komplizierteste und risikoreichste, weshalb Adressänderungen im OpenScape 4000 LAN Segment möglichst vermieden werden sollten.

Der Grund dafür liegt im Sicherheitskonzept von IPDA. Ein Access Point darf sich nur von CC-A oder CC-B steuern lassen. Dazu sind die IP-Adressen der beiden Prozessoren im Access Point konfiguriert. Ändern sich nun diese Adressen, kann der Access Point nicht mehr gesteuert werden und müsste lokal neu konfiguriert werden.

Diese potenziell riskante Aufgabe wurde in HiPath 4000 V6 R2 verbessert. Seit dieser Version besteht die Möglichkeit, die Verbindung zum Access Point von einer beliebigen IP-Adresse aus herzustellen, wenn keine aktive HSR-Verbindung vorhanden ist. Auf diese Weise ist es möglich, eine neue Verbindung zu öffnen, die Konfigurationsdaten an den Access Point oder das OpenScape 4000 SoftGate zu übertragen und die reguläre Steuerungsverbindung herzustellen. Nach diesem Schritt wird wieder der ursprüngliche Sicherheitsmechanismus, also die Überprüfung der Remote CC-A- oder CC-B-Adresse, aktiviert.

Wenn die Steuerungsverbindung zu einem Access Point nicht geöffnet werden kann, besteht außerdem die Möglichkeit, eine SSH-Sitzung über dessen Steuerungs-IP-Adresse zu starten und die Konfiguration von Hand zu ändern.



Beispielinstallation

Vom Netzwerkadministrator des Kunden bekommen wir diese Infos:

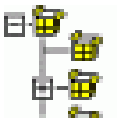
Tabelle 49: Adressänderung im OpenScape 4000 LAN Segment

Name	Adresse NEU	Adresse ALT
Netzmaske	255.255.255.224	255.255.255.0
Netzadresse	10.123.1.64	192.168.1.0
CC-A	10.123.1.65	192.168.1.1
CC-B	10.123.1.66	192.168.1.2
ADP	10.123.1.67	192.168.1.3
Router Ra	10.123.1.94	192.168.1.254
Router R1	10.123.1.83	192.168.1.101
Router R10	10.123.1.93	192.168.1.102
AP 17	10.123.1.77	192.168.1.17
AP 18	10.123.1.78	192.168.1.18
STMI-1	10.123.1.68	192.168.1.10
STMI-2	10.123.1.69	192.168.1.11

Das folgende Vorgehen vermeidet die lokale Neukonfiguration der Access Points.

Schritt 1

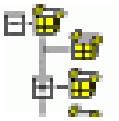
Ändern der IP-Adressen im OpenScape 4000 LAN Segment.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf der Registerkarte **Anlagendaten** IP-Adressen und gegebenenfalls **Netzmaske** ändern und auf **Sichern** klicken.
	`CHANGE-SIPCO:TYPE=LSNET,NETADDR=10.123.1.64, NETMASK=255.255.255.224,DEFRT=10.123.1.94, CCAADDR=10.123.1.65,CCBADDR=10.123.1.66;`

Damit sind die Adressen umgestellt. Die Änderung ist aber erst nach einem Neustart des Systems wirksam, der aber erst als letzter Schritt in dieser Kette erfolgen darf.

Schritt 2

Für „networked“ Access Points ändert sich implizit die CC-A und CC-B Adresse. Explizit muss `LSRTADR` geändert werden, die Adresse des Routers am OpenScape 4000 LAN Segment (Router Ra) , über den die Signalisierungsverbindung eingerichtet ist.

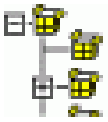
	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle (NW)** die Adresse des Routers in AP-Netzwerk ändern und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.
	`AENDERN-UCSU:ART=AP,LTU=xx,LSRTADR=10.123.1.94; EXEC-USSU:MODE=UPDATAP,LTU=xx;` für **jeden** „networked“ AP, in diesem Beispiel also 43, 98 und 99.

Damit gehen die Access Points außer Betrieb, bis sowohl die CC-Adressumstellung im System wirksam ist, als auch das Routing im Kundennetz umgestellt wurde. Bestehende **Verbindungen werden dadurch getrennt.**

Schritt 3

Ändern der OpenScape 4000 LAN Adressen der „direct link“ Access Points.

Annahme ist hierbei, dass die Adressierung im internen Netz der „direct link“ Access Points nicht verändert wird.

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf der Registerkarte **IP-Schnittstelle (DL)** die Adresse des Routers in AP-Netzwerk ändern und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken und den Tätigkeitsmodus **AP aktualisieren** einstellen. Mit **OK** bestätigen.

	`AENDERN-UCSU:ART=AP,LTU=17,LSRTADR=10.123.1.77;`
	`EXEC-USSU:UPDATAP,17;`
	`AENDERN-UCSU:ART=AP,LTU=18,LSRTADR=10.123.1.78;`
	`EXEC-USSU:UPDATAP,18;`

Damit gehen die Access Points außer Betrieb, bis die CC-Adressumstellung im System wirksam ist. Bestehende **Verbindungen werden dadurch getrennt.**

Schritt 4

Ändern der Survivability-Router Adressen am OpenScape 4000 LAN Segment.

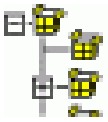
Im Beispiel gibt es die Router R1 und R10. Um deren Adressen im OpenScape 4000 LAN Segment zu ändern, müssen sie aus der Konfiguration entfernt - und wieder hinzugefügt werden.

Leider kann ein Survivability Router erst entfernt werden, wenn keine Access Points mehr auf diesen Router konfiguriert sind.

In diesem Beispiel sind dies die Access Points 18, 43 und 98, die für Signaling Survivability konfiguriert sind. Auch hier muss die Konfiguration entfernt und danach wieder hinzugefügt werden.

Die Adress-Konfiguration der Survivability-Router muss natürlich ebenfalls angepasst werden.

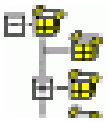
Der Gesamtablauf sieht also folgendermaßen aus:

	**Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** die Router-Nummer bei **Signaling Survivability** löschen und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA -- > IPDA Signaling Survivability Router** Auf **Suchen** klicken und Router auswählen > **Löschen**. Auf **Neu** klicken, Router mit geänderten Daten eingeben und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA Access Point** Auf **Suchen** klicken und den Access Point auswählen. Auf Registerkarte **Allgemein** die Router-Nummer bei **Signaling Survivability** eingeben und auf **Sichern** klicken.

	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=43;`
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=98;`
	`DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1;`
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=1,`
	`LSADDR=10.123.1.83;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=43,ROUTERNO=1;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=98,ROUTERNO=1;`
	`DELETE-APRT:TYPE=SURV,CONF=AP,LTU=18;`
	`DELETE-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10;`
	`ADD-APRT:TYPE=SURV,CONF=ROUTER,ROUTERNO=10,`
	`LSADDR=10.123.1.93;`
	`ADD-APRT:TYPE=SURV,CONF=AP,LTU=18,ROUTERNO=10;`

Schritt 5

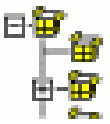
Ändern der Adressen der HG 3500 Baugruppen:

	**Configuration Management > Anlagendaten > Baugruppe > Baugruppe** Auf **Suchen** klicken und **STMI** auswählen. Auf der Registerkarte **STMI Baugruppendaten** die Adresse unter **IP-Gateway** ändern und auf **Sichern** klicken.

	`AENDERN-`
	`BCSU:ART=IPGW,LTU=5,EBT=85,IPADR=10.123.1.68;`
	`AENDERN-`
	`BCSU:ART=IPGW,LTU=5,EBT=91,IPADR=10.123.1.69;`

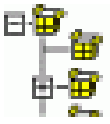
Wichtig: Werden in der Konfiguration des IPDA Systems Sonderrouten verwendet (zwischen Access Points und HG 3500), so sind diese alle zu überprüfen und müssen gegebenenfalls angepasst werden. (`AENDERN-APRT:TYP=ROUTTBL ...`)

Danach müssen die geänderten Adressen auf die HG 3500 Baugruppen gebracht werden durch:

	**Configuration Management > Anlagendaten > Wartung > BG-Wartung** Auf **Suchen** klicken und **STMI** auswählen. Im Pull-Down-Menü **Aktion** auf **Ausführen** klicken, **Neustart** einstellen und mit **OK** bestätigen.
	`RESTART-BSSU:ADDRTYPE=PARTNO,PARTNO=Q2316-X,FCTID=1;`

Schritt 6

Zum Abschluss muss nun noch das OpenScape 4000 System rückgesetzt werden, damit die mit SIPCO eingestellten Adressen wirksam werden.

	Der Neustart kann nur über den Expertenmodus ausgelöst werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`EXEC-REST:UNIT,BP,SOFT;`

Der Kontakt zu den „networked“ Access Points kann erst wiederhergestellt werden, wenn auch das Routing im Kundennetz umgestellt ist.

10.2.15 A-Law/µ-Law Konvertierung im AP-Shelf

10.2.15.1 Leistungsmerkmalbeschreibung

Es ist möglich Telefone in AP-Shelves anzuschließen, die mit anderen Kompandierungskennlinien arbeiten als das Host-System (z.B. Host-System in Deutschland (a-Law), Access Point in USA (µ-Law)).

10.2.15.2 Serviceinformationen

Die Konvertierung wird unterstützt für

- SIP- und H323-Sätze und
- HFA-, SIP-, TDM- und analoge Endgeräte.

10.2.15.3 Generierung (Beispiel)

```
AENDERN-UCSU:ART=AP,LTU=17,KONVLAW=JA;
```

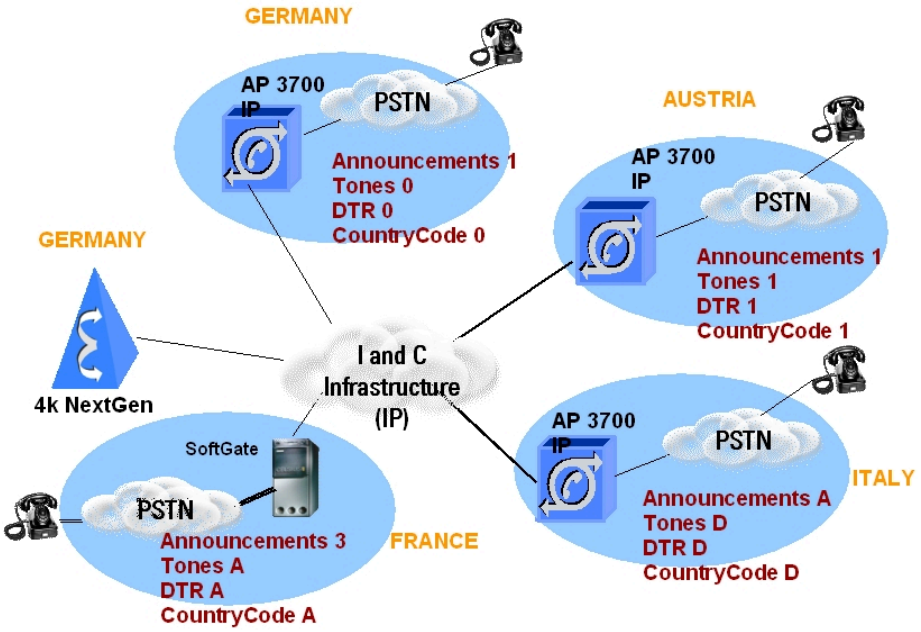
Nun muss noch die NCUI-Baugruppe zurückgesetzt werden, damit die Funktionalitt aktiviert wird. Ab diesem Zeitpunkjt arbeitet das AP-Shelf mit einer anderen Kompandierungslinie als das Host-System. Die NCUI stellt also einen G711-Law-Konvertierungspunkt dar.

10.2.16 Verschiedene Ansagen, Töne und DTMF DialTone Empfänger pro Access Point

Es ist möglich, die Sprachen- und Ländereinstellungen mit AMO UCSU für jeden Access Point gesondert festzulegen. Aus diesem Grund können verschiedene Access Points dieselben oder unterschiedliche SIU-Init-Datendateien aufweisen.

10.2.16.1 Leistungsmerkmalbeschreibung

Mit diesem Leistungsmerkmal können Sie für Access Points in unterschiedlichen Sprachen oder Ländern eigene Töne und Ansagen einstellen. Auf diese Weise erreichen Sie, dass die einzelnen Teilnehmer die zur ihrer jeweiligen Länder- und Spracheneinstellung passenden Töne und Ansagen zu hören bekommen. Diese werden vom SIU-Teil der NCUI-Baugruppe erzeugt. Außerdem haben Sie die Möglichkeit, einzelne Töne je nach Access Point verschiedenen SIU-Funktionen zuweisen. Darüber hinaus lässt sich die Länderkennzahl gezielt für den Access Point festlegen.



Leistungsmerkmalübersicht

Es können alle bekannten Teilnehmertypen (analog, digital, IP) verwendet werden.

Analoge Teilnehmer können für jeden Access Point gesondert länderspezifisch konfiguriert werden (dies kann beispielsweise notwendig sein, um den richtigen Komprimierungsalgorithmus einzustellen.

Der Wähltonempfänger des SIU-Teils der NCUI-Baugruppe lässt sich ebenfalls länderspezifisch konfigurieren.

Externe Ansagegeräte (konfigurierbar über AMO SSC) lassen sich wahlweise allen AP-Rahmen (oder nur ausgesuchten AP-Rahmen) zuweisen.

Dieses Leistungsmerkmal ist sowohl für klassische Access Points als auch für Soft-APs gültig.

10.2.16.2 Serviceinformation

Wenn auf alle Access Points dieselben Länder- und Spracheinstellungen angewendet werden wie auf das Hostsystem, kann die Konfiguration wie bei HiPath 4000-Systemen bis V5 durchgeführt werden. Beachten Sie jedoch, dass die systemweiten Einstellungen (via AMO ZAND) vorgenommen werden müssen, bevor die Access Point konfiguriert werden. Systemweite Einstellungen, die nachträglich geändert werden, gelten nur noch für Host-Rahmen. Wenn sie auch für Access Points gelten sollen, müssen Sie sie für jeden der betroffenen Access Points gesondert eingestellt werden.

Die folgenden systemweiten Einstellungen (via AMO ZAND) können auch für einzelne Access Points vorgenommen werden:

Tabelle 50: Access Point-spezifische Konfiguration

	AMO ZAND D1 = Typ, D2 = Parameter (Deutsch) E1 = Typ, E2 = Parameter (Englisch)			
	(D1) DATENALL (D2) SIUSPKZ	(D1) DATENALL (D2) LANDKZ	(D1) TOENE (D2) SIU	(D1) TOENE (D2) HZE
	(E1) ALLDATA (E2) SIUANN	(E1) ALLDATA (E2) CNTRYCD	(E1) TN (E2) SIUC	(E1) TN (E2) DTR
Funktion / Funktion	SIU Ansagen / SIU announcements	Länderkennzeichen für Steuerung Baugruppenloadware SLMA / Country code to control board loadware SLMA	SIU Töne / SIU tones	Hörzeichenempfänger / dial tone receiver

Access Point-spezifische Einstellungen werden mit AMO UCSU vorgenommen. Die Parameternamen in AMO ZAND werden für die neuen Parameter in AMO UCSU unverändert übernommen.

Wenn eine dieser Einstellungen geändert wird, während der Access Point in Betrieb ist (via CHANGE-UCSU), muss der ACDR- oder Ton-Parameter von Hand geladen werden. Dies geschieht mithilfe des Befehls `EXEC-USSU:NCUILOAD;`.

Die Änderung wird erst beim Zurücksetzen der betreffenden NCUI-Baugruppe wirksam. Dies geschieht mithilfe des Befehls `EXEC-USSU:UPDATAP;`.

Wenn diese systemweiten Einstellungen nachträglich geändert werden, gelten die Änderungen nur für Host-Rahmen. Änderungen, die auch für Access Points gelten sollen, müssen für jeden Access Point gesondert vorgenommen werden.

Besonderheiten der Einstellung für USA:

In den USA wird der Komprimierungsalgorithmus µ-law (und nicht wie in allen anderen Ländern A-law) verwendet.

Es ist möglich, Telefone in AP-Rahmen zu verbinden, die mit einem anderen Komprimierungsalgorithmus arbeiten als das Hostsystem (z.B. Hostsystem in Deutschland, AP in den USA). Hierbei galt jedoch die Einschränkung, dass keine analogen Telefone in diesen AP-Rahmen verbunden werden können. Mit Einführung des Leistungsmerkmal „Unterschiedliche Ansagen pro Access Point“ wird diese Einschränkung aufgehoben, sodass auch dann analoge Telefone in den AP-Rahmen verbunden werden können, wenn der Access Point und das Hostsystem unterschiedliche Komprimierungsalgorithmen verwenden. Siehe auch Abschnitt 2.15, „A-Law/µ-Law Konvertierung im AP-Shelf“.

Einschränkungen

- Die Funktionen peripherer SIU (SIU Typ 2 und 3, SIU TDS) sind nicht Access Point-spezifisch konfigurierbar, d.h. die systemweite Einstellung gilt für alle Access Points. (In Verbindung mit OpenScape 4000 SoftGate Access Points sind überhaupt keine peripheren SIU möglich.)
- Wartemusik (MOH) Wenngleich Wartemusik (MOH) nicht von der Sprach-/Ländereinstellung abhängig ist, kann sie nicht für jeden Access Point gesondert konfiguriert werden.
- Andere länderspezifische Leistungsmerkmale wie MFC-Varianten, Loadware-Varianten für SLMA2 / SLMAR, länderspezifische Töne und Dämpfung für Konferenzbaugruppe von Kompakthardware und SCC-Baugruppe usw. werden nur systemweit unterstützt.

10.2.16.3 Generierungsbeispiel

Das folgende Beispiel zeigt nur die AMOs/Parameter, die für jeden Access Point gesondert eingestellt werden können, und stellt daher nur einen Teil der Gesamtkonfiguration dar.

10.2.16.3.1 Access Point in einem anderen Land als das Hostsystem

Zunächst müssen die Parameter für das Hostsystem eingestellt werden (z.B. Deutschland):

```
AENDERN-ZAND:TYP=DATENALL,LANDKZ=0,SIUSPKZ=1;
ANDERN-ZAND:TYP=TOENE,SIU=0,HZE=0,RDS=0,CONFKHW=0;
```

Anschließend können die Töne/Ansagen für andere Länder (z.B. Italien) für einen Access Point festgelegt werden:

```
EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=17,LTSACHNR=âQ2323-X
",SRCGRP=17,FRAMETYP=L80XF,VERBART=APDL,LSRTADR=198.16.16.63,APR
TADR=198.16.16.150,STANDOID=017,STANDORT=âLOCATIONâ,TEL=3140,FAX
=3141,PLCHECK=JA,ANZBKAN=60,KONVLAW=NEIN,TCLASS=0,ALARMNR=0,SIUS
PKZ=A,SIU=D,DTR=D,LANDKZ=D;
```

10.2.16.3.2 Access Point mit abweichendem Komprimierungsalgorithmus

Zunächst müssen die Parameter für das Hostsystem eingestellt werden (z.B. Deutschland):

```
AENDERN-ZAND:TYP=DATENALL,LANDKZ=0,SIUSPKZ=1;
ANDERN-ZAND:TYP=TOENE,SIU=0,HZE=0,RDS=0,CONFKHW=0;
```

Anschließend können Töne/Ansagen für einen Access Point in einem Land mit einem anderen Komprimierungsalgorithmus (USA) festgelegt werden:

```
EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=17,LTSACHNR=âQ2323-X
",SRCGRP=17,FRAMETYP=L80XF,VERBART=APDL,LSRTADR=198.16.16.63,APR
TADR=198.16.16.150,STANDOID=017,STANDORT=âLOCATIONâ,TEL=3140,FAX
=3141,PLCHECK=JA,ANZBKAN=60,KONVLAW=JA,TCLASS=0,ALARMNR=0,SIUANN
=D,SIU=K,HZE=K,LANDKZ=K;
```

Wenn der Komprimierungsalgorithmus geändert wird, während der Access Point bereits in Betrieb ist (via CHANGE-UCSU), muss der Access Point zunächst deaktiviert werden (via DEACTIVATE-USSU). Erst danach wird der geänderte **KONVLAW**-Parameter berücksichtigt. Abschließend sollten Sie den Access Point (via ACTIVATE-UCSU) wieder aktivieren.

10.2.16.3.3 Access Point mit individueller CP-Ton/SIU-Funktionszuweisung

Beim Einstellen systemweiter Töne (via AMO ZAND) wird auch die Standardzuweisung der CP-Töne für SIU-Funktionen für das System festgelegt. Diese Zuweisung kann systemweit via AMO ZAND (**TYP=TONTBL**, Parameter **CPTON** und **SIU**) angepasst werden.

Beim Einstellen Access Point-spezifischer Töne (via AMO UCSU) wird auch die Standardzuweisung der CP-Töne für SIU-Funktionen für den jeweiligen Access Point festgelegt. Diese Zuweisung kann via AMO UCSU (Parameter **CPTON** und **SIU**) für einen bestimmten Access Point angepasst werden.

Beispiel: Zuweisung des CP-Tons „Nicht möglich“ für die SIU-Funktion 0:

```
AENDERN-UCSU:ART=AP,LTG=1,LTU=17,CPTON=NIMO,SIU=0;
```

10.2.16.3.4 Externe Ansagegeräte

CP-Töne können auch externen Ansagegeräten zugewiesen werden, die sich via AMO SSC für eine analoge Baugruppe konfigurieren lassen. Die Zuweisung von CP-Tönen für externe Ansagegeräte kann systemweit oder individuell konfiguriert werden:

- nur für alle Host-Rahmen, oder
- für alle Host-Rahmen und x Access Points, oder
- nur für x Access Points.

(x steht für einen AP oder alle APs)

Wenn AMO SSC für Ansagegeräte konfiguriert wird, gelten die Einstellungen für alle Rahmen (Host und AP). Wenn die Ansagegeräte für einzelne Rahmen individuell konfiguriert werden sollen, muss der Parameter **LTU** eingegeben werden. Dies bedeutet, dass bei Eingabe eines Host-Rahmens die Einstellung auf alle Host-Rahmen und bei Eingabe eines AP-Rahmens (oder eines AP-Rahmenbereichs) die Einstellung auf den AP-Rahmen (oder die entsprechenden AP-Rahmen) angewendet wird.

Sie können bis zu 300 verschiedene externe Ansagegeräte konfigurieren.

1) Externe Ansagegeräte systemweit einstellen:

2)
```
EINRICHTEN-SSC:LAGE=1-18-1-0,TYP=EXTANS,CPTON=WTONINT;
```

3) Externe Ansagegeräte nur für alle Host-Rahmen einstellen:

4)
```
EINRICHTEN-SSC:1-18-1-0,EXTANS,WTONINT,LTU=1;
```

5) Externe Ansagegeräte für alle Host-Rahmen und einen AP-Rahmen einstellen:
6) `EINRICHTEN-`
`SSC:LAGE=1-18-1-0,TYP=EXTANS,CPTON=WTONINT;`**`LTU=1;`**

`EINRICHTEN-`
`SSC:LAGE=1-18-1-0,TYP=EXTANS,CPTON=WTONINT;`**`LTU=17;`**
7) Externe Ansagegeräte für mehrere AP-Rahmen einstellen:
8) `EINRICHTEN-`
`SSC:LAGE=1-18-1-0,TYP=EXTANS,CPTON=WTONINT;`**`LTU=17;`**

`EINRICHTEN-`
`SSC:LAGE=1-18-1-0,TYP=EXTANS,CPTON=WTONINT;`**`LTU=20;`**

10.2.16.4 Relevante AMOs

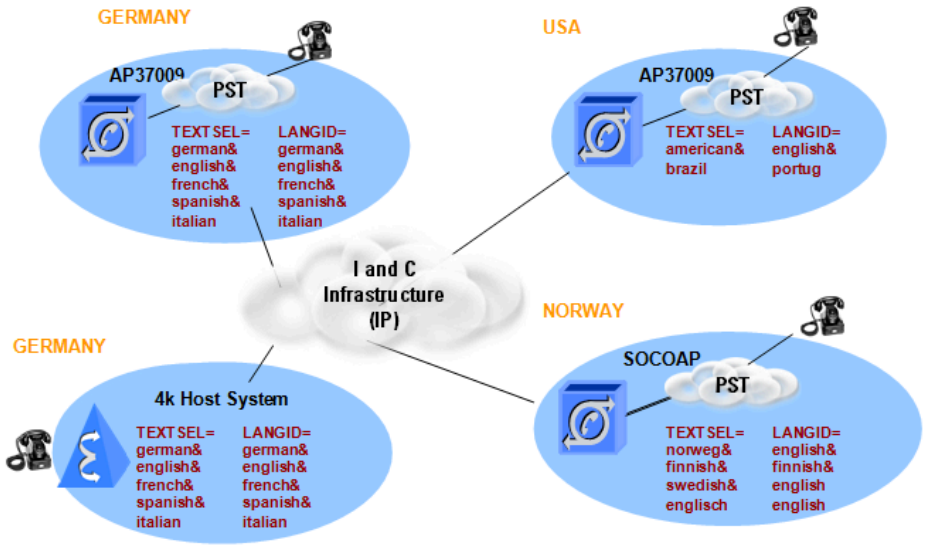
AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SSC	TYP=EXTANS	d	Externe Ansage
	TYPE=EXTANN	e	External announcement
	LTU	d	LTU-Nummer
	LTU	e	LTU Number
UCSU	CPTON	d	Vermittlungstechnischer Ton
	CP	e	Call processing tone
	HZE	d	Auswahl der länderspezifischen Hörzeichenempfängertabelle
	DTR	e	Selection of country-specific dial tone receiver table
	KONVLAW	d	A-Law/Mu-Law Konvertierung auf der NCUIx-Baugruppe
	CONVLAW	e	A-Law/Mu-Law conversion on NCUIx board
	LANDKZ	d	Loadwarevariante für SLMA2 / SLMAR
	CNTRYCD	e	Loadware variant for SLMA2 / SLMAR
	SIU	d	Auswahl der länderspezifischen SIU-Tontabelle
	SIUC	e	Selection of country-specific SIU tone table
	SIUSPKZ	d	Sprachkennzeichen für SIU-Texte

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SIUANN	e	Set options for SIU announcement texts
	SIUTON	d	Zugeordneter Ton der SIU
	SIU	e	Assigned siu tones
ZAND	HZE	d	Auswahl der länderspezifischen Hörzeichenempfängertabelle
	DTR	e	Selection of country-specific dial tone receiver table
	LANDKZ	d	Loadwarevariante für SLMA2 / SLMAR
	CNTRYCD	e	Loadware variant for SLMA2 / SLMAR
	SIU	d	Auswahl der länderspezifischen SIU-Tontabelle
	SIUC	e	Selection of country-specific SIU tone table
	SIUSPKZ	d	Sprachkennzeichen für SIU-Texte und SWU-Displaytexte
	SIUANN	e	Set options for SIU announcement texts
	TYP=TONTBL	d	Zuordnungstabelle CP-Ton -> SIU-Ton
	TYPE=TONES	e	Tone table, assignment of CP tones to SIU tones
	CPTON	d	Vermittlungstechnischer Ton
	CP	e	Call processing tone
	SIUTON	d	Zugeordneter Ton der SIU
	SIU	e	Assigned siu tones

10.2.17 Verschiedene Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point

Es können individuell für jeden Access Point unterschiedliche Paare von Sprachen/nationalen Zeichensätzen für Textanzeigen an Endgeräten konfiguriert werden. Außerdem können die Einstellungen auch unterschiedlich zum Host System sein. Daher können an einem Endgerät, dass an einen Access Point angeschlossen ist andere Display-Sprachen zur Verfügung stehen als an einem Endgerät, dass am Host System angeschlossen ist.

10.2.17.1 Leistungsmerkmalbeschreibung



Sprachen/nationale Zeichensätze für Textanzeigen pro Access Point

Dieses Leistungsmerkmal ermöglicht es für jeden Access Point individuell fünf Sprachen zu konfigurieren. Dies geschieht über den AMO UCSU, Parameter **TEXTSEL**. Dies können entweder die gleichen Sprachen wie im Host System oder unterschiedliche Sprachen sein. Außerdem können entweder für alle Access Points/OpenScape 4000 SoftGates die gleichen Sprachen oder individuell für jeden Access Point unterschiedliche Sprachen konfiguriert werden.

Da für Access Points/OpenScape 4000 SoftGates individuelle Sprachen eingestellt werden können, sind auch die entsprechenden nationalen Zeichensätze (AMO UCSU, Parameter **SPRACHID**) Access Point spezifisch einstellbar. Für das Host System können weiterhin 5 Zeichensätze (die für alle Host-Shelves gleich sind) eingestellt werden (AMO ZAND, Parameter **SPRACHID**).

Analog zum Host System (AMO ZAND, Parameter **TEXTSEL**) gilt auch für Access Points/OpenScape 4000 SoftGates, dass die erste mit AMO UCSU, Parameter **TEXTSEL** eingestellte Sprache die Default-Sprache für den entsprechenden Access Point ist.

Alle Endgeräte die am Host System angeschlossen sind, verwenden die Default-Sprache des Host System als Vorzugssprache. Endgeräte, die an einem Access Point angeschlossen sind, verwenden die Default-Sprache des entsprechenden Access Points/OpenScape 4000 SoftGate als Vorzugssprache.

Die Vorzugssprache eines Endgerätes kann weiterhin mit AMO SBCSU bzw. SCSU individuell geändert werden. Es sind allerdings nur die Sprachen möglich, die für das Shelf (an dem das Endgerät konfiguriert ist) gültig sind.

10.2.17.2 Serviceinformation

Allgemeine Hinweise

- Dieses Leistungsmerkmal wird ab OpenScape 4000 V7 R0 unterstützt.

- Die Sprachen für Textanzeigen sind unabhängig von anderen länderspezifischen Einstellungen (z.B. Ansagen oder Töne) konfigurierbar.
- Das Leistungsmerkmal ist sowohl für traditionelle Access Points als auch für Soft Access Points (z.B. OpenScape 4000 SoftGate, OpenScape Access) gültig.
- Die verwendeten Werte für **TEXTSEL** und **SPRACHID** müssen zusammen passen.
- Das Transferieren der Spracheinstellung für das Leistungsmerkmal „PIN mobil“ ist weiterhin möglich. Das bedeutet, dass nach der Identifikation die Vorzugssprache der Heimatstation verwendet wird. Voraussetzung ist allerdings, dass die Sprache der Heimatstation auch für das Shelf konfiguriert ist, an dem die Besuchsstation angeschlossen ist. Ist dies nicht der Fall, so wird die erste Sprache des besuchten Shelfs eingestellt.
- Das Gleiche gilt für das Leistungsmerkmal „Mobile HFA“. Nach dem mobile Login wird die Vorzugssprache der Heimatstation verwendet. Voraussetzung ist ebenfalls, dass die Sprache der Heimatstation auch für das Shelf konfiguriert ist, an dem die Besuchsstation angeschlossen ist. Ist dies nicht der Fall, so wird die erste Sprache des besuchten Shelfs eingestellt.
- Sprachwahl am Endgerät ist wie gewohnt möglich , d.h. die Sprache kann mittels Sprachwahltaste geändert werden. Zur Auswahl stehen die Sprachen, die für das Shelf konfiguriert sind, an dem das Endgerät angeschlossen ist.
- Es ist nach wie vor möglich , die Sprache für ein einzelnes Endgerät (über AMO SBCSU oder AMO SCSU) zu ändern.
- Werden die Änderungen an einem Access Point der schon in Betrieb ist mittels AENDERN-UCSU durchgeführt, dann müssen die Texte geladen bzw. der Zeichensatz eingestellt werden. Erst dann ist die Änderung wirksam. Dies erfolgt durch
- – ein Rücksetzen des Access Points:

  RESTART-USSU:RESTYP=LTU,LTU=<LTU nummer>;

  – Hard-Restart mit Rücksetzen der Peripherie

  AENDERN-ZANDE:TYP=LOADBHV,PIT=HRBHV,LOAD=LWLOAD;

  und

  EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=RELOAD;

  oder

  – Reload

  EXEC-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=RELOAD;

Einschränkung

Mit Einführung dieses Leistungsmerkmals kann keine „System Default-Sprache“ mehr konfiguriert werden.

Wenn weiterhin eine Default-Sprache für das ganze System eingestellt werden soll, so darf entweder:

- für Access Points keine eigenen Sprachen mit AMO UCSU eingestellt werden. In diesem Fall gelten dann nämlich die im Host System mit AMO ZAND konfigurierten Sprachen.

oder

- die erste Sprache für Host-Shelves und alle Access Points muss gleich sein (Parameter **TEXTSEL** für erste Sprache in AMO ZAND und in AMO UCSU).
- Beispiel:

  Bei CMI Endgeräten wird die Sprache für Menütexte (z.B. „WAHLWIEDERHOLUNG“) mittels CATool für alle CMI Endgeräten des Systems identisch eingestellt. Dazu wird die Default-Sprache des Systems verwendet.

  Die Service-Menütexte (z.B. "Bitte wählen") werden in der Sprache dargestellt, die für das jeweilige CMI Endgerät konfiguriert ist (mittels AMO SBCSU). Diese Sprache kann aus den für Host-Shelves bzw. AP-Shelves konfigurierten Sprachen ausgewählt werden (je nachdem, ob das CMI Endgerät an einem Host- oder AP-Shelf konfiguriert ist). Wenn für alle CMI Endgeräte die Sprache für die Service-Menütexte gleich der Sprache für die Menütexte sein soll, so muss die erste Sprache bei ZAND und UCSU identisch sein mit der Sprache für Menütexte; dies entspricht dann der „System Default-Sprache“.

10.2.17.3 Generierung (Beispiel)

Wenn alle Access Points die gleichen Spracheinstellungen bekommen wie das Host System, kann die Konfiguration unverändert zur Vorgängervariante durchgeführt werden. Es ist allerdings darauf zu achten, dass zuerst die systemweiten Einstellungen (mittels AMO ZAND) durchgeführt werden müssen, bevor die Access Points konfiguriert werden. Systemweite Einstellungen, die nachträglich geändert werden, gelten nur noch für Host-Rahmen. Wenn diese auch für Access Points gültig sein sollen, müssen sie einzeln für jeden betroffenen Access Point eingestellt werden.

10.2.17.3.1 Access Point mit den gleichen Einstellungen wie das Host System

Zuerst werden die Parameter für das Host System eingestellt (z.B. deutsch, englisch, französisch, spanisch und italienisch):

```
AENDERN-
ZAND:TYP=DATEN2,TEXTSEL=deutsch&englisch&franzoes&spanisch&itali
en;
AENDERN-
ZAND:TYP=OPTISET,SPRACHID=deutsch&englisch&franzoes&spanisch&ita
lien;
```

Nun können für einen Access Point die gleichen Texte/Zeichensätze wie für das Host System verwendet werden:

Wenn die Parameter **TEXTSEL** und **SPRACHID** nicht angegeben sind, werden diese automatisch aus den zentralen Einstellungen übernommen:

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2324-X
",SRCGRP=17,FRMTYPE=AP37009,CONNTYPE=APDL,LSRTADDR=198.16.16.63,
APRTADDR=198.16.16.150,LOCID=017,LOCATION="LOCATION",PHONE=3140,
FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=NO,TCLASS=0,ALARMNO=0,SI
UANN=1,SIUC=0,DTR=0,CNTRYCD=0;
```

Die Parameter **TEXTSEL** und **SPRACHID** können aber auch mit den gleichen Werten angegeben werden:

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=17,LTPARTNO="Q2324-X
",SRCGRP=17,FRMTYPE=AP37009,CONNTYPE=APDL,LSRTADDR=198.16.16.63,
APRTADDR=198.16.16.150,LOCID=017,LOCATION="LOCATION",PHONE=3140,
```

```
FAX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=NO,TCLASS=0,ALARMNO=0,SI
UANN=1,SIUC=0,DTR=0,CNTRYCD=0,TEXTSEL=GERMAN&ENGLISH&FRENCH&SPAN
ISH&ITALIAN,LANGID=GERMAN&ENGLISH&FRENCH&SPANISH&ITALIAN;
```

10.2.17.3.2 Access Point mit anderen Einstellungen als das Host System

Zuerst werden die Parameter für das Host System eingestellt (z.B. deutsch, englisch, französisch, spanisch und italienisch):

```
AENDERN-
ZAND:TYP=DATEN2,TEXTSEL=deutsch&englisch&franzoes&spanisch&itali
en;
AENDERN-
ZAND:TYP=OPTISET,SPRACHID=deutsch&englisch&franzoes&spanisch&ita
lien;
```

Nun können für einen Access Point die Texte/Zeichensätze mit anderen Werten eingestellt werden (z.B. amerikanisch und brasilianisch):

```
ADD-UCSU:UNIT=AP,LTG=1,LTU=20,LTPARTNO="Q2329-X
",SRCGRP=20,FRMTYPE=SOCOAP,CONNTYPE=APDL,LSRTADDR=198.16.16.20,A
PRTADDR=198.16.16.150,LOCID=020,LOCATION="LOCATION",PHONE=3140,F
AX=3141,PLCHECK=YES,BCHLCNT=60,CONVLAW=YES,TCLASS=0,ALARMNO=0,SI
UANN=D,SIUC=K,DTR=K,CNTRYCD=K,TEXTSEL=AMERICAN&BRAZIL,LANGID=ENG
LISH&PORTUG;
```

10.2.17.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
UCSU	TEXTSEL	d	Grundeinstellungen für die teilnehmerindividuelle Einstellung der Sprache der Ausgabetexte im Display pro Access Point. Jede Sprache kann nur einmal eingegeben werden. Doppeleinträge werden nach Meldung H14 ignoriert. Die Sprachen werden nacheinander eingetragen, wobei der erste Eintrag als Standardwert im Shelf verwendet wird. Werden weniger als 5 Sprachen eingegeben, werden die restlichen Felder mit „Leerzeichen“ belegt. Außerdem wird überprüft, ob zur einzutragenden Sprache das Textsubsystem auf Hard Disk vorhanden ist. Falls nicht, wird die Sprache nach Meldung F34 ignoriert.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	TEXTSEL	e	General settings for individual language setting of display texts. None of the languages may be stated more than once. The multiple entries will be ignored and the advisory message H14 will be displayed. All languages are entered one after the other, whereby the first language is used as default value for the shelf. If less than 5 languages are entered, the remaining places of the table are filled with blank. There is an additional check if the corresponding text subsystems are available on the hard disk. If not, the language will be ignored and the message F34 will be displayed.
	SPRACHID	d	Festlegen des nationalen Zeichensatzes für das Display
	LANGID	e	National character set for display

10.3 Lastkalkulation

Die folgenden Bitraten-Berechnungen berücksichtigen jeweils nur eine Richtung. Der Weg zurück benötigt dieselbe Bitrate.

Wenn ein „Shared Medium“ für beide Richtungen benutzt wird, d.h. beide Richtungen gehen über dieselbe Leitung, müssen beide Richtungen in die Kalkulation einbezogen werden. Dies ist bei 10Base5, 10Base2 und 10BaseT oder 100BaseT halbduplex der Fall.

Die Ethernet Media Access Schicht (MAC) ist bei den IPDA Komponenten nach dem IEEE 802.3 / DIX Ethernet II Standard mit MAC-Type 0800 (IP) realisiert. Die Alternative nach IEEE 802.3 und 802.2 LLC/SNAP ist unüblich und würde mehr Bandbreite benötigen.

Die Berechnungen wurden mit aktivem VLAN-Tagging nach IEEE 802.1q durchgeführt. Das ergibt die höhere Netzlast. Ohne VLAN-Tagging reduziert sich die Paketgröße um 4 Oktette (Bytes).

Wichtig: Im Vergleich zu den Vorgängerversionen dieser Dokumentation wurde die Bitratenberechnung umgestellt. Auf vielfachen Wunsch wird nicht mehr die Bitrate auf der physikalischen Ebene (PHY) sondern auf Media Access Ebene (MAC) angegeben. Die 8 Bytes Preamble werden nicht mehr in die Berechnung einbezogen.

Payload Transport mit RTP (Realtime Transmission Protocol)

Tabelle 51: Lastkalkulation für eine RTP Verbindung (VoIP)

Codec Typ	Sample-Größe [ms]	Payload [Oktette]	Ethernet Paketgröße [Oktette]	Verhältnis Overhead / Payload	Ethernet Last ohne Preamble [kBit/s]	Verhältnis RTP / ISDN Bitrate
G.711	20	160	222	39%	88,8	139%
G.711	**30**	**240**	**302**	**26%**	**80,5**	**126%**
G.711	60	480	542	13%	72,3	113%
G.729A	**20**	**20**	**82**	**310%**	**32,8**	**51%**
G.729A	40	40	102	155%	20,4	32%
G.729A	60	60	122	103%	16,3	25%

Das G.711 Codec erzeugt alle 125 µs ein Sample. Das G.729A Codec erzeugt alle 10 ms einen 10 Oktett-Rahmen.

Die Basis für die Overhead-Berechnungen ist folgende:

Tabelle 52: Overhead bei RTP-Verbindungen

Protokoll	Overhead
RTP	12
UDP	8
IP	20
IEEE 802.1Q VLAN-Tagging	4
Ethernet MAC (DA,SA,TYPE,FCS - keine Preamble)	18
Gesamt	**62**

Die Übertragungsbitrate hängt nicht nur vom verwendeten Codec-Typ und der Sample-Größe ab, sondern auch davon, auf welcher Stack-Ebene man die Bitrate betrachtet. Details zum Aufbau der RTP-Payload finden Sie im Abschnitt 3.3, „Berechnungsgrundlagen - Aufbau der Payload Pakete“.

In diesem Dokument wird immer der „worst case“ auf der physikalischen Schnittstelle betrachtet, d.h. der Ethernet MAC-Frame inclusive FCS bei eingeschaltetem VLAN-Tagging. Zur Berechnung der Last nach Umsetzung auf andere Medien, sind auch die Bitraten auf höheren Stack-Ebenen von Bedeutung. Die folgende Tabelle gibt die Übersicht. Die Werte sind in kBit/s angegeben und gelten für eine RTP-Verbindung in einer Richtung:

Tabelle 53: Last einer RTP-Verbindung [kBit/s] - Betrachtung nach Stack-Ebene

Stack-Ebene (Protokoll)	Codec Typ / Sample Größe					
	G.711			G.729		
	20 ms	30 ms	60 ms	20 ms	30 ms	60 ms
RTP	68,8	67,2	65,6	12,8	10,4	9,6
UDP	72,0	69,3	66,7	16,0	12,0	10,7
IP	80,0	74,7	69,3	24,0	16,0	13,3
Ethernet ohne Preamble ohne VLAN-TAG	84,0	79,5	71,7	31,2	19,6	15,7
Ethernet ohne Preamble mit VLAN-TAG	85,6	80,5	72,3	32,8	20,4	16,3
Ethernet mit Preamble ohne VLAN-TAG	87,2	81,6	72,8	34,4	21,2	16,8
Ethernet mit Preamble mit VLAN-TAG	88,8	82,7	73,3	36,0	22,0	17,3

RTP-Last während Inaktivität bei VAD bzw. DMC-Master-Verbindungen

Wird bei eingeschalteter Voice Activity Detection „Ruhe“ erkannt, so wird vorübergehend kein Audiosignal übertragen. Trotzdem geht die Last auf der RTP-Verbindung nicht ganz nach Null. Denn zur Prüfung der Verbindung und (Codec-abhängig) zur Übertragung des Hintergrundgeräusches werden auf der RTP-Verbindung weiterhin Daten übertragen. Diese Daten heißen SID-Frames (**S**ilence **I**nsertion **D**escriptor). Die RTCP-Verbindung ist von VAD nicht betroffen.

Tabelle 54: Last einer RTP-Verbindung [kBit/s] bei VAD während Inaktivität

Stack-Ebene (Protokoll)	Codec Typ	
	G.711	G.729
RTP	1,8	1,1
UDP	2,5	1,8

IP	4,1	3,4
Ethernet, ohne Preamble, ohne VLAN-TAG	4,9	4,2
Ethernet, ohne Preamble, mit VLAN-TAG	5,2	4,5
Ethernet, mit Preamble, ohne VLAN-TAG	5,5	4,8
Ethernet, mit Preamble, mit VLAN-TAG	5,8	5,1

Kontrolle der Payload-Verbindung durch die parallele RTCP-Verbindung (Realtime Transmission Control Protocol)

Je RTP-Verbindung wird alle 5 Sekunden von jedem beteiligten Verbindungspartner eine **Sender Report** Meldung geschickt. Es werden keine Receiver Reports geschickt. Das ergibt eine Last von 0,2 kBit/s in jede Richtung. Die Paketgröße wurde wieder mit VLAN-Tag und Preamble gerechnet.

Tabelle 55: Lastkalkulation für eine RTCP-Verbindung

Report Typ	Report Intervall [s]	durchschnittliche Ethernet Paketgröße [Oktette]	Ethernet Last ohne Preamble [kBit/s]
Sender Report	5	130	**0,2**

10.3.1 Lastkalkulation für Access Points

Wichtig: Die veranschlagte Bandbreite von 32kBit/s (Mindestbandbreite) bzw. 64kBit/s für TCP-Signalisierung ist für den vermittlungstechnischen Betrieb ausreichend. Aallerdings wird auch die Inbetriebnahme und das Laden der Baugruppen in einem AP-Shelf (teilweise grosse Loadwaremengen) über TCP geregelt und somit können sehr lange Inbetriebnahmezeiten die Folge sein!

Kalkulation der hochprioren Last für einen einzelnen Access Point

Tabelle 56: Hochpriore Last eines Access Points (G.711 / 20 ms Sample Size)

Protokoll	Datenart	Maximale Bitrate pro Port kBit/s]	Gesamtbitrate [kBit/s] mit N Payload-Ports		
			N=30	N=60	N=120
RTP	VoIP	88,8	2.664	5.328	10.656
RTCP	VoIP	0,2	6	12	25
TCP/IP	Signalisierung	64,0	64	64	64

Protokoll	Datenart	Maximale Bitrate pro Port kBit/s]	Gesamtbitrate [kBit/s] mit N Payload-Ports		
			N=30	N=60	N=120
TCP/IP	Supervisory (nur wenn Signaling Supervisory konfiguriert ist)	0,1	4	8	15
Gesamtlast			**2.738**	**5.412**	**10.760**

Die benötigte Bitrate für eine Überwachungsverbindung hängt von der Einstellung des Keep-Alive-Timers für diese Verbindung ab. Der Parameter dafür ist SUPVTIME im TIMING-Zweig des AMO SIPCO. In der Tabelle wurde der Maximalwert angegeben.

Die ebenfalls hochpriore Last, welche durch Signalisierung und Steuerung zwischen OpenScape 4000 Zentrale und einem Access Point erzeugt wird, wurde pauschal mit 64 kBit/s angegeben.

Die tatsächliche Last hängt aber von der Anzahl der Teilnehmer-, Amts- und Querverbindungen ab und vom tatsächlichen Telefonierverhalten im Access Point. 64 kBit/s ist ein Wert der mit Sicherheit immer ausreicht, die tatsächliche Last wird meist wesentlich geringer ausfallen.

Werden jedoch Baugruppen nachgeladen, so entsteht zusätzliche Last, welche, bei begrenzter Bandbreite, die Signalisierung verzögern kann.

Das absolut erforderliche Minimum an Signalisierungsbandbreite liegt bei 32 kBit/s. Stehen weniger als 64 kBit/s Signalisierungsbandbreite zur Verfügung, so muss das Traffic Shaping aktiviert und auf die tatsächlich verfügbare Bandbreite eingestellt werden. Siehe Abschnitt 2.7.1, „Begrenzung der nutzbaren Signalisierungsbandbreite (Traffic Shaping)“.

Zusätzlich zur hochprioren Last kommen in bestimmten Situationen noch niederpriore Lastanteile für:

1) SNMP Abfragen durch das Netzwerkmanagement

2)
- TAP/Service PC Zugang am Access Point
- FTP-Laden einer neuen HG 3575 Loadware als Hintergrundjob

Hochpriore Last eines Access Points in Abhängigkeit von Codec-Typ und Sample-Größe

Tabelle 57: Hochpriore Last AP in Abhängigkeit von Codec und Sample-Größe

Codec Typ	Sample Größe	RTP-Last [kBit/s] mit N Payload Ports			Gesamte Ethernet Last kBit/s] mit N Payload Ports		
		N=30	N=60	N=120	N=30	N=60	N=120
G.711	20	2.664	5.328	10.656	2.738	5.412	10.760

Codec Typ	Sample Größe	RTP-Last [kBit/s] mit N Payload Ports			Gesamte Ethernet Last kBit/s] mit N Payload Ports		
		N=30	N=60	N=120	N=30	N=60	N=120
G.711	**30**	**2.416**	**4.832**	**9.664**	**2.490**	**4.916**	**9.768**
G.711	60	2.168	4.336	8.672	2.242	4.420	8.776
G.729A	**20**	**984**	**1.968**	**3.936**	**1.058**	**2.052**	**4.040**
G.729A	40	612	1.224	2.448	686	1.308	2.552
G.729A	60	488	976	1.952	562	1.060	2.056

Hinweis

Diese Betrachtung ist mit Vorsicht zu genießen, denn die Nutzbarkeit des G.729A Codecs ist durch verschiedene Faktoren eingeschränkt:

1) Erlaubt einer der beteiligten Teilnehmer / Sätze keine Kompression, wird unkomprimiert übertragen

- Verbindungen mit Fax, Modem oder Datenendgeräten werden ausschließlich unkomprimiert übertragen
- Externe Musik und Ansagen werden meist unkomprimiert übertragen (konfigurationsabhängig (RCSU-CLASSMRK))
- Verbindungen mit einer Konferenzeinheit werden meist unkomprimiert geschaltet (konfigurationsabhängig (ZAND-IPDAVCCF))

In allen diesen Fällen wird G.711 oder kein Codec verwendet.

Es gelten damit die Bitraten für G.711.

Um garantiert nie in Engpässe der verfügbaren Bandbreite zu laufen, muss der Anschluss des Access Points also für die G.711 Bitrate ausgelegt werden.

Durch statistische Betrachtungen unter Berücksichtigung der tatsächlichen Konfiguration (wieviele Faxe/Datengeräte gibt es tatsächlich, wieviele Kompressionslizenzen sind verfügbar, sind alle möglichen Teilnehmer- / Verbindungssätze für Kompression eingerichtet, wie häufig werden Konferenzen genutzt) kann eine Mischkalkulation durchgeführt werden.

Die Last in Abhängigkeit einer Sample-Größe kann nur genommen werden, wenn sichergestellt ist, dass alle IPDA Komponenten ausschließlich auf diese Sample-Größe eingestellt sind. Sonst müsste zur Sicherheit der schlechteste Wert für den jeweiligen Codec-Typ genommen werden.

Hochpriore Last eines Access Points in Abhängigkeit von der maximalen B-Kanalzahl

Tabelle 58: Hochpriore Last AP in Abhängigkeit von der erlaubten B-Kanalzahl

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
1	153	145	137
2	242	226	209
3	331	306	282
4	420	387	354
5	509	468	427
6	598	549	499
7	687	629	571
8	776	710	644
9	865	791	716
10	954	872	789
11	1.043	952	861
12	1.132	1.033	934
13	1.221	1.114	1.006
14	1.310	1.195	1.079
15	1.399	1.275	1.151
16	1.488	1.356	1.224
17	1.577	1.437	1.296
18	1.666	1.517	1.369
19	1.755	1.598	1.441
20	1.844	1.679	1.514
21	1.933	1.760	1.586
22	2.022	1.840	1.659
23	2.111	1.921	1.731
24	2.200	2.002	1.804

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
25	2.289	2.083	1.876
26	2.378	2.163	1.948
27	2.467	2.244	2.021
28	2.556	2.325	2.093
29	2.645	2.406	2.166
30	2.734	2.486	2.238
31	2.823	2.567	2.311
32	2.912	2.648	2.383
33	3.001	2.729	2.456
34	3.090	2.809	2.528
35	3.179	2.890	2.601
36	3.268	2.971	2.673
37	3.357	3.052	2.746
38	3.446	3.132	2.818
39	3.535	3.213	2.891
40	3.624	3.294	2.963
41	3.713	3.375	3.036
42	3.802	3.455	3.108
43	3.891	3.536	3.181
44	3.980	3.617	3.253
45	4.069	3.697	3.325
46	4.158	3.778	3.398
47	4.248	3.859	3.470
48	4.337	3.940	3.543
49	4.426	4.020	3.615
50	4.515	4.101	3.688
51	4.604	4.182	3.760

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
52	4.693	4.263	3.833
53	4.782	4.343	3.905
54	4.871	4.424	3.978
55	4.960	4.505	4.050
56	5.049	4.586	4.123
57	5.138	4.666	4.195
58	5.227	4.747	4.268
59	5.316	4.828	4.340
60	5.405	4.909	4.413
61	5.494	4.989	4.485
62	5.583	5.070	4.558
63	5.672	5.151	4.630
64	5.761	5.232	4.703
65	5.850	5.312	4.775
66	5.939	5.393	4.847
67	6.028	5.474	4.920
68	6.117	5.555	4.992
69	6.206	5.635	5.065
70	6.295	5.716	5.137
71	6.384	5.797	5.210
72	6.473	5.878	5.282
73	6.562	5.958	5.355
74	6.651	6.039	5.427
75	6.740	6.120	5.500
76	6.829	6.200	5.572
77	6.918	6.281	5.645
78	7.007	6.362	5.717

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
79	7.096	6.443	5.790
80	7.185	6.523	5.862
81	7.274	6.604	5.935
82	7.363	6.685	6.007
83	7.452	6.766	6.080
84	7.541	6.846	6.152
85	7.630	6.927	6.224
86	7.719	7.008	6.297
87	7.808	7.089	6.369
88	7.897	7.169	6.442
89	7.986	7.250	6.514
90	8.075	7.331	6.587
91	8.164	7.412	6.659
92	8.253	7.492	6.732
93	8.342	7.573	6.804
94	8.431	7.654	6.877
95	8.520	7.735	6.949
96	8.609	7.815	7.022
97	8.698	7.896	7.094
98	8.787	7.977	7.167
99	8.876	8.058	7.239
100	8.965	8.138	7.312
101	9.054	8.219	7.384
102	9.143	8.300	7.457
103	9.232	8.380	7.529
104	9.321	8.461	7.601
105	9.410	8.542	7.674

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
106	9.499	8.623	7.746
107	9.588	8.703	7.819
108	9.677	8.784	7.891
109	9.766	8.865	7.964
110	9.855	8.946	8.036
111	9.944	9.026	8.109
112	10.033	9.107	8.181
113	10.122	9.188	8.254
114	10.211	9.269	8.326
115	10.300	9.349	8.399
116	10.389	9.430	8.471
117	10.478	9.511	8.544
118	10.567	9.592	8.616
119	10.656	9.672	8.689
120	10.745	9.753	8.761

10.3.2 Lastkalkulation für eine HG 3500

Kalkulation der hochprioren Last für eine HG 3500

Tabelle 59: Hochpriore Last einer HG 3500 (G.711 / 20 ms Sample Size)

Protokoll	Datenart	Maximale Bitrate pro Port kBit/s]	Gesamtbitrate [kBit/s] mit N Payload-Ports		
			N=30	N=60	N=120
RTP	VoIP	88,8	2.664	5.328	10.656
RTCP	VoIP	0,2	6	12	25
Gesamtlast			**2.670**	**5.340**	**10.681**

Zusätzlich zur hochprioren Last kommen in bestimmten Situationen noch niederpriore Lastanteile für:

1) SNMP Abfragen durch das Netzwerkmanagement

- TAP/Service PC Zugang am Access Point
- FTP-Laden einer neuen HG 3575 Loadware als Hintergrundjob

Hochpriore Last einer HG 3500 in Abhängigkeit von Codec-Typ und Sample-Größe

Tabelle 60: Hochpriore Last HG 3500 in Abhängigkeit von Codec und Sample-Größe

Codec Typ	Sample Größe	RTP-Last [kBit/s] mit N Payload Ports			Gesamte Ethernet Last kBit/s] mit N Payload Ports		
		N=30	N=60	N=120	N=30	N=60	N=120
G.711	20	2.664	5.328	10.656	2.670	5.412	10.760
G.711	**30**	**2.416**	**4.832**	**9.664**	**2.490**	**4.916**	**9.768**
G.711	60	2.168	4.336	8.672	2.242	4.420	8.776
G.729A	**20**	**984**	**1.968**	**3.936**	**1.058**	**2.052**	**4.040**
G.729A	40	612	1.224	2.448	686	1.308	2.552
G.729A	60	488	976	1.952	562	1.060	2.056

Hinweis

Diese Betrachtung ist mit Vorsicht zu genießen, denn die Nutzbarkeit des G.729A Codecs ist durch verschiedene Faktoren eingeschränkt:

1) Erlaubt einer der beteiligten Teilnehmer / Sätze keine Kompression, wird unkomprimiert übertragen

- Verbindungen mit Fax, Modem oder Datenendgeräten werden ausschließlich unkomprimiert übertragen
- Externe Musik und Ansagen werden meist unkomprimiert übertragen (konfigurationsabhängig (RCSU-CLASSMRK))
- Verbindungen mit einer Konferenzeinheit werden meist unkomprimiert geschaltet (konfigurationsabhängig (ZAND-IPDAVCCF))

In allen diesen Fällen wird G.711 oder kein Codec verwendet.

Es gelten damit die Bitraten für G.711.

Um garantiert nie in Bandbreitenengpässe zu laufen, muss der Anschluss des Access Points also für die G.711 Bitrate ausgelegt werden.

Durch statistische Betrachtungen unter Berücksichtigung der tatsächlichen Konfiguration (wieviele Faxe/Datengeräte gibt es tatsächlich, wieviele Kompressionslizenzen sind verfügbar, sind alle möglichen Teilnehmer- / Verbindungssätze für Kompression eingerichtet, wie häufig werden Konferenzen genutzt) kann eine Mischkalkulation durchgeführt werden.

Die Last in Abhängigkeit einer Sample-Größe kann nur genommen werden, wenn sichergestellt ist, dass alle IPDA Komponenten ausschließlich auf diese Sample-Größe eingestellt sind. Sonst müsste zur Sicherheit der schlechteste Wert für den jeweiligen Codec-Typ genommen werden.

Hochpriore Last einer HG 3500 in Abhängigkeit von der maximalen B-Kanalzahl

Tabelle 61: Hochpriore Last HG 3500 in Abhängigkeit von der erlaubten B-Kanalzahl

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
1	89	81	72
2	178	161	145
3	267	242	217
4	356	323	290
5	445	404	362
6	534	484	435
7	623	565	507
8	712	646	580
9	801	727	652
10	890	807	725
11	979	888	797
12	1.068	969	870
13	1.157	1.050	942
14	1.246	1.130	1.015
15	1.335	1.211	1.087
16	1.424	1.292	1.160
17	1.513	1.373	1.232
18	1.602	1.453	1.305
19	1.691	1.534	1.377
20	1.780	1.615	1.449
21	1.869	1.696	1.522

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
22	1.958	1.776	1.594
23	2.047	1.857	1.667
24	2.136	1.938	1.739
25	2.225	2.019	1.812
26	2.314	2.099	1.884
27	2.403	2.180	1.957
28	2.492	2.261	2.029
29	2.581	2.341	2.102
30	2.670	2.422	2.174
31	2.759	2.503	2.247
32	2.848	2.584	2.319
33	2.937	2.664	2.392
34	3.026	2.745	2.464
35	3.115	2.826	2.537
36	3.204	2.907	2.609
37	3.293	2.987	2.682
38	3.382	3.068	2.754
39	3.471	3.149	2.827
40	3.560	3.230	2.899
41	3.649	3.310	2.971
42	3.738	3.391	3.044
43	3.827	3.472	3.116
44	3.916	3.553	3.189
45	4.005	3.633	3.261
46	4.094	3.714	3.334
47	4.183	3.795	3.406
48	4.272	3.876	3.479

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
49	4.361	3.956	3.551
50	4.450	4.037	3.624
51	4.539	4.118	3.696
52	4.628	4.199	3.769
53	4.717	4.279	3.841
54	4.806	4.360	3.914
55	4.895	4.441	3.986
56	4.984	4.522	4.059
57	5.073	4.602	4.131
58	5.162	4.683	4.204
59	5.251	4.764	4.276
60	5.340	4.844	4.348
61	5.429	4.925	4.421
62	5.518	5.006	4.493
63	5.608	5.087	4.566
64	5.697	5.167	4.638
65	5.786	5.248	4.711
66	5.875	5.329	4.783
67	5.964	5.410	4.856
68	6.053	5.490	4.928
69	6.142	5.571	5.001
70	6.231	5.652	5.073
71	6.320	5.733	5.146
72	6.409	5.813	5.218
73	6.498	5.894	5.291
74	6.587	5.975	5.363
75	6.676	6.056	5.436

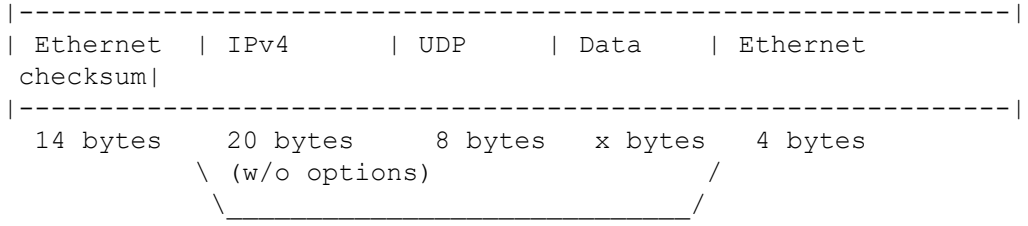
Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
76	6.765	6.136	5.508
77	6.854	6.217	5.581
78	6.943	6.298	5.653
79	7.032	6.379	5.725
80	7.121	6.459	5.798
81	7.210	6.540	5.870
82	7.299	6.621	5.943
83	7.388	6.702	6.015
84	7.477	6.782	6.088
85	7.566	6.863	6.160
86	7.655	6.944	6.233
87	7.744	7.024	6.305
88	7.833	7.105	6.378
89	7.922	7.186	6.450
90	8.011	7.267	6.523
91	8.100	7.347	6.595
92	8.189	7.428	6.668
93	8.278	7.509	6.740
94	8.367	7.590	6.813
95	8.456	7.670	6.885
96	8.545	7.751	6.958
97	8.634	7.832	7.030
98	8.723	7.913	7.103
99	8.812	7.993	7.175
100	8.901	8.074	7.247
101	8.990	8.155	7.320
102	9.079	8.236	7.392

Maximal erlaubte B-Kanalzahl	Gesamte Ethernet Last bei G.711/20ms [kBit/s]	Gesamte Ethernet Last bei G.711/30ms [kBit/s]	Gesamte Ethernet Last bei G.711/60ms [kBit/s]
103	9.168	8.316	7.465
104	9.257	8.397	7.537
105	9.346	8.478	7.610
106	9.435	8.559	7.682
107	9.524	8.639	7.755
108	9.613	8.720	7.827
109	9.702	8.801	7.900
110	9.791	8.882	7.972
111	9.880	8.962	8.045
112	9.969	9.043	8.117
113	10.058	9.124	8.190
114	10.147	9.205	8.262
115	10.236	9.285	8.335
116	10.325	9.366	8.407
117	10.414	9.447	8.480
118	10.503	9.527	8.552
119	10.592	9.608	8.624
120	10.681	9.689	8.697

10.3.3 Berechnungsgrundlagen - Aufbau der Payload Pakete

10.3.3.1 MTU-Paket

Wir arbeiten mit einer MTU Größe von 1500 Byte als Standard. Um hier mehr Klarheit zu erhalten, wie die sich zusammensetzt hier eine Übersicht:



```
                                  |
                                 MTU
```

Eine andere Darstellung:

```
  1472 bytes Nutzlast des ICMP-Protokolles
 (Transportschicht)
+    8 bytes ICMP-Header (Transportschicht)
+   20 bytes IPv4-Header (der Vermittlungsschicht)
-------------
= 1500 bytes (Nutzlast von Ethernet) /* das ist für uns der
 einge▶
stelle MTU Wert
+   14 bytes (Header der Sicherungsschicht)
+    4 bytes (Frame Check Sequence)
-------------
= 1518 bytes (kompletter Ethernetrahmen)
```

Wenn die MTU-Größe nicht größer 1500 sein darf, dann darf die OpenScape 4000 als Nutzdaten nur maximal 1472 Byte für UDP senden.

Bei einem anderen Protokoll anstelle UDP (8 Byte) z.B. TCP (20 Byte) dann ändert sich die Größe vom Header und somit die resultierende Größe für die Nutzdaten.

Es ist also in Ordnung, wenn in einem Wireshark Trace eine Paketlänge von z.B. 1510 Byte dargestellt wird. Man muss dann ausrechnen, wie groß die tatsächliche Länge (abzüglich Overhead) ist.

Anmerkung: Zur Veränderung der MTU-Paketgröße gibt es auch das Verfahren MSS Clamping. MSS Clamping wird im WAN benutzt und passt die TCP-Paketgröße im Dialog zwischen Router und OpenScape 4000 Host oder Access Point automatisch an.

10.3.3.2 Aufbau des Ethernet MAC Frames

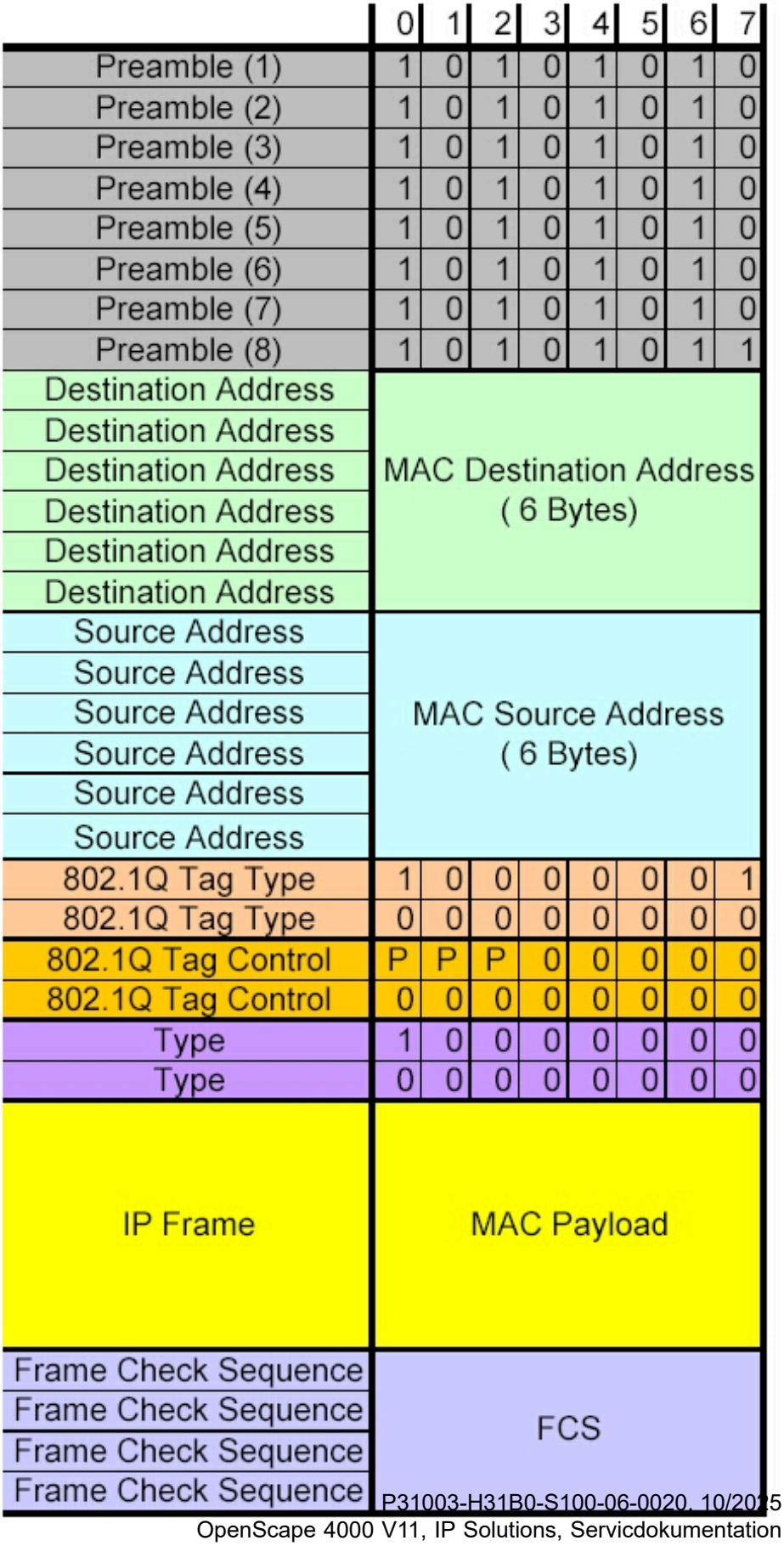
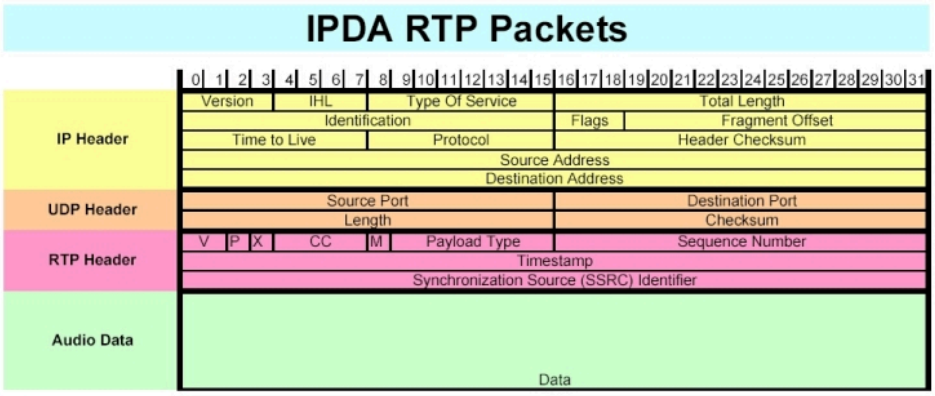


Tabelle 62: Aufbau der Ethernet MAC Frames für IPDA Payload

10.3.3.3 Aufbau des IP Frames



Version	Version of Internet Header	4
IHL	Internet Header Length	20
Type Of Service	Type of Service / Packet Handling Behavior Class acc. To DiffServ - Administrated Value	
Total Length	Length of IP datagram including header	160/280/400/520 for G.711 with 15/30/45/60 msec Audio 60/80/100 for G.729 with 20/40/60 msec Audio
Identification	ID to assemble fragments of datagram	
Flags	set to May fragment, Last fragment	0
Fragment Offset	sent unfragmented -> no offset	0
Time to Live	decremented by each instance the datagram passes	
Protocol	UDP	17
Header Checksum	Checksum on IP Header only	
Source Address	IP Address	
Destination Address	IP Address	
Source Port		
Destination Port		
Length	Length of UDP datagram including UDP header	140/260/380/500 for G.711 with 15/30/45/60 msec Audio 40/60/80 for G.729 with 20/40/60 msec Audio
Checksum	Checksum over IP Header, UDP Header und UDP Data	
V	Version of RTP	2
P	Padding	0
X	Extension	0
CC	Contributing Source (CSRC) identifiers	0
M	Marker	0
Payload Type	Payload Type (G.711 µ-law = PCMU = 0 / G.711 A-law = PCMA = 8 / G.729A = ???)	0/8/18
Sequence Number	Incremented by 1 with each RTP packet - initial value is random	
Timestamp	Timestamp for 1st sample in packet - incremented by 1 for each sampling period - every 125 µsec	
Synchronization Source (SSRC) Identifier	chosen randomly, valid only per session	

Tabelle 63: Aufbau des IP Frames für IPDA Payload

10.4 Lokale Administration des Access Points am CLI mittels Terminal

Steht für die lokale Konfiguration eines Access Points kein TAP/Service PC mit „Expertenzugang“ Applikation zur Verfügung, so kann notfalls die Administration auch direkt mit einem Terminal bzw. einer Terminalemulation erfolgen.

Die RS 232 / V.24 Schnittstelle an der HG 3575 ist beschriftet mit „Service“ und eingestellt auf 38400 Baud, 8 Bit, no Parity.

Das Command Line Interface meldet sich nach Eingabe von = mit:

1) `Please log in.`
`Username:`

Logindaten

1) neue Baugruppe (vor Inbetriebnahme)

2) Login: HP4K-DEVEL

Password: 4K-admin

3) nach Inbetriebnahme (OpenScape 4000 steuert NCUI4)

4) Login: TRM

Password: HICOM

War die Baugruppe bereits im Einsatz - und wurde dort das CLI-Login und Passwort verändert, so gelten die dort eingestellten Werte.

Nach erfolgreichem Login erscheint:

```
Welcome to the HG 3575 V4.0 <LW-Version der aktuell
 geladenen
LW> Command Line Interpreter.
vxTarget>
```

Nach dem Prompt können jetzt die notwendigen Parameter eingegeben werden.

Eine Liste aller verfügbarer Kommandos kann nun über das Kommando `help` abgefragt werden.

Das CLI unterscheidet nicht zwischen „direct link“ und „networked“ Access Points. Die Benennung der Parameter spiegelt die Programmiernamen der Loadware. Wie schon gesagt, die direkte Bedienung des CLI ohne „Expertenzugang“ Applikation ist nur eine Notlösung.

Die folgenden Tabellen sollen helfen, den richtigen Inhalt für die Parameter zu finden. Die Tabellen listen die notwendigen CLI-Parameter auf und setzen sie in Beziehung zu den AMO-Parametern, von denen die Werte abgeleitet werden müssen:

10.4.1 Networked Access Point

Wichtig: Um die folgenden Kommandos ausführen zu können, benötigen Sie ADMIN-Rechte in CLI.

Tabelle 64: CLI-Parameter für „networked“ Access Point

CLI-Parameter Name	Parameterbedeutung	AMO - Zweig - Parameter
ip_addr_eth	IP-Adresse des Access Point	APRT TYP=APNET - APIPADR
netmask_eth	Netzmaske im Netz des Access Point	APRT TYP=APNET - NETMASK
default_gateway	IP-Adresse des Default Routers im Netz des Access Point	UCSU ART=AP - APRTADR
ip_addr_signaling	IP-Adresse des Access Point	APRT TYP=APNET - APIPADR

CLI-Parameter Name	Parameterbedeutung	AMO - Zweig - Parameter
netmask_signaling	Netzmaske im Netz des Access Point	APRT TYP=APNET - NETMASK
ip_addr_CC_A	IP-Adresse des CC-A	SIPCO TYP=LSNET - CCAADR
ip_addr_CC_B	IP-Adresse des CC-B	SIPCO TYP=LSNET - CCBADR
netmask_hhs	Netzmaske des OpenScape 4000 LAN Segments	SIPCO TYP=LSNET - NETMASK
vlan_tag	VLAN-Tagging aus/ eingeschaltet [0 = AUS,1 = EIN]	STMIB: MTYP=NCUI2, TYP=IFDATA - VLAN
vlan_id	VLAN-ID [0.. 4095]	STMIB: MTYP=NCUI2, TYP=IFDATA - VLANID
eth_link_mode	Betriebsart der Ethernet-Schnittstelle 0 : Autonegotiation 21 : 10 MBit/s Halfduplex 22 : 10 MBit/s Fullduplex 23 : 100 MBit/s Halfduplex 24 : 100 MBit/s Fullduplex	STMIB: MTYP=NCUI2, TYP=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 MBit/s, Halfduplex 10MBFD: 10 MBit/s, Fullduplex 100MBHD: 100 MBit/s, Halfduplex 100MBFD: 100 MBit/s, Fullduplex

Hinweis

Für „networked“ Access Points **muss**

1) ip_addr_signaling = ip_addr_eth

und

1) netmask_signaling = netmask_eth

gesetzt werden !

Die Kommando-Syntax ist

1) `set ip address` *Parametername Wert* bzw. `set id` *Parametername Wert*

Für Access Point 99 aus den Konfigurationsbeispielen (siehe Bild 3 „OpenScape 4000 LAN Segment“ und Bild 5 „Einrichten eines „networked“ Access Points“) ergibt sich die folgende Befehlsfolge:
`get write access`

```
set ip address ip_addr_eth 192.168.23.99

set ip address netmask_eth 255.255.255.0

set ip address default_gateway 192.168.23.1

set ip address ip_addr_signaling 192.168.23.99

set ip address netmask_signaling 255.255.255.0

set ip address ip_addr_CC_A 192.168.1.1

set ip address ip_addr_CC_B 192.168.1.1

set ip address netmask_hhs 255.255.255.0

set id vlan_tag 0

set id vlan_id 0

set id eth_link_mode 0

finish
```

Wichtig: Zwischen den `set`-Kommandos und dem `finish`-Kommando, das die Daten in den Flash-Speicher übernimmt, dürfen **keine** anderen Kommandos (z.B. show) abgesetzt werden!

10.4.2 Direct Link Access Point

Wichtig: Um die folgenden Kommandos ausführen zu können, benötigen Sie ADMIN-Rechte in CLI.

Tabelle 65: CLI-Parameter für „direct link“ Access Point

CLI-Parameter Name	Parameter	AMO - Zweig - Parameter
ip_addr_eth	IP-Adresse des Access Points im OpenScape 4000 LAN Segment	UCSU ART=AP - LSRTADR
netmask_eth	Netzmaske des OpenScape 4000 LAN Segments	SIPCO TYP=LSNET - NETMASK
default_gateway	IP-Adresse des Default Routers im OpenScape 4000 LAN Segment	UCSU ART=AP - APRTADR

CLI-Parameter Name	Parameter	AMO - Zweig - Parameter
ip_addr_signaling	IP-Adresse des Access Points im AP-internen Netzsegment	APRT TYP=APNET - APIPADR
netmask_signaling	Netzmaske des AP-internen Netzsegments	APRT TYP=APNET - NETMASK
ip_addr_CC_A	IP-Adresse des CC-A	SIPCO TYP=LSNET - CCAADR
ip_addr_CC_B	IP-Adresse des CC-B	SIPCO TYP=LSNET - CCBADR
netmask_hhs	Netzmaske des OpenScape 4000 LAN Segments	SIPCO TYP=LSNET - NETMASK
vlan_tag	VLAN-Tagging aus/ eingeschaltet [0 = AUS,1 = EIN]	STMIB: MTYP=NCUI2, TYP=IFDATA - VLAN
vlan_id	VLAN-ID [0.. 4095]	STMIB: MTYP=NCUI2, TYP=IFDATA - VLANID
eth_link_mode	Betriebsart der Ethernet-Schnittstelle 0 : Autonegotiation 21 : 10 MBit/s Halfduplex 22 : 10 MBit/s Fullduplex 23 : 100 MBit/s Halfduplex 24 : 100 MBit/s Fullduplex	STMIB: MTYP=NCUI2, TYP=IFDATA - BITRATE AUTONEG: Autonegotiate 10MBHD: 10 MBit/s, Halfduplex 10MBFD: 10 MBit/s, Fullduplex 100MBHD: 100 MBit/s, Halfduplex 100MBFD: 100 MBit/s, Fullduplex

Die Kommando-Syntax ist

1) `set ip address` *Parametername Wert* bzw. `set id` *Parametername Wert*

Für Access Point 17 aus den Konfigurationsbeispielen (siehe Bild 3 „OpenScape 4000 LAN Segment“ und Bild 6 „Einrichten eines „direct link“ Access Points“) ergibt sich die folgende Befehlsfolge:

```
get write access

set ip address ip_addr_eth 192.168.1.17

set ip address netmask_eth 255.255.255.0
```

```
set ip address default_gateway 192.168.1.254

set ip address ip_addr_signaling 192.168.200.1

set ip address netmask_signaling 255.255.255.252

set ip address ip_addr_CC_A 192.168.1.1

set ip address ip_addr_CC_B 192.168.1.2

set ip address netmask_hhs 255.255.255.0

set id vlan_tag 0

set id vlan_id 0

set id eth_link_mode 0

finish
```

Wichtig: Zwischen den `set`-Kommandos und dem `finish`-Kommando, das die Daten in den Flash-Speicher übernimmt, dürfen **keine** anderen Kommandos (z.B. `show`) abgesetzt werden!

10.4.3 Zuordnung der Parameternamen im LW-CLI zu den AMO-Parametern

Die folgende Tabelle gibt abschließend einen Überblick über alle CLI-Parameter und deren Zuordnung zu den AMO-Parametern.

Tabelle 66: Zuordnung der Parameternamen im LW-CLI zu den AMO-Parametern

Parametername im LW-CLI		Parametername	AMO	Zweig
ip_addr_eth	*	APDL: LSRTADR APNW: APIPADR	UCSU APRT	ART=AP TYP=APNET
netmask_eth	*	APDL: NETMASK APNW: NETMASK	SIPCO APRT	TYP=LSNET TYP=APNET
default_gateway	*1	APRTADR	UCSU	ART=AP
ip_addr_signaling	*	APIPADR	APRT	TYP=APNET
netmask_signaling	*	NETMASK	APRT	TYP=APNET
ip_addr_survivability	*2	SURVNET (letztes Byte identisch LTU - UCSU)	SIPCO	TYP=LSNET

Parametername im LW-CLI		Parametername	AMO	Zweig
netmask_survivability	*2	fix: 255.255.255.0	-	-
gateway_survivability	*2	SURVNET (letztes Byte identisch ROUTERNR - TYP=SURV -APRT)	SIPCO	TYP=LSNET
netmask_hhs	*	NETMASK	SIPCO	TYP=LSNET
ip_addr_CC_A	*	CCAADR	SIPCO	TYP=LSNET
ip_addr_CC_B	*3	CCBADR	SIPCO	TYP=LSNET
vlan_tag		VLAN	STMIB	MTYP=NCUI2 TYP=IFDATA
vlan_id		VLANID	STMIB	MTYP=NCUI2 TYP=IFDATA
eth_link_mode		BITRATE	STMIB	MTYP=NCUI2 TYP=IFDATA
debug_details		DEBUGDET	STMIB	MTYP=NCUI2 TYP=DEBUG
file_access_mode		FACCMODE	STMIB	MTYP=NCUI2 TYP=DEBUG
server_port_signaling		fix: 4000	-	-
keep_alive_time_-signal		ALVTIME	SIPCO	TYP=TIMING
reset_timer_sign_loss		RESTIME	SIPCO	TYP=TIMING
server_port_super-visory		fix: 4001	-	-
tos_lan		TOSLAN	STMIB	MTYP=NCUI2 TYP=IFDATA
tos_modem		TOSMODEM	STMIB	MTYP=NCUI2 TYP=IFDATA
survivability_enable	*2	abgeleitet aus ip_addr_survivability > 0.0.0.0	-	-

*	Notwendiger Parameter für Erstinitialisierung NCUI2/4
***1**	Notwendiger Parameter für Erstinitialisierung NCUI2/4 *für „networked“ Access Points*

***2**	Notwendiger Parameter für Erstinitialisierung NCUI2/4 *mit Signaling Survivability*
***3**	Notwendiger Parameter für Erstinitialisierung NCUI2/4 *an Duplex-Systemen*

Bei einigen Parametern ist die Unterscheidung nach eingestellter Verbindungsart VERBART - ART=AP - UCSU nötig. Hier sind unterschiedliche Zuordnungen für APDL und APNW nötig.

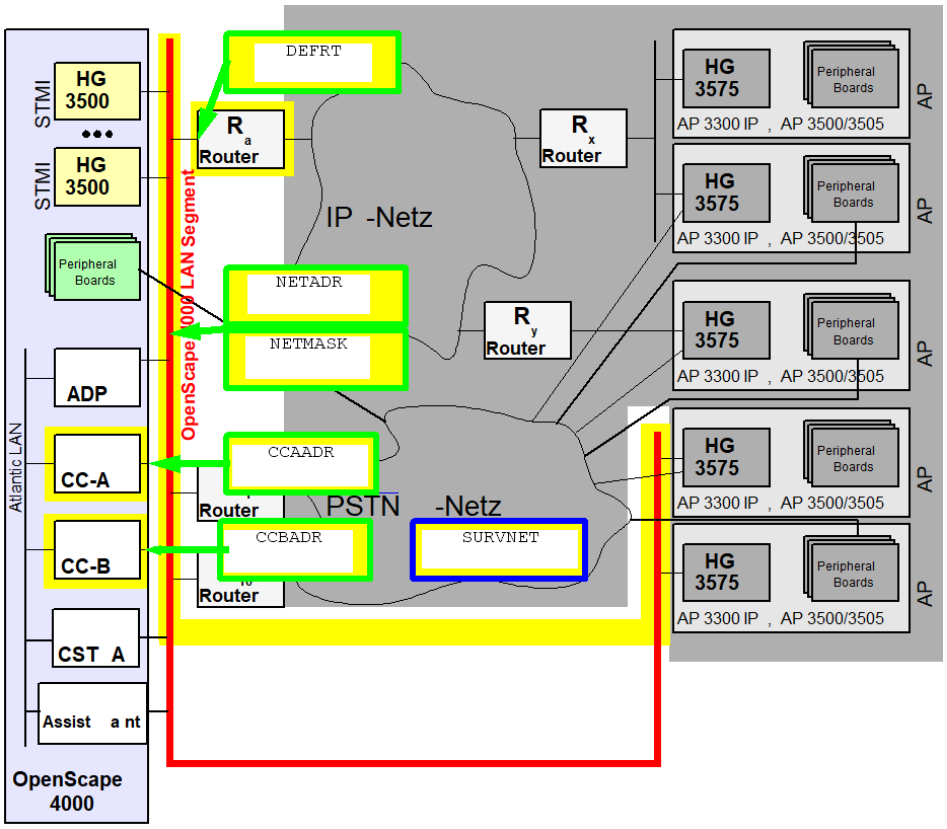
10.5 Arbeitsblätter - IPDA-Konfiguration

Die folgenden Arbeitsblätter sollen bei den ersten Schritten zu einer IPDA-Konfiguration helfen. Sie sind so angelegt, dass sich auf der Vorderseite jeweils ein Konfigurationsbild und AMO-Template zum Ausfüllen befindet, auf der Rückseite das ausgefüllte Beispiel aus dem Servicehandbuch.

Die folgenden Arbeitsblätter (mit Beispiel) werden zur Verfügung gestellt:

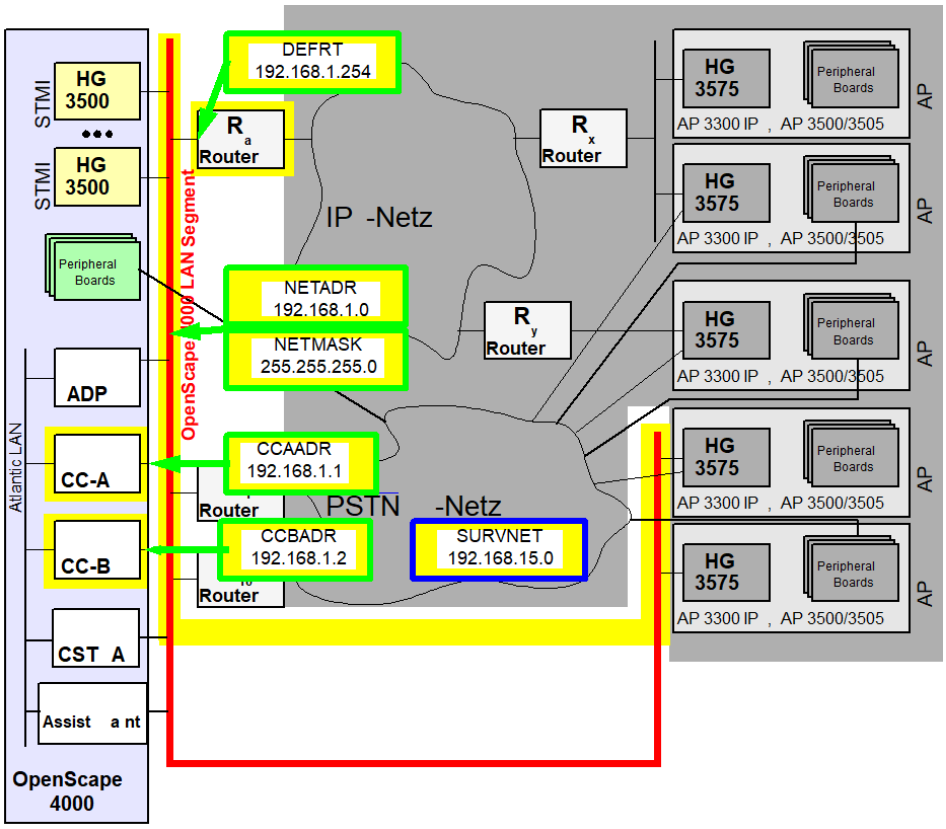
- Arbeitsblatt: Einrichten des OpenScape 4000 LAN Segments
- Arbeitsblatt: Einrichten eines „networked“ Access Points
- Arbeitsblatt: Einrichten eines „direct link“ Access Points
- Arbeitsblatt: Einrichten von OpenScape HG 3500 als HG 3570 im OpenScape 4000 System

Arbeitsblatt: Einrichten des OpenScape 4000 LAN Segments



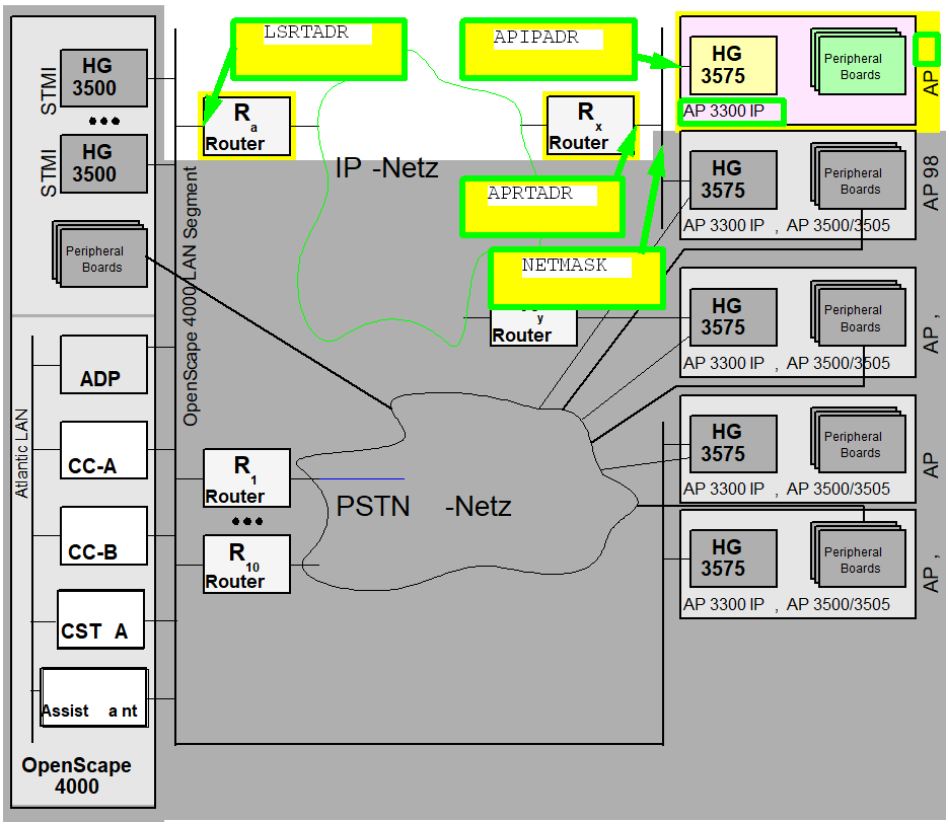
EINRICHTEN-SIPCO:	NETADR= . . . ,	NETMASK= . . . ,
	DEFRT= . . . ,	CCAADR= . . . ,
	CCBADR= . . . ,	SURVNET= . . .0;

Beispielblatt: Einrichten des OpenScape 4000 LAN Segments



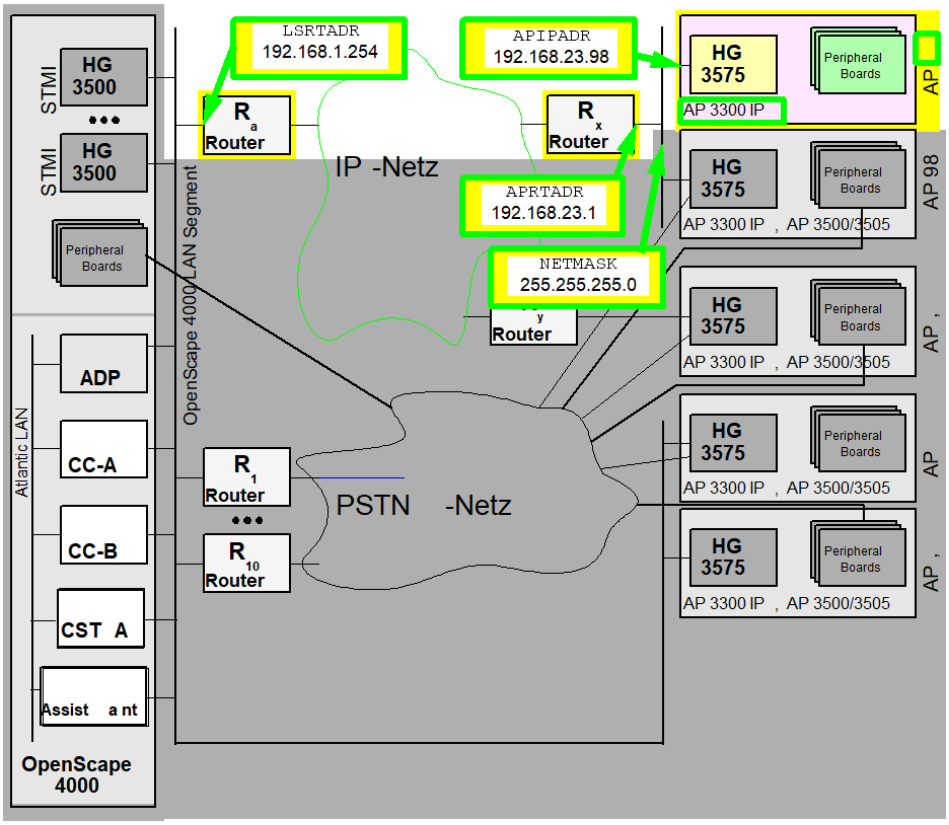
EINRICHTEN-SIPCO:	NETADR=192.168.1.0, NETMASK=255.255.255.0,
	DEFRT=192.168.1.254, CCAADR=192.168.1.1,
	CCBADR=192.168.1.2, SURVNET=192.168.15.0;

Arbeitsblatt: Einrichten eines „networked“ Access Points



EINRICHTEN-UCSU:	ART=AP,	LTU= ,
	LTSACHNR=Q23 -X ,	SRCGRP= ,
	FRAMETYP= ,	VERBART=APNW,
	LSRTADR= . . . ,	APRTADR= . . . ,
	STANDOID= ,	STANDORT=" ",
	TEL= ,	FAX= ,
	PLCHECK= ,	ANZBKAN= ,
	KONVLAW= ;	
EINRICHTEN-APRT:	TYP=APNET,	LTU= ,
	APIPADR= . . . ,	NETMASK= . . . ;

Beispielblatt: Einrichten eines „networked“ Access Points




```
EINRICHTEN-      ART=AP,                 LTU=99,
UCSU:

                 LTSACHNR=Q2305-X35,     SRCGRP=2,

                 FRAMETYP=AP37009,       VERBART=APNW,

                 LSRTADR=192.168.1.254,APRTADR=192.168.23.1,

                 STANDOID=2,             STANDORT="BLN
                                          ROHRDAMM
                                         85. GEB. 30-222",

                 TEL=03038612345,        FAX=03038654321,

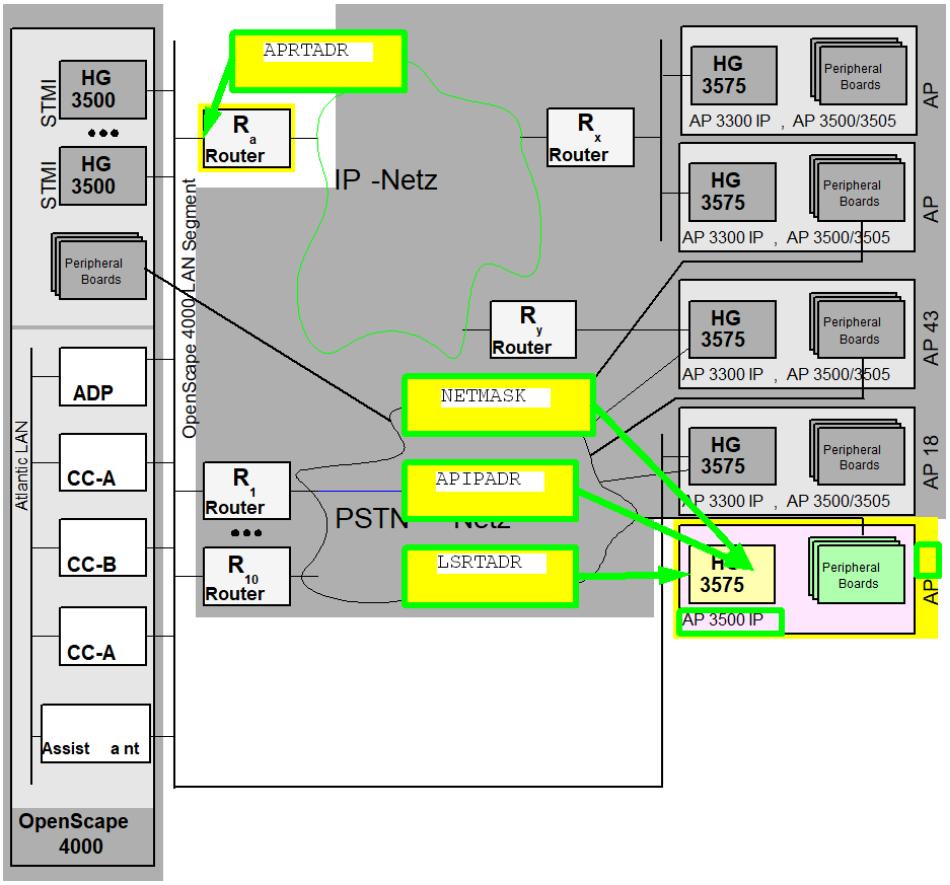
                 PLCHECK=JA,             ANZBKAN=40,

                 KONVLAW=NEIN;

EINRICHTEN-      TYP=APNET,              LTU=99,
APRT:

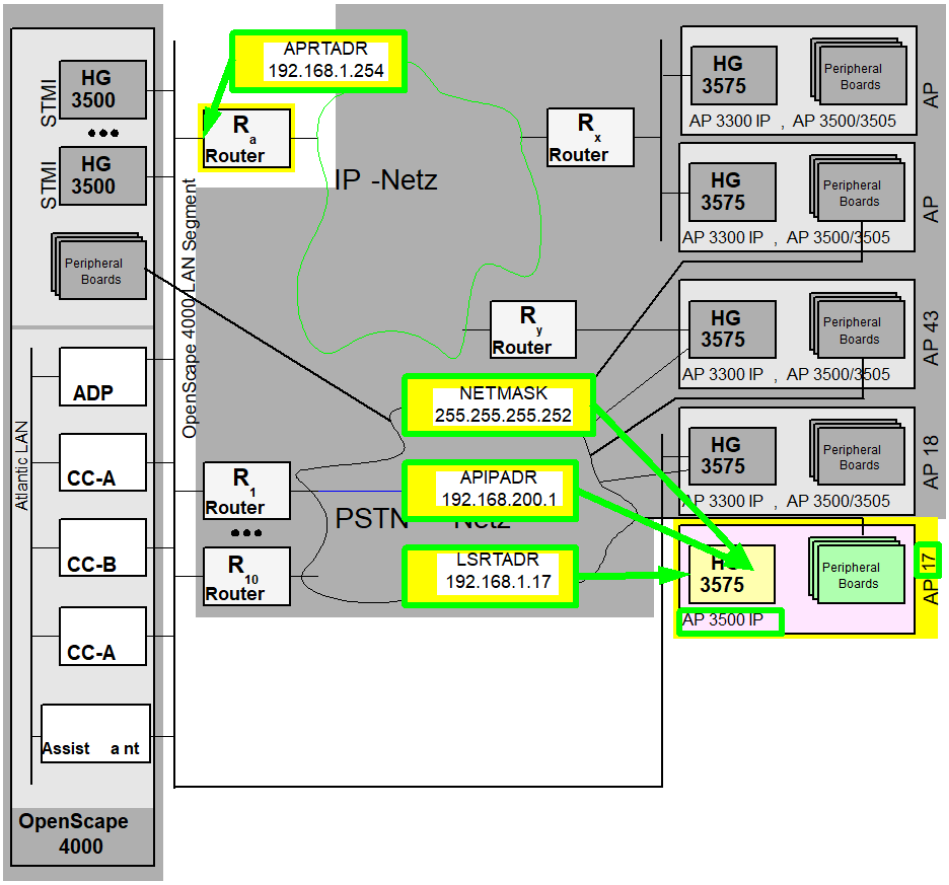
                 APIPADR=192.168.23.99,NETMASK=255.255.255.0;
```

Arbeitsblatt: Einrichten eines „direct link“ Access Points



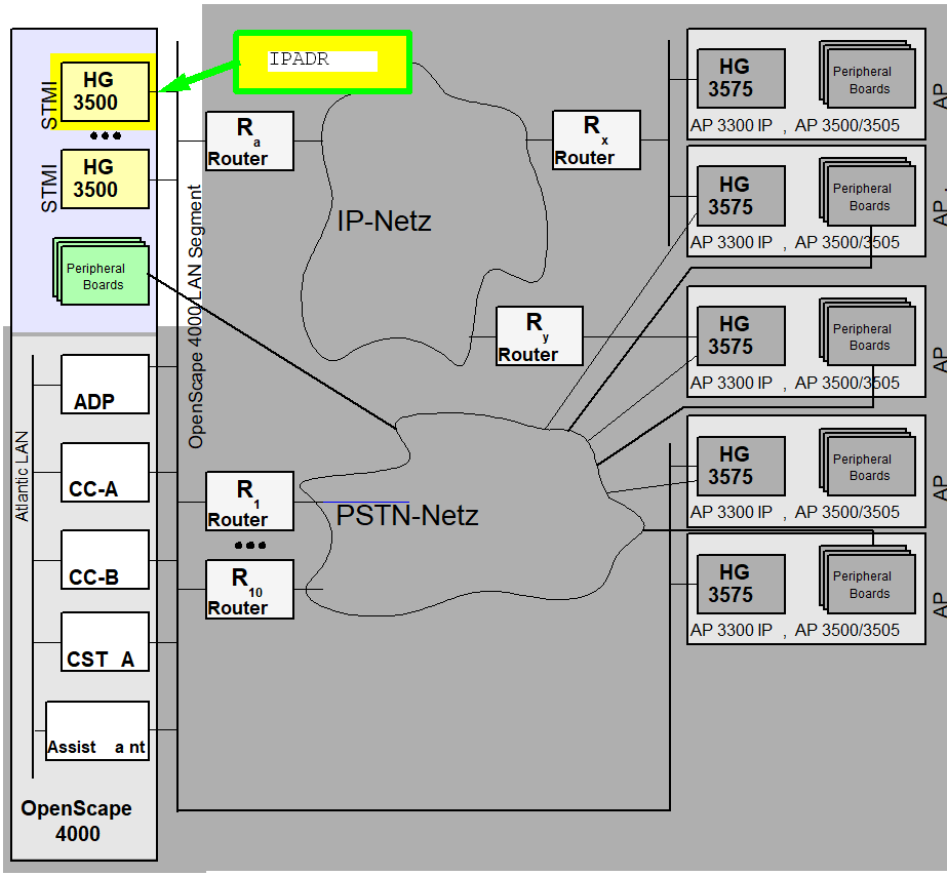
EINRICHTEN-UCSU:	ART=AP,	LTU= ,
	LTSACHNR=Q23 -X ,	SRCGRP= ,
	FRAMETYP= ,	VERBART=APDL,
	LSRTADR= . . . ,	APRTADR= . . . ,
	STANDOID= ,	STANDORT=“ “,
	TEL= ,	FAX= ,
	PLCHECK= ,	ANZBKAN= ,
	KONVLAW= ;	
EINRICHTEN-APRT:	TYP=APNET,	LTU= ,
	APIPADR= . . . ,	NETMASK= . . . ;

Beispielblatt: Einrichten eines „direct link“ Access Points



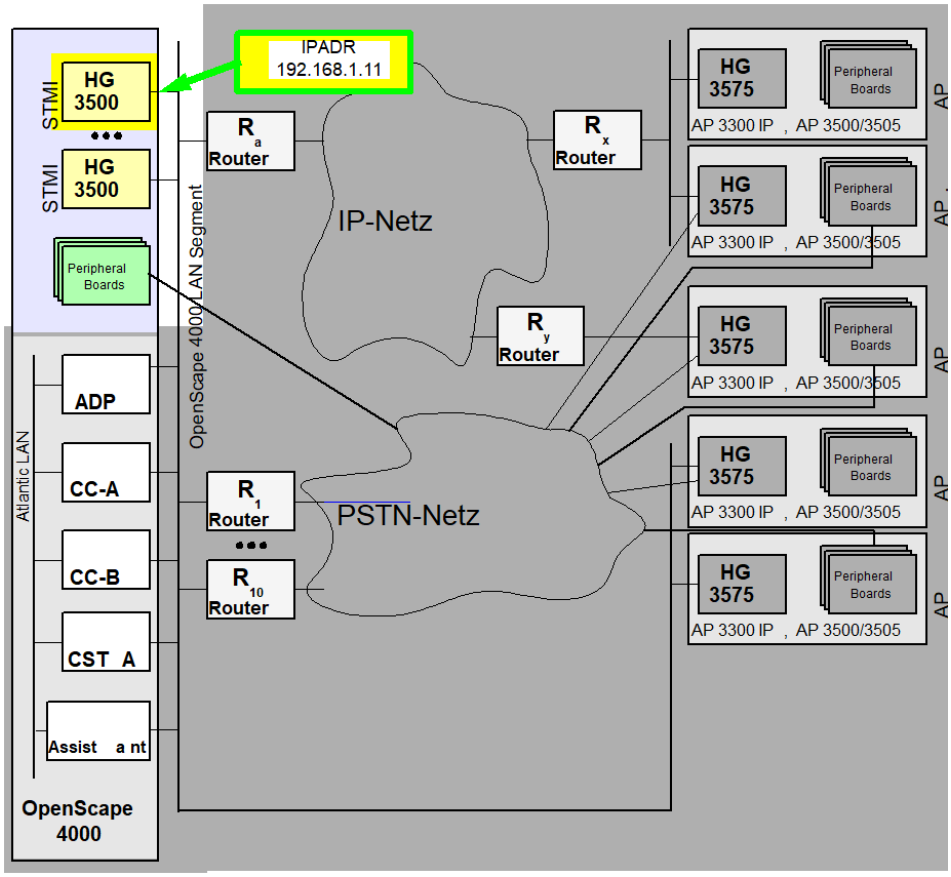
EINRICHTEN-UCSU:	ART=AP,	LTU=17,
	LTSACHNR=Q2302-X10,	SRCGRP=1,
	FRAMETYP=INCH19,	VERBART=APDL,
	LSRTADR=192.168.1.17,	APRTADR=192.168.1.254,
	STANDOID=1,	STANDORT=“MCH MACHTLFIN-GERSTR.1 GEB. 7202-111“,
	TEL=08972223456,	FAX=08972265432,
	PLCHECK=JA,	ANZBKAN=20,
	KONVLAW=NEIN;	
EINRICHTEN-APRT:	TYP=APNET,	LTU=17,
	APIPADR=192.168.200.1	NETMASK=255.255.255.252 ;

Arbeitsblatt: Einrichten von OpenScape HG 3500 als HG 3570 im OpenScape 4000 System



EINRICHTEN-BFDAT:	FCTBLK= ,	FUNCTION=HG3570,
	BGBKAN= ;	
AENDERN-BFDAT:	CONFIG=WEITER,	FCTBLK= ,
	FUNCTION= ,	ANZBKAN= ;
AENDERN-BFDAT:	CONFIG=OK,	FCTBLK= ,
	ANTW= ;	
EINRICHTEN-BCSU:	TYP=IPGW,	LTU= ,
	EBT= ,	SACHNR=Q23 -X ,
	FCTID= ,	FCTBLK= ,
	IPADR= . . . ,	BKAN3570= ;
AENDERN-BCSU:	ART=HWYBDL,	LTU= ,
	EBT= ,	SACHNR=Q23 -X ,
	HWYBDL=A;	

Beispielblatt: Einrichten von HG 3500 als HG3570 im OpenScape 4000 System



EINRICHTEN-BFDAT:	FCTBLK=1,	FUNCTION=HG3570,
	BGBKAN=BKAN60&BKNA120;	
AENDERN-BFDAT:	CONFIG=WEITER,	FCTBLK=1,
	FUNCTION=HG3570,	ANZBKAN=40;
AENDERN-BFDAT:	CONFIG=OK,	FCTBLK=1,
	ANTW=JA;	
EINRICHTEN-BCSU:	TYP=IPGW,	LTU=5,
	EBT=91,	SACHNR=Q2316-X,
	FCTID=1,	FCTBLK=1,
	IPADR=192.168.1.11,	BKAN3570=40;
AENDERN-BCSU:	ART=HWYBDL,	LTU=5,
	EBT=91,	SACHNR=Q2316-X,
	HWYBDL=A;	

10.6 Hinweise für Netzwerkadministratoren

10.6.1 Zentralprozessor

Mit der Installation eines IPDA Systems bekommt jeder Zentralprozessor eine zusätzliche LAN-Schnittstelle, um die Access Points zu steuern.

PHY	1 GBit - autosensing bzw. fest einstellbar
MAC-Adresse	fest auf Schnittstellenkarte programmiert, ->Aufkleber
IP-Adresse	Im OpenScape 4000 System konfiguriert, frei einstellbar
IEEE 802.1p/q VLAN-Tagging	Konfigurierbar, wenn aktiv werden immer die Prioritätsbits gesetzt. Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Die VLAN-ID ist frei einstellbar. Konfiguration im OpenScape 4000 System.
TOS / DiffServ	TOS / DiffServ Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Konfiguration im OpenScape 4000 System.
Protokolle / Ports	Siehe Kapitel 21, „IP-Ports“ im Dokument „Gateways HG 3500 und HG 3575“
Routing	zu jedem Access Point wird ein Host-Route benutzt, der im OpenScape 4000 System konfiguriert wird. Keine Default-Route.
Firewall	Der Zentralprozessor erlaubt nur Verbindungen zu ihm bekannten Adressen, d.h. den Access Points, bzw. denen zugeordnete Service PCs.
Verbindungszahl	maximal 166 TCP/IP Verbindungen (2 je Access Point)

In großen Systemen werden 2 redundante Zentralprozessoren eingesetzt, von denen immer nur einer aktiv ist. Jeder Prozessor hat seinen eigenen IP-Netzanschluss mit eigener IP und MAC-Adresse. Der Standby-Prozessor hat die PHY aktiv, empfängt und sendet aber keine Pakete. Der Prozessor empfängt und sendet jedoch keine Pakete.

10.6.2 HG 3500 Voice Gateway

Wichtig: IP-Pakete mit den verwendeten Ports (hard-coded und per AMO konfiguiert) müssen im IP-Netzwerk transparent

geroutet werden, d.h. es darf keine Manipulation (z.B. durch Firewall) vorgenommen werden. Ohne transparentes Routing kommt es zu funktionalen Problemen!

Diese Baugruppen werden im OpenScape 4000 Zentralsystem eingesetzt. Maximal 83 HG 3500 Baugruppen können in einem System eingerichtet werden.

PHY	10/100 Base T - autosensing bzw. fest einstellbar
MAC-Adresse	fest auf Baugruppe programmiert, ->Aufkleber
IP-Adresse	Im OpenScape 4000 System konfiguriert, frei einstellbar, muss im gleichen Netzsegment wie Zentralprozessor liegen. Die Adresse ist dem Steckplatz im System zugeordnet. Die Adresse wird dem Slot im System zugeordnet. Bei Austausch einer Baugruppe übernimmt die neue automatisch die IP-Adresse.
IEEE 802.1p/q VLAN-Tagging	Konfigurierbar, wenn aktiv werden immer die Prioritätsbits gesetzt. Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Die VLAN-ID ist frei einstellbar. Konfiguration im OpenScape 4000 System.
TOS / DiffServ	Die 6 höchstwertigen Bits der TOS-Bytes sind frei einstellbar. Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Konfiguration im OpenScape 4000 System.
Protokolle / Ports	Siehe Kapitel 21, „IP-Ports“ im Dokument „Gateways HG 3500 und HG 3575“.
Routing	Im OpenScape 4000 System konfigurierte Routing-Tabelle mit Default-Route und max. 8 zusätzlichen Routen. Routing ist für alle HG 3500 im System identisch.
Verbindungszahl	Abhängig von der verwendeten HW maximal 30/60/120 RTP und RTCP Verbindungen zu beliebigen Access Points. Verbindungsaufbau komplett aus OpenScape 4000 gesteuert. H.323 Fast Connect für Direct Media Connections außerhalb des IPDA-Gateway-Verbunds, kein Gatekeeper nötig. Bandbreite der Verbindungen siehe Lastkalkulation für eine HG 3500 auf Seite 708

10.6.3 Access Points mit HG 3575

Je Access Point kommt eine HG 3575 als Zentralbaugruppe zum Einsatz. Die Access Points sind nur über IP an das Zentralsystem angekoppelt. Maximal 83 Access Points können in einem System eingerichtet werden.

Bezüglich der Adressierung muss zwischen „Networked“ und „Direct Link“ Access Points unterschieden werden.

„Networked“ Access Points sind in einem anderen Netzsegment als die Zentrale und daher nur über Router erreichbar.

„Direct Link“ Access Points sind im selben Netzsegment angeschlossen, wie das Zentralsystem.

Die Konfiguration der Adressen und Porteinstellungen wird aus dem OpenScape 4000 System heraus gemacht. Der Access Point speichert sie lokal ab. Für die Erstinbetriebnahme müssen die Parameter lokal eingestellt werden.

PHY	10/100 Base T - autosensing bzw. fest einstellbar
MAC-Adresse	fest auf Baugruppe programmiert, ->Aufkleber
IP-Adressen	siehe unten
IEEE 802.1p/q VLAN-Tagging	Konfigurierbar, wenn aktiv werden immer die Prioritätsbits gesetzt. Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Die VLAN-ID ist frei einstellbar. Konfiguration im OpenScape 4000 System.
TOS / DiffServ	Die 6 höchstwertigen Bits der TOS-Bytes sind frei einstellbar. Siehe Tabelle 3 „TOS-Werte“ im Dokument „Gateways HG 3500 und HG 3575“. Konfiguration im OpenScape 4000 System.
Protokolle / Ports	Siehe Kapitel 21, „IP-Ports“ im Dokument „Gateways HG 3500 und HG 3575“.
Routing	Im OpenScape 4000 System konfigurierte Routing-Tabelle mit Default-Route und max. 8 zusätzlichen Routen. Routing ist individuell für denen Access Point einstellbar.

Verbindungszahl	Abhängig von der verwendeten HW maximal 30/60/120 RTP und RTCP Verbindungen zu beliebigen HG 3500 oder Access Points. Verbindungsaufbau komplett aus OpenScape 4000 gesteuert. H.323 Fast Connect für Direct Media Connections außerhalb des IPDA-Gateway-Verbunds, kein Gatekeeper nötig. Maximal 2 TCP/IP Verbindungen zum Zentralprozessor. Bei Nutzung des Leistungsmerkmals AP-Emergency zusätzlich eine TCP/IP Verbindung zur survivability Unit. Bandbreite der Verbindungen siehe Abschnitt 3.1, „Lastkalkulation für Access Points“

IP-Adressen für „Networked“ Access Points:

IP-Adresse des Access Points	Für Signalisierung, Payload, SNMP, FTP, Telnet. Siehe Bild 4 „Unterschied zwischen „networked“ und „direct link“ Access Point“ Adresse muss im Netz geroutet werden.
IP-Adresse für Signaling Survivability	Diese Adresse bleibt im LAN unsichtbar, da sie nur für die PPP-Verbindung zwischen Survivability-Router und Modem-Anschluss des Access Points genutzt wird. Diese Adresse wird indirekt durch die Konfiguration der Netzwerkadresse für das virtuelle Überlebensnetzwerk (PPP über ISDN) vergeben. Hier sollte nur eine „private“ Adresse wie 192.168.x.0 verwendet werden.

IP-Adressen für „Direct Link“ Access Points:

IP-Adresse des Access Points	Für Payload, SNMP, FTP, Telnet, jedoch nicht für Signalisierung. Siehe Bild 4 „Unterschied zwischen „networked“ und „direct link“ Access Point“ . Adresse muss im selben Netzsegment liegen wie Zentralprozessor. Adresse muss im Netz geroutet werden.

IP-Adresse für Signalisierung	Die Signalisierungsverbindung zwischen Zentralprozessor und Access Point muss über einen Router gehen. Siehe Bild 4 „Unterschied zwischen „networked“ und „direct link“ Access Point“ . Bei Ausfall der LAN-Verbindung wird die bestehende TCP-Verbindung zur Signaling Survivability Verbindung umgeroutet. Das kann nur durch Wechsel des Routers erfolgen, während die Zieladresse gleich bleibt. Daher wird bei „Direct Link“ Access Points ein interner Router eingesetzt, der zwischen der IP-Adresse des Access Points und der internen Adresse der Signalisierungsinstanz routet. Die IP-Adresse für Signalisierung muss in einem „privaten“, eigenen Netzsegment liegen. Sie ist im LAN (per Sniffer) als Zieladresse der Signalisierungspakete sichtbar. Da die Signalisierungspakete aber ausschließlich vom Zentralprozessor über Host-Route an die IP-Adresse des Access Point geroutet werden, braucht / darf kein Router im LAN diese Adresse routen. Hier sollte nur eine „private“ Adresse wie 192.168.x.0 verwendet werden.
IP-Adresse für Signaling Survivability	Diese Adresse bleibt im LAN unsichtbar, da sie nur für die PPP-Verbindung zwischen Survivability-Router und Modem-Anschluss des Access Points genutzt wird. Diese Adresse wird indirekt durch die Konfiguration der Netzwerkadresse für das virtuelle Überlebensnetzwerk (PPP über ISDN) vergeben. Hier sollte nur eine „private“ Adresse wie 192.168.x.0 verwendet werden.

10.6.4 Redundante LAN-Schnittstelle

Wichtig: Nur möglich wenn die HG 3500 ohne WAML-Funktion konfiguriert ist!

Voraussetzungen

Für eine erhöhte Ausfallsicherheit sollten die Baugruppen HG 3500 und HG 3575 jeweils über LAN-Kabel an zwei verschiedene Switches angeschlossen werden.

Funktionsweise des Leistungsmerkmals

- Beim Hochlauf der Baugruppe:

- Sind beide LAN-Kabel gesteckt, und die HG-Baugruppe läuft hoch, so wird immer LAN-Port 1 aktiviert.

  LAN-Port 2 ist in diesem Fall auf Standby. Es ist nur die Schicht 1 aktiv (höhere Protokollschichten sind inaktiv).

  Ist beim Hochlauf der Baugruppe nur ein LAN-Port angeschaltet (LAN1 oder LAN2), so wird dieser Port verwendet.
- Falls der aktive LAN-Port (bei Anschaltung beider LAN-Ports) durch einen Peer oder die Hardware getrennt/deaktiviert wird:
- – Die Baugruppen aktivieren den Standby-LAN-Port.
  – Der „neue“ Port sendet eine GRATUITOUS ARP-Meldung mit derselben MAC- und IP-Adresse wie der „alte“ Port (die zweite MAC-Adresse wird nur verwendet, wenn auch ein anderes Leistungsmerkmal auf die Schnittstelle konfiguriert wird (WAML/PPP-Router)).
  – Beim Wechseln der Ports durch die Baugruppe geht die Payload für einen Zeitraum von mindestens 2 Sek. verloren. Aktive Verbindungen werden gespeichert und werden NICHT getrennt.
  – Der Port-Wechsel wird über eine OpenScape-4000-F-Meldung in HISTA protokolliert.
  – Wenn der „alte“ Port wieder in Betrieb geht, erfolgt keine erneute Port-Umschaltung.

Einschränkung

Wenn die Baugruppe im AMO BFDAT mit FUNCTION=WAML konfiguriert wurde, funktioniert die Umschaltung auf LAN-Port2 im Falle eines Ausfalls von LAN-Port 1 nicht.

Das liegt daran, weil das Leistungsmerkmal WAML2/WAML Replacement für das Leistungsmerkmal Signaling-Survivability verwendet wird. Die verwendete STMI Baugruppe, kann dann nicht auch redundante LAN Schnittstellen verwenden.

Hinweise

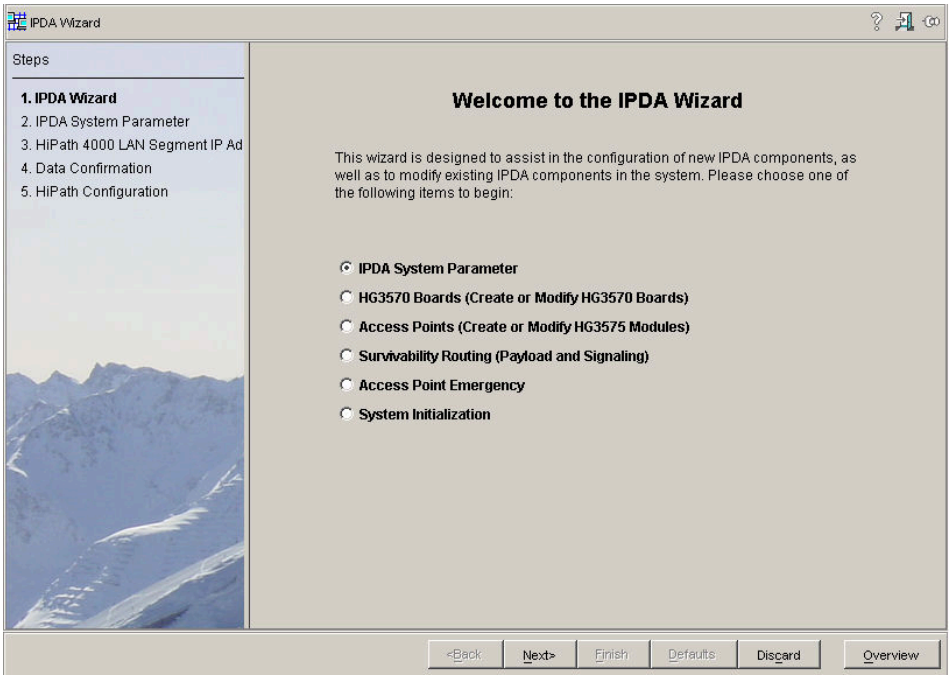
- Die Baugruppen haben jeweils nur eine IP- und MAC-Adresse.
- Es ist immer nur ein Port gleichzeitig aktiv.
- Läuft die Baugruppe mit zwei angeschalteten Ports hoch, wird LAN1 aktiviert.
- Es erfolgt keine Port-Umschaltung.
- Zur Aktivierung des Leistungsmerkmals ist keine Konfiguration in der OpenScape 4000 bzw. den HG-Baugruppen notwendig.
- Nach der Installation des Leistungsmerkmale „Redundante LAN-Schnittstellen“ wird empfohlen die Funktionalität zu testen. Dieser Test kann durch ziehen des aktiven LAN-Kabels für ca. 5 Sekunden erfolgen. Beobachten Sie, ob die Umschaltung erfolgreich ist. Der Grund für diesen Test ist das korrekte Verhalten der HG 3550/3575 im Zusammenspiel mit redundanten IT/LAN-Infrastrukturen (z.B.: L2 Switche/Router) zu verifizieren.
- Selbst wenn ein separates Management LAN konfiguriert ist, kann die LAN-Redundanz auf STMIX weiterhin verwendet werden, wenn VLANs verwendet werden.

10.7 IPDA-Assistent

Der IPDA Assistent unterstützt Sie bei der Konfiguration von IPDA und OpenScape 4000 SoftGates über eine Schritt-für-Schritt Benutzeroberfläche.

Sie finden den Assistenten unter:

	**Configuration Management > IPDA-Assistent**



IPDA-Assistent - Startseite

10.7.1 Funktionen

Sie können die folgenden IPDA Komponenten hinzufügen oder ändern:

- **IPDA Systemparameter**
- Die folgenden Funktionen stehen zur Verfügung:
  - Konfiguration der System-IP-Adressen

    IP-Adressen des OpenScape 4000 LAN-Segments, der Zentralprozessoren sowie der Standard-Router des OpenScape 4000 LAN-Segments
  - Konfiguration der Netzwerkparameter

    Hier werden die Parameter für die Übertragungsbitrate und für VLAN-Tagging sowie die Quality-of-Service-Parameter konfiguriert.
  - Konfiguration der Grenzwerte für Payload Quality

    Hier können Sie Grenzwerte (z. B. Timer) zur Überwachung der Übertragungsqualität einer Verbindung konfigurieren.
- **HG 3570 Baugruppen (Einrichten oder Modifizieren von HG 3570 Baugruppen)**

- **Access Points (Einrichten oder Modifizieren von HG 3575 Modulen)**
- Mit dieser Funktion können Sie neue Access Points/OpenScape 4000 SoftGates einrichten oder bestehende Access Points/OpenScape 4000 SoftGates modifizieren. Es ist auch möglich einen vorhandenen Access Point/OpenScape 4000 SoftGate als Vorlage für einen neuen Access Point/ OpenScape 4000 SoftGate zu verwenden.

  Ergebnis Access Point:

  – AMO-Stapel
  – CLI-Stapel (zum konfigurieren der NCUI-Baugruppe im AP)

  Ergebnis OpenScape 4000 SoftGate:

  – AMO-Stapel
  – xml-Datei (zum konfigurieren des OpenScape 4000 SoftGates)
- **Survivability Routing (Payload und Signaling)**
- Hier können Sie als Vorkehrung für einen Ausfall des IP-Netzwerks alternative Richtungen für die Signalisierungs- und Payload-Verbindungen konfigurieren.
- **Access Point Emergency**
- Bei der Funktion Access Point Emergency werden auf den Access Points zusätzliche Steuerungsprozessoren (CC-AP) eingesetzt. Diese können die Steuerung einer Gruppe von Access Points übernehmen, wenn die Access Points infolge eines Netzwerkausfalls oder eines Ausfalls des Host-Systems die Verbindung zu den Host-Steuerungsprozessoren (CC-A, CC-B) verloren haben.

  Die folgenden Funktionen stehen zur Verfügung:

  – Einrichten einer lokalen CC für einen Access Point
  – Hier können Sie einen Steuerungsprozessor auf einem Access Point zum Einsatz in Notfällen konfigurieren.
  – Einrichten einer Emergency-Gruppe

  Hier können Sie Daten zur Emergency-Gruppe konfigurieren, z. B. Kritierien zum Umschalten in den Notfallmodus und zurück sowie den zu verwendenden Steuerungsprozessor.

  – Zuweisen eines Acccess Points zu einer Emergency-Gruppe

  Hier können Sie den zuvor definierten Emergency-Gruppen einen einzelnen Access Point zuweisen oder den Einfluss dieses Access Points zum Umschalten der Gruppe in den Notfallmodus ändern.

  – Einrichten von Alternate Routing für Notfälle

  Hier können Sie pro Source Group eine alternative Amtsrichtung zur Belegung im Notfall konfigurieren.
- **Systeminitialisation**

- Unter Systeminitialisation stehen die folgenden Funktionen zur Verfügung:
  – Zurücksetzen von Baugruppen

  Reloads von HG3570 Baugruppen bzw. Access Points durchführen.

  – Übertragen von Loadware und SIU-Dateien auf Access Points

  Neue Loadware auf Access Points laden.

  – Ausführen von Systemrestarts

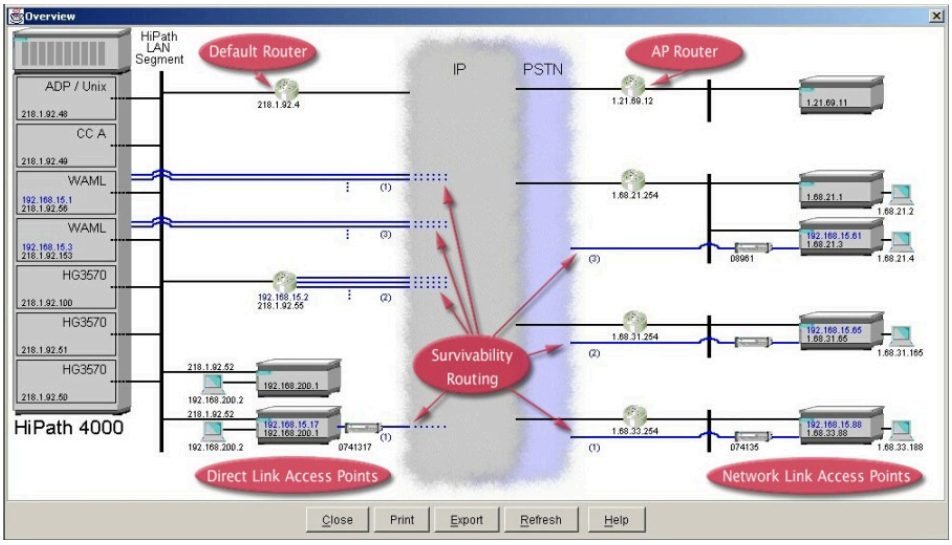
  Ausführen von Soft- oder Systemrestarts im OpenScape 4000 System

  – Umschalten des Systemmodus

  Systemeinheiten in den Emergencymodus bzw. zurück in den Normalbetrieb schalten.

Schaltfläche „Übersicht“

Der Assistent bietet außerdem einen grafischen Überblick über die aktuelle IPDA-Konfiguration.



IPDA-Assistent - Grafische Übersicht über die aktuelle IPDA-Konfiguration

10.8 FAQ - Häufig gestellte Fragen

1) **Frage:** Brauche ich tatsächlich für jeden Access Point AP 3300 IP oder AP 3500 IP eine HG 3500-Baugruppe in der Zentralanlage?
2) **Antwort:** NEIN, definitiv nicht. Es wird immer wieder angenommen, dass eine feste Beziehung zwischen einer HG 3575 und einer HG 3500 bestehen muss, um die Signalisierungsdaten zu übertragen. Die Signalisierungsdaten kommen aber (über das SL 200 oder SL 100 Modul) direkt aus dem Zentralprozessor. Die HG 3500 ist ausschließlich für den Payload-Transport zuständig. Die Zahl der benötigten HG 3500 im System hängt allein vom Verkehrsaufkommen zwischen den Access Points (Summe über alle APs) und dem Zentralsystem ab.
3) **Frage:** Wie stelle ich sicher, dass beim Ausfall einer HG 3500 nicht immer eine bestimmte Zahl von Access Points abgehängt wird?
4) **Antwort:** Es gibt keine Zuordnung von HG 3500 zu bestimmten Access Points. Sind mehrere HG 3500 im System, so teilen diese sich das

Gesamtverkehrsaufkommen. Die Belegung der HG 3500 im System erfolgt zyklisch, d.h. die erste Verbindung geht über die erste HG 3500, die nächste über die zweite und so weiter. Fällt eine HG 3500 aus, werden natürlich alle gerade aktiven Gespräche über diese Baugruppe unterbrochen. Die Baugruppe wird dann bei neuen Gesprächen nicht mehr belegt. Die anderen HG 3500 übernehmen diese neuen Gespräche, soweit Kapazität frei ist.

5) **Frage:** Warum dürfen IPDA-Komponenten nicht über Hubs angeschlossen werden?
6) **Antwort:** Hubs arbeiten im klassischen „Shared Medium“ Betrieb des Ethernet. Alle angeschlossenen Einheiten teilen sich die Gesamtbandbreite. Jeder kann alles mithören. Nur einer kann zu einem Zeitpunkt senden. Sprachkommunikation ist bidirektional, der Datenstrom von A nach B ist (außer bei Nutzung von VAD) gleich groß wie der Datenstrom von B nach A. Da bei Shared Medium nur immer einer senden kann, belegen Sende- und Empfangsrichtung jeweils einen gleichen Teil der verfügbaren Gesamtbandbreite. Der Einsatz von Layer 2 Switches, die inzwischen oft billiger sind als Hubs, entkoppelt die Anschlussmedien der einzelnen Einheiten. Alle können gleichzeitig senden und empfangen. Die Bandbreite (nun je Einheit verfügbar) kann effizienter genutzt werden.
7) **Frage:** Warum sind die LAN-Ports der IPDA Komponenten per Default auf *Autonegotiate* eingestellt. Man liest immer wieder, dass das zu Problemen führt.
8) **Antwort:** Die Default-Einstellung soll einen relativ problemlosen Ersthochlauf gewährleisten. Wegen der immer wieder auftretenden Probleme mit Autonegotiation raten wir dringend dazu, eine **feste** Einstellung **beider** Schnittstellenpartner einzurichten. Es ist zwingend erforderlich, beide Schnittstellen gleich einzurichten - und natürlich auf die selben Werte. Der Betrieb einer autonegotiate Schnittstelle mit einer fest eingestellten führt häufig nicht dazu, dass sich die autonegotiate Schnittstelle auf die Einstellung der festeingestellten „verhandelt“. Beachten Sie dazu auch den Hinweis auf Seite 672.
9) **Frage:** Im AMO SIPCO muss ich die Netzwerkadresse für das OpenScape 4000 LAN Segment eingeben. Braucht jede OpenScape 4000 ihr eigenes LAN Segment, oder kann ich mehrere OpenScape 4000 Systeme im gleichen LAN Segment betreiben?
10) **Antwort:** Es können auch mehrere OpenScape 4000 Systeme im selben Netzwerk betrieben werden. Dabei dürfen die IP-Adressen der Komponenten aber nicht mehrfach genutzt werden und die Leistungsfähigkeit der Router bzw. WAN-Anbindung muss den gesamten Bandbreitebedarf abdecken.
11) **Frage:** Die für IPDA dokumentierten Default-Werte für das TOS-Byte, d.h. die vorgegebenen DiffServ CodePoints (DSCP) bewirken zusammen mit der Standardeinstellung populärer Router-Hersteller genau das Gegenteil dessen, was beabsichtigt ist. Die von uns als hochprior gekennzeichneten Pakete werden vom Router bevorzugt weggeworfen. Was soll der Unsinn?
12) **Antwort:** Die für IPDA verwendeten Default-Werte stammen aus einem Firmen-internen Standard der in allen HG 35xx Gateways umgesetzt wurde. Das Interoperabilitätsproblem ist mittlerweile bekannt - und der Hausstandard soll demnächst geändert werden. Die Default-Werte können aber jederzeit verändert und an die tatsächlichen Gegebenheiten im Kundennetz angepasst werden.
13) **Frage:** Unterstützt IPDA VLANs?

14) **Antwort:** Ja, aber nur zusammen mit Priority Tagging. Tagging nach IEEE 802.1 p/q wurde für IPDA eingeführt um Priority-Tagging zu unterstützen. Wird Tagging eingeschaltet, so werden immer die fest vorgegebenen Priority-Bits der unterschiedlichen Verkehrsarten gesetzt. (siehe letzte Spalte der Tabelle 3 „TOS-Werte“ in Dokument „Gateways HG 3500 und HG 3575“). Ist Tagging aktiv, kann zusätzlich die VLAN-ID eingestellt werden (Default-Wert ist Null). Was nicht unterstützt wird ist VLAN-ID ohne gesetzte Priority-Bits.
15) **Frage:** Unterstützt IPDA Subnetting (RFC 950)?
16) **Antwort:** Ja. Bei der Eingabe der Netzmaske wird überprüft, ob der Block der gesetzten Einsen mindestens so lange ist, wie es für die Klasse der Adresse erforderlich ist, d.h. 8 Einsen für Klasse A, 16 für B sowie 24 für C. Ist die Zahl der Einsen größer als für die Klasse erforderlich, ist Subnetting aktiviert.
17) **Frage:** Unterstützt IPDA Supernetting (RFC 1338) ?
18) **Antwort:** Nein.
19) **Frage:** Kann man einen Access Point so betreiben, dass nur die Signalisierung über IP geht? Die Sprache könnte ja als Wählverbindung über ISDN geführt werden wie bei Payload Survivability.
20) **Antwort:** Payload Survivability ist als Notbetrieb bei ausgefallenem/gestörtem IP-Netz konzipiert. Es kann nur die Basic Call Funktionalität garantiert werden. Außerdem wäre zu berücksichtigen, dass die Signalisierung über IP Quality of Service bieten muss, was bei Nutzung extrem schmalbandiger WAN-Strecken zusammen mit Datenkommunikation in bestehenden Installationen häufig nicht unterstützt wird.

    Nachfrage: Es kann doch wohl nicht so schwer sein, dass eine ISDN TK-Anlage Sprachverbindungen über ein Carrier-Netz schaltet.

    Antwort: Dafür sind die Anlagen ausgelegt. Im oben geforderten Fall muss sich die Anlage aber über Amt selber anrufen und dies darüber hinaus als internen Ruf mit vollem Leistungsmerkmalspektrum abhandeln - und das ist schon nicht mehr trivial.
21) **Frage:** Warum braucht der „direct link“ Access Point zusätzliche IP-Adressen? Anschluss im selben LAN-Segment müsste doch einfacher sein als LAN-Segment übergreifend mit Routern.
22) **Antwort:** Der Grund für den internen Router und die zusätzliche Adresse liegt in der Signaling Survivability. Für Signaling Survivability ist es erforderlich, Pakete der TCP-Schicht, welche nicht mehr über LAN zugestellt werden können, auf einer anderen Route - eben dem „Survivability-Weg“ auszuliefern, bevor die Überwachungstimer im TCP ablaufen. Dazu muss die IP-Zieladresse gleich bleiben, nur der angesprochene Router kann umgeschaltet werden. Beim „networked“ Access Point wird vom (default) LAN-Router auf den Survivability Router umgeschaltet. Beim „direct link“ Access Point gibt es diesen LAN-Router nicht, da CC und AP im selben LAN-Segment liegen. Umschalten von *kein* Router auf Survivability-Router geht nicht. Somit könnte für „direct link“ keine Signaling Survivability angeboten werden. Die einzige praktikable Lösung ist es, den LAN-Router in den Access Point zu integrieren. Daher gibt es 2 IP-Adressen beim „direct link“ Access Point. Die des Router-Ports am OpenScape 4000 LAN Segment und die der Signalisierungsinstanz im „internen Netz“ des AP.
23) **Frage:** Ist es möglich, IPDA Komponenten in einem Netz zu betreiben, das kein Quality of Service unterstützt?

24) **Antwort:** Ist das gesamte Netz ideal dimensioniert, treten auch bei Langzeitmessungen keine Paketverluste und keine signifikaten Paketlaufzeiten auf und ist die Netzwerkauslastung (inklusive der IPDA-Last) auf allen Pfaden moderat, dann wird ein IPDA-System in diesem Netz auch ohne QoS Maßnahmen funktionieren. Werden, z.B. durch Lastverschiebungen o.ä., diese Bedingungen verletzt, ist mit Funktionsstörungen zu rechnen. Ein ständiges, hoch entwickeltes Network-Monitoring ist in diesem Fall unbedingt erforderlich, um Engpässe im Netz bereits im Entstehen zu erkennen und sofort zu beseitigen. Sind in dem für IPDA genutzten Netz schmalbandige WAN-Verbindungen im Einsatz, die auch für Datenverbindungen genutzt werden und eine hohe Auslastung haben, sind ohne QoS Funktionalität zur Priorisierung des IPDA-Verkehrs im Netz Störungen garantiert.

25) **Frage:** Ein Access Point ist über WAN abgesetzt. Es stehen nur 800 kBit/s an Übertragungskapazität zur Verfügung. In der Hauptverkehrszeit treten massive Störungen auf, teilweise fährt der Access Point Restarts. Der Verkehr vom/zum Access Point ist gegenüber dem parallel aktiven Datenverkehr höher priorisiert. Kann die von OpenScape 4000 belegte Bandbreite auf dem WAN-Link auf 800 kBit/s begrenzt werden?

26) **Antwort:** Die vom Access Point benötigte Bitrate lässt sich über den Resource Manager begrenzen. Tabelle 41 „Hochpriore Last AP in Abhängigkeit von der erlaubten B-Kanalzahl“ gibt einen Überblick über die benötigte Kapazität in Abhängigkeit der Anzahl der gleichzeitig aktiven Verbindungen. Basis sind Gespräche mit G.711 Codec. Die Signalisierungslast wurde zu 64 kBit/s angesetzt. Bei 30 ms Sample Size (default) könnten also 9 Verbindungen gleichzeitig genutzt werden, um unter 800 kBit/s (792) zu bleiben.

    Nachfrage: Wenn ich G.729 Codec einsetze, zeigt mir Tabelle 40 „Hochpriore Last AP in Abhängigkeit von Codec und Sample-Größe“, dass ich wesentlich mehr B-Kanäle mit der vorhandenen Bandbreite transportieren kann.

    Antwort: Theoretisch würden die verfügbaren 800 kBit/s sogar über 30 B-Kanäle transportieren können, wenn G.729 mit 40 ms Sample Size eingestellt wird. Es muss aber beachtet werden, dass dafür alle an Gesprächen beteiligten Sätze der gesamten Anlage für die Unterstützung von G.729 eingerichtet sein müssen (Classmark G729OPT). Das ist die Default Einstellung. Darüber hinaus müssen alle Sätze im Access Point mit Classmark G729 eingerichtet werden, was die Nutzung des G.729 Codecs erzwingt. Das gilt dann auch für Konferenzanschaltung und Music-On-Hold. Dabei empfehlen wir, die Konferenzeinheit nicht für G.729 zu konfigurieren, um bestmögliche Sprachverständlichkeit in der Konferenz zu gewährleisten. Auch bei Music-On-Hold muss beachtet werden, dass Warte**musik** durch die Sprachkompression erheblich verzerrt wird. Darüber hinaus muss beachtet werden, dass Faxgeräte, Modems, ISDN-Datenendgeräte nicht mit Kompression G.729 betrieben werden dürfen. Werden diese Geräte aktiv, werden (in diesem Beispiel mit G.711 - 30 ms und G.729 - 40 ms) immer 81 kBit/s statt der erwarteten 21 kBit/s belegt. Das heißt, auch bei maximal möglichem Einsatz von G.729 darf die B-Kanalzahl in diesem Beispiel nicht auf 30 eingestellt werden. Der richtige Wert liegt zwischen 9 und 30. Er hängt davon ab, wie viele G.711 Verbindungen noch benötigt werden. Wird die B-Kanalzahl zu hoch eingestellt, so werden bei Überschreitung der Kapazität des WAN-Links **ALLE** Verbindungen gestört. Auch die Signalisierungsverbindung kann

betroffen sein, was bei entsprechend massiver Störung zur Umschaltung auf Signaling Survivability oder zum Restart des Access Point führen kann.

27) **Frage:** Ich möchte einen Access Point über ISDN absetzen. Da die NCUI nur einen LAN-Anschluss zur Verfügung stellt, möchte ich einen Router mit einer S0-Schnittstelle einsetzen. Der bietet mir 128 kBit/s Bandbreite, was mir doch für 7 B-Kanäle ausreicht. Das Signalisierungsaufkommen schätze ich als sehr gering ein. Sind da Probleme zu erwarten?

28) **Antwort:** Ja, von dieser Konfiguration sollten Sie dringend Abstand nehmen. 7 B-Kanäle belegen zwar bei G.729-Kompression und 60 ms Sample-Größe nur gute 114 kBit/s. Aber nicht ohne Grund sollen immer etwa 64 kBit/s für Signalisierung freigehalten werden. Damit stehen nur noch 64 kBit/s für Payload zur Verfügung. Und die reichen nicht aus, wenn auch nur ein Gespräch nicht komprimiert werden kann (Fax, Modem, ISDN-Daten) (siehe auch Frage 13).

29) **Frage:** Ich möchte zwischen Access Point und OpenScape 4000 LAN Segment einen PCM30-Router einsetzen, habe also maximal 2 MBit/s an Bandbreite zur Verfügung. Da der Kunde aber keine Standleitung nutzen möchte, sondern Wählverbindungen durch das öffentliche Telefonnetz, soll die tatsächlich gewählte Bandbreite möglichst klein sein, und nur bei Bedarf angepasst/erhöht werden. Als Minimum würden wir 1 Kanal für die geforderten 64 kBit/s Signalisierung bereitstellen. Sind da Probleme zu erwarten?

30) **Antwort:** Ja, mit „dynamischer“ WAN-Bandbreite wird es sicher Probleme geben, die nur durch fest verfügbare Bandbreite lösbar sind. Die Begründung dafür ist einfach. Nehmen Sie an, die aktuell verfügbare Bandbreite reicht genau aus. Jetzt kommt noch ein Call dazu. Damit reicht die Bandbreite nicht mehr aus. Was macht der Router? Zuerst wird er die Pakete, die er mangels Bandbreite nicht mehr los wird, stauen, was alle Verbindungen gleichermaßen betrifft. Baut sich der Stau innerhalb einer bestimmten Zeit nicht ab, wird er eine weitere 64 kBit/s Verbindung im Telefonnetz aufbauen. Nach Abschluss des Verbindungsaufbaus steht dann genügend Bandbreite zur Verfügung. (Wenn nicht, werden weitere 64 kBit/s aufgebaut.) Die dafür benötigte Zeit liegt im Bereich einiger Sekunden. Während dieser Zeit werden alle Payloadverbindungen gestört und auch - falls nicht durch Priorisierung geschützt - die Signalisierungsverbindung.

31) **Frage:** Wie kann ich die tatsächlich verfügbare Quality of Service an einem Access Point abfragen? Der Netzbetreiber sagt, es sei alles bestens. Die Telefonteilnehmer klagen sporadisch über schlechte Sprachverständlichkeit.

32) **Antwort:** An allen HG 3575 und HG 3500 Baugruppen lassen sich die von Real Time Transmission Protocol erfassten QoS Werte über SNMP abfragen. Siehe Kapitel 20, „SNMP Support HG 3500 / HG 3575“ im Dokument „Gateways HG 3500 und HG 3575“. Zusätzlich gibt es im OpenScape 4000 Assistant die Möglichkeit, gesprächsbezogen die QoS Parameter aufzuzeichnen, auszuwerten und anzuzeigen. Siehe OpenScape 4000 Assistant -> Diagnose -> IPDA Service Access -> Call Quality Recording Viewer, MIB Viewer, bzw. QoS Viewer.

Nachfrage: Laut Netzbetreiber ging in der Zeit der Sprachstörungen kein einziges IP-Paket verloren. Gibtâs da noch eine andere Ursache für schlechte Sprachqualität?

Antwort: Wenn der Netzbetreiber Pakete mit einer Verzögerung größer als die Jitter-Buffer-Größe zustellt, stehen sie für den Codec nicht zur Verfügung, wenn er sie braucht. Damit sind die Pakete aus Sicht des

Netzbetreiber korrekt zugestellt, im Echtzeitkontext der Sprachübertragung jedoch verloren.

33) **Frage:** Fax und Daten über Voice Over IP Verbindungen gelten als sehr kritisch. Wie gut funktioniert das wirklich?

34) **Antwort:** Es gibt drei Einflussgrößen, die hier relevant sind. Die Paketverlustrate, der Jitter und die Verzögerung. Moderne Sprach-Codecs bringen durch Verfahren wie „Packet Loss Concealment“ *(Verschleierung des Paketverlusts)* auch bei einer Paketverlustrate von 5% noch akzeptable Sprachqualität. Für Fax, Modem oder ISDN-Datenverbindungen lässt sich der Paketverlust jedoch nicht verschleiern. Hier sinkt wegen der nötigen Übertragungswiederholungen der Durchsatz. Ist die Paketverlustrate zu hoch, wird die Verbindung von den Endgeräten ausgelöst. Jitter ist die Ursache für indirekten Paketverlust. Hier ist die Dimensionierung des Jitter-Buffers ausschlaggebend. Dieser soll so klein wie möglich dimensioniert werden, um die Verzögerung klein zu halten. Pakete, deren Abweichung von der „normalen“ Verzögerung nicht mehr im Jitter-Buffer ausgeglichen werden können, sind aber verloren. Für Sprache darf also die Summe aus im Netz verlorenen und wegen zu hohen Jitters verlorenen Paketen wesentlich höher sein, als bei Fax, Modem und Daten. Um den unterschiedlichen Anforderungen der Verkehrsarten an den durch Jitter verursachten Paketverlust gerecht zu werden (Sprache < 5%, Fax, Modem Daten ~0%), wird bei den OpenScape 4000 Komponenten HG 3500 und HG 3575 der eingestellte Wert für den Jitter-Buffer für Fax-, Modem- oder Daten-Verbindungen um 30 ms erhöht. Auch die Verzögerung auf der Verbindung kann - in Abhängigkeit von den verwendeten Datenübertragungsprotokollen - kritisch werden. Erfolgt die Übertragung quittungsgesteuert, so kommt durch die Übertragungsverzögerung die Quittung verzögert an, was gegenüber der unverzögerten Verbindung den Durchsatz reduziert.
Die Signalprozessoren werten beim Verbindungsaufbau die Signalisierungstöne der verbundenen Fax- bzw. Modem-Geräte aus. Dabei wird zwischen Hoch- und Niedergeschwindigkeitsgeräten unterschieden und die Übertragung entsprechend optimiert.

35) **Frage:** Welche Bitraten garantiert IPDA für Faxgeräte bzw. Modems?

36) **Antwort:** IPDA kann keine höhere Bitrate garantieren, als vom OpenScape 4000 Zentralsystem sichergestellt wird. Das sind 14,4 kBit/s. Bei höheren Bitraten gibt es z.B. Abhängigkeiten vom Dämpfungsplan, der eingestellten Dämpfung am T-Referenzpunkt etc. Höhere Bitraten als 14,4 kBit/s sind in bestimmten Konstellationen technisch möglich, können aber nicht garantiert werden.

37) **Frage:** Der Kunde verwendet Kombigeräte (Drucker/Scanner/Modem) als Faxgeräte. Faxverbindungen zu konventionellen Faxgeräten funktionieren problemlos. Faxe von identischen Geräten innerhalb des IPDA-Systems machen aber Probleme.

38) **Antwort:** Probleme machen Kombigeräte, welche am Fax-Standard vorbei die Übertragungsgeschwindigkeit verbessern wollen. Diese Geräte gehen als „normale“ G3-Faxgeräte in die Verhandlungsphase am Beginn der Faxverbindung. Stellen sie dabei fest, dass sie beide ein proprietäres - schnelleres - Übertragungsverfahren unterstützen, so nutzen sie dieses. Das Problem der IPDA Gateways ist das selbe, das auch auf Fernstrecken auftritt. Aufgrund der Signalisierungstöne, die eine niederbitratige Verbindung kennzeichnen, wird die Übertragungsstrecke optimiert. Die Geräte entscheiden sich aber während der Verhandlung, eine hochbitratige Übertragung zu verwenden. Und das führt wegen der für niederbitratige Übertragung optimierten Strecke zu Problemen.

39) **Frage:** Im Servicehandbuch wird immer wieder darauf hingewiesen, dass die IP-Adressen der IPDA-Komponenten angepingt werden sollen. Jetzt mach ich das, und es funktioniert nicht oder nur manchmal.

40) **Antwort:** Es gibt 3 Dinge, die einen erfolgreichen ping beeinflussen

- Der ping-Request muss zum Ziel kommen, um dort beantwortet zu werden. Dazu muss das Routing von dem Port des Rechners, der den ping absetzt zum Ziel sichergestellt sein. Es ist deshalb wichtig, dass ping-Requests von bekannten IPDA-Komponenten (AMO SIPCO, Parameter **LSNET** und AMO APRT, Parameter **APNET**) und nicht von irgendwelchen anderen unbekannten Netzwerkadressen-Segmenten/ Geräten kommen (z.B. Service-PC in einem anderen Netzwerk).
- Der ping-Request darf am Ziel nicht von Firewall verworfen werden. Die Steuerungsprozessoren CC-A/CC-B schützen sich gegen Fluten von ping-Requests, indem sie nur eine bestimmte Menge von Requests pro Zeiteinheit zulassen. Das Filter ist so abgestimmt, dass ein Standard-ping-Kommando mit ca. 5 Anfragen im ca. Sekundenabstand problemlos beantwortet wird. Wird aber wesentlich häufiger oder in kürzeren Abständen gefragt, so werden die Anfragen verworfen. CCA- und CC-B antworten.
- Der ping-Response muss zurück zum Requestor kommen, um dort bewertet zu werden. Dazu muss das Routing von der angepingten IPDA-Komponente zu dem Rechner, der den ping abgesetzt hat, sichergestellt sein. Die Steuerungsprozessoren CC-A/CC-B verwenden spezielle Host-Routen zu den eingerichteten Geräten (das ist auch der Grund warum es keine Default-Routen in unbekannte Netze gibt, in denen andere Geräte angeschlossen sind). AMO SIPCO, Parameter **DEFRT** wird deshalb nur für diese speziellen Routen verwendet und ist kein klassischer Default-Router.

41) **Frage:** Ich habe jetzt schon mehrfach - bei unterschiedlichen Fehlerbildern - die NCUI-Baugruppen „über Kreuz“ getauscht. Der Fehler ist immer mitgewandert. Das darf doch nicht sein, oder?

42) **Antwort:** Gerade bei der NCUI ist ein Überkreuztausch der Baugruppen sehr problematisch, da beim Tausch die lokalen Konfigurationsdaten geändert werden müssen. Wenn Sie nur eben mal die Baugruppen vertauschen - und nicht umkonfigurieren, dann nehmen Sie auch die LTU-Nummer und die gesamte Konfiguration des Rahmens mit. Die Zentrale spricht LTU 17 mit der konfigurierten IP-Adresse an. Sitzt die NCUI mit dieser Adresse jetzt mechanisch in einem anderen Rahmen, ist dieser jetzt LTU 17. Sie müssen also beim Baugruppentausch unbedingt die Anweisungen im Servicehandbuch unter Abschnitt 2.2.9, „Hinweise zum Austauschen von HG 3575 Baugruppen“ beachten. Auch der Überkreuztausch ist ein Austausch der Baugruppen. Die Übernahme der lokalen Konfiguration (mit „Expertenzugang“) gehört genauso dazu wie der `EXEC-USSU:UPDATAP,`LTU-Nummer`,UL;`

43) **Frage:** Aus Sicht des Kunden ist ein IPDA Access Point ein Gerät, das sowohl einen IP-, als auch TDM-Anschlüsse besitzt. Der Einsatz derartiger Geräte ist im Kundennetz aus Sicherheitsgründen verboten.

44) **Antwort:** Ein Verbot, PCs am LAN zu betreiben, die gleichzeitig auch einen Netzzugang in einem anderen (nicht durch Firewalls etc. schütz- bzw. kontrollierbaren) Netz haben, ist weit verbreitet - und sinnvoll.

Derartige Geräte könnten als „private“ Gateways verwendet werden, um z.B. eine unsichere Einwahlverbindung ins LAN anzubieten.

Ein IPDA Access Point als Gateway für Sprachverbindungen von (TDM <-> IP) muss natürlich sowohl Zugriff auf das LAN, als auch auf TDM-Anschlüsse haben.

Das Design der HG 3575 stellt eine harte Trennung zwischen der Durchschalte- (Payload) und der Steuerungsfunktionalität (Signaling) sicher.

Im Payload-Teil werden auf Anforderung der OpenScape 4000 Zentrale beliebige Verbindungen TDM <-> TDM bzw. TDM <-> IP <-> TDM hergestellt. Der Verbund aus OpenScape 4000 Zentrale und den IPDA Access Points stellt nach aussen einen in sich geschlossenen TDM-Betrieb sicher, der sich intern zur Vernetzung der Access Points eines IP Netzes bedient.

Ein Missbrauch der HG 3575 würde es erforderlich machen, dass zusätzliche IP-Verbindungen von der NCUI z.B. per PPP auf TDM-Verbindungen geroutet werden.

Dies ist nicht möglich, weil

a) der IP-Stack nur auf wenige Ports reagiert (siehe Kapitel 21, „IP-Ports“ im Dokument „Gateways HG 3500 und HG 3575“)

b) • kein Zugriff des Signalisierungsteils auf TDM Payload möglich ist

Das HG 3575 unterstützt PPP, aber nur für die Signalisierungsverbindung über ein **externes**, über eine serielle V.24-Schnittstelle angeschlossenes Modem im Fall der Signaling Survivability.

45) **Frage:** Wir haben das Mouth-to-Ear-Delay einer Sprachverbindung zwischen OpenScape 4000 Zentrale und einem IPDA Access Point nachgemessen. Dabei fällt auf, dass das Delay einen sehr langsamen Sägezahnverlauf hat. D.h. es sinkt kontinuierlich bis auf einen unteren Grenzwert und springt dann wieder auf einen Maximalwert, von dem aus es wieder kontinuierlich sinkt. Wie kommt es zu diesem Verhalten, was kann man dagegen tun?

46) **Anwort:** Sie haben keine digitalen Amtsschnittstellen im Access Point, bzw. Sie verwenden diese nicht zur Taktung der HG 3575. Ohne Synchronisation über digitale Amtsschnittstellen im Access Point laufen die Taktgeneratoren von OpenScape 4000 Zentrale und Access Point asynchron. Die Genauigkeit des freilaufenden Taktgenerators auf der HG 3575 ist extrem hoch (ISO 11 573 class III, TIA stratum 4, CTR4 und CTR12/13). Dennoch laufen nicht synchronisierte Taktgeneratoren über die Zeit auseinander. In dem von Ihnen gemessenen Fall arbeitet der Empfänger mit einer etwas höheren Taktfrequenz als der Sender. Die IP-Verbindung startet mit dem voreingestellten Jitter-Buffer-Wert. Da mehr Daten gelesen als gesendet werden, läuft der Jitter-Buffer langsam leer. Das erklärt das stetig fallende Mouth-to-Ear-Delay. Ist der minimale Füllstand des Jitter-Buffers erreicht, wird empfangsseitig „Zeit eingefügt“, in welcher der Jitter-Buffer wieder gefüllt wird. Das erklärt den Sprung auf den Maximalwert. In der Gegenrichtung beobachten Sie den umgekehrten Effekt. Das Mouth-to-Ear-Delay steigt stetig, bis eine Obergrenze des Jitter-Buffers überschritten wird. Dann wird „Zeit entfernt“ und auf dem Sollwert des Jitter-Buffers neu aufgesetzt.

Diesen Effekt können Sie bei allen Geräten beobachten, welche über längere Zeit Daten mit konstanter Rate übertragen und keine

Synchronisation des Übertragungstaktes haben. Bei den IPDA Access Points gibt es als Abhilfe die Synchronisation der Zentrale und aller HG 3575 auf einen gemeinsamen Amtstakt.

47) **Frage:** Es macht ja keinen Sinn, dass im Falle der Payload-Survivability Gespräche vom IPDA zum zentralen Voice-Mail-Server übers Amt geroutet werden. Kann man dies verhindern?

48) **Antwort:** VoiceMail-Systeme sind von der Behandlung durch Payload Survivability ausgenommen. Das ist auch in der Vertriebsfreigabe der OpenScape 4000 (1. Nachtrag) explizit als Ausnahme dokumentiert. Gespräche werden also in diesem Fall nicht über den Survivability-Pfad (d.h.) AMT weitergeleitet.

49) **Frage:** Wird NAT bei IPDA unterstützt?

50) **Antwort:** NEIN.

51) **Frage:** Welche Ressourcem stehen pro Access Point (NCUI2+/NCUI4/ OpenScape 4000 SoftGate) zur Verfügung?

52) **Antwort:**

- 64 TSLs für Konferenz
- 4 Empfänger für DTMF-Signalisierung (CR) - 32 Empfänger für OpenScape 4000 SoftGate
- 4 Sender für DTMF-Signalisierung (CS) - 32 Sender für OpenScape 4000 SoftGate
- 2 Dauerton Wähltonempfänger (DTR-DT)
- 2 Wähltonempfänger für rhytmische Töne (DTR-TT)
- 2 Test-Empfänger (TESTR)
- 1 Test-Sender (TESTS)
- bis zu 18 verschiedene Töne
- 6 verschiedene Ansagen
- 1 Wartemusik
- 1 TDS Port

53) **Frage:** Ich möchte die IP-Adressen des Host-Systems beim nächsten Upgrade von einer Major Version auf eine andere Major Version (z.B. HiPath 4000 V6 -> OpenScape 4000 V7) ändern. Gibt es einen einfachen Weg um das zu erreichen?

54) **Antwort:** Ab den Loadware-Linien der HiPath 4000 V6 R2 akzeptieren die Access Points HSR-Verbindungen von jeder IP-Adresse, so lange es keinen schon aktiven Access Point gibt (d.h. IPDA muss den Status NOT READY für diese Arbeiten haben). Das bedeutet, dass Sie die CCA-/CCB-Adressen im AMO SIPCO (auch für NCUI/OpenScape 4000 SoftGate) einfach ändern können und der Access Point wird ab dem nächsten Startup die neue HSR-Verbindung akzeptieren. Die alternative Methode, die im Abschnitt 2.14, „IP-Adressänderungen“ beschrieben ist, kann nach wie vor für laufende Systeme mit aktiven HSR-Verbindungen verwendet werden.

11 Access Point Emergency (APE)

11.1 Leistungsmerkmalbeschreibung Access Point Emergency

Mit dem Leistungsmerkmal Access Point Emergency gilt es, den Betrieb der Access Points/OpenScape 4000 SoftGates unabhängig von der Verfügbarkeit des Zentralsystems aufrecht zu erhalten.

Hierfür wird die Möglichkeit geschaffen, Access Points/OpenScape 4000 SoftGates von zusätzlichen, räumlich verteilbaren Steuerungen aus zu betreiben. Diese zusätzlichen Steuerungen - „Survivability Unit“ genannt - können in jedem Access Point vom Typ AP 3700 IP montiert werden.

Prinzipiell ist es möglich, von einer Survivability Unit aus alle Access Points/ OpenScape 4000 SoftGates eines OpenScape 4000 Systems zu steuern (eine mögliche Begrenzung stellt die Prozessorleistung der Survivability Unit dar). Derartige Szenarien verzichten meist auf „klassische“ Shelves mit TDM-Anbindung und verwenden ausschließlich IPDA Access Points oder OpenScape 4000 SoftGates.

Im Falle des Leistungsmerkmals „Survivable OpenScape 4000 SoftGate“ wird die Survivability Unit als Software auf den Rechnern des OpenScape 4000 SoftGates realisiert. Die Access Points/OpenScape 4000 SoftGates sind auf dem Campus verteilt und über eine hochverfügbare IP Infrastruktur vernetzt. Ist der Communication Server im Haupt-Rechenzentrum nicht verfügbar, so übernimmt die Survivability Unit den gesamten Betrieb der Anlage.

Es steht die folgende Umgebung zur Verfügung:

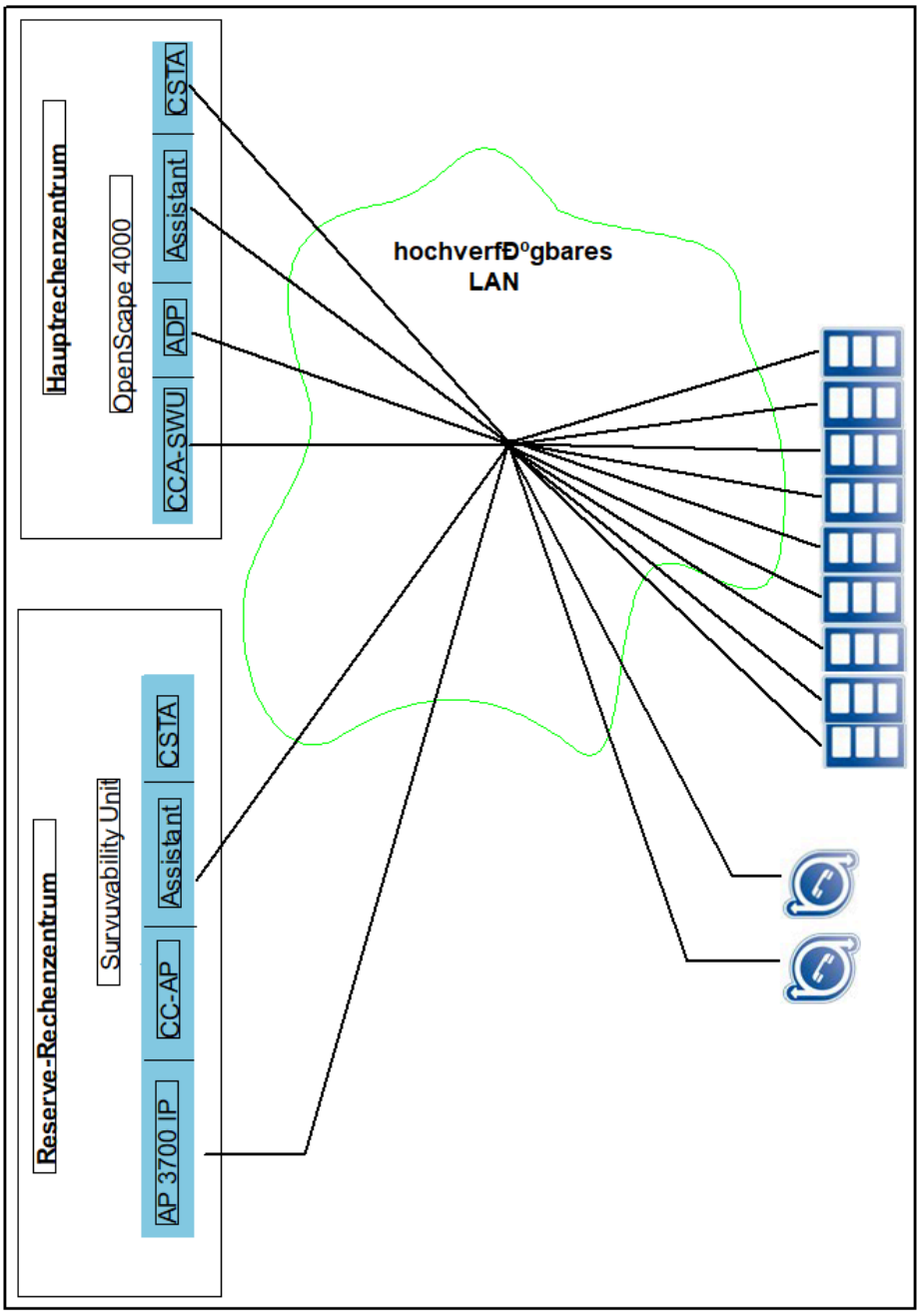
OpenScape 4000 Plattform: sie ist der Host für die folgenden virtuellen Maschinen (VM):

- VM ADP, CCA, CCB, CCAP (RMX)
- VM Assistant
- VM CSTA

11.1.1 Einsatz-Szenarien für Access Point Emergency

11.1.1.1 LAN-Szenario

Die zentrale Steuerung - der Communication Server - steht dabei oft im Haupt-Rechenzentrum, die Access Points/OpenScape 4000 SoftGates mit der Survivability Unit im Reserve-Rechenzentrum. Die Access Points/OpenScape 4000 SoftGates sind auf dem Campus verteilt und über eine hochverfügbare IP Infrastruktur vernetzt. Ist der Communication Server im Haupt-Rechenzentrum nicht verfügbar, so übernimmt die Survivability Unit den gesamten Betrieb der Anlage.



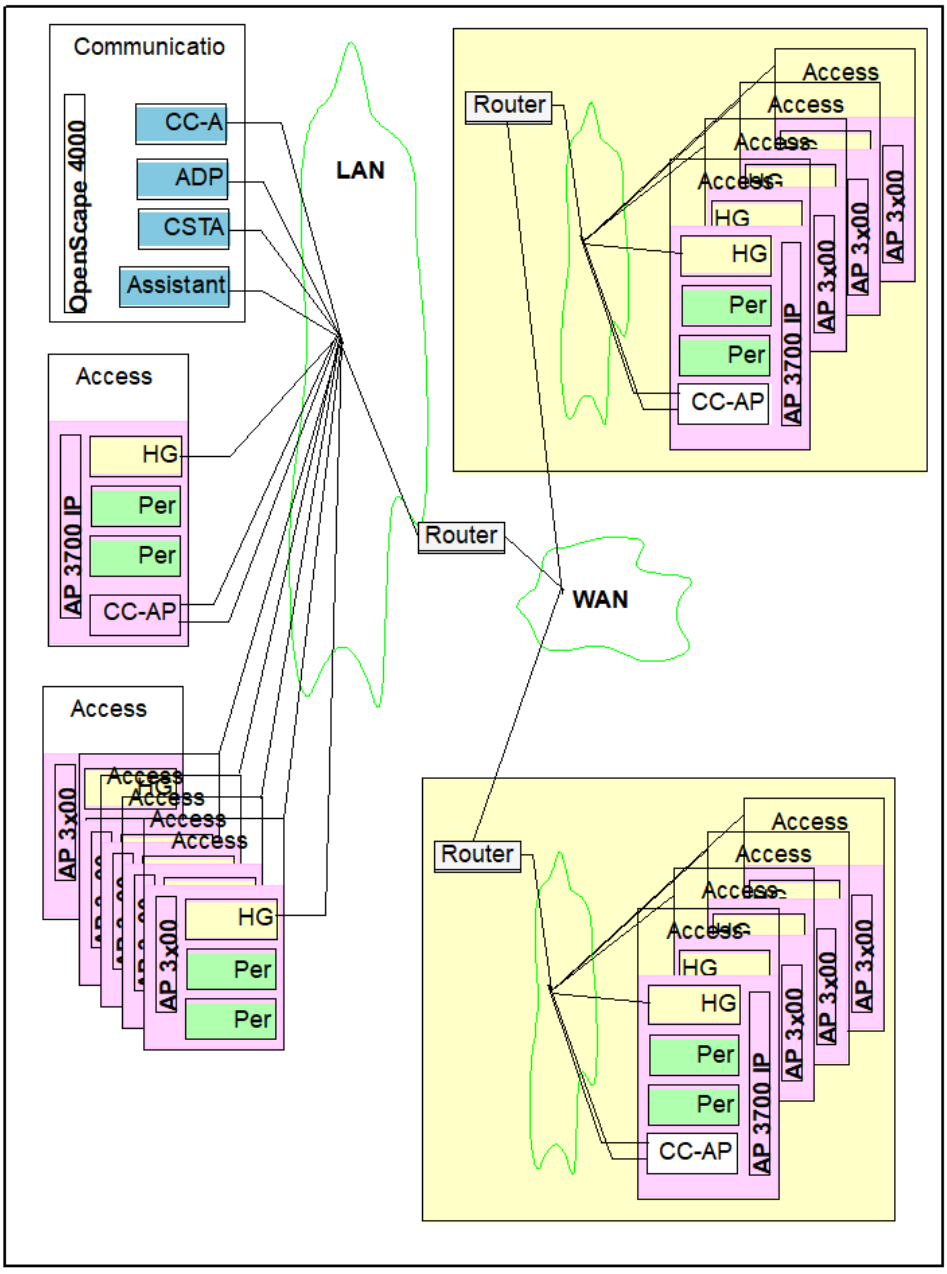
LAN-Szenario

In allen folgenden Bildern wird die Survivability Unit, wie auch an allen betriebstechnischen Bedienoberflächen, kurz mit CC-AP bezeichnet. Das ist die logische Fortschreibung der Bezeichnung für die Steuerungsprozessoren (CCA-SWU und ADP). Natürlich läuft auf der Survivability Unit nicht nur der CC-AP, sondern zusätzlich auch wie im Host System OpenScape 4000 Assistant und OpenScape 4000 CSTA.

11.1.1.2 LAN-/WAN-Szenario

Sind im Netz WAN-Strecken enthalten, über die z.B. Standorte mit mehreren IPDA Access Points/OpenScape 4000 SoftGates angekoppelt sind, so bietet

es sich an, diese LAN-Inseln mit jeweils einer eigenen Survivability Unit auszustatten. Die Access Points/OpenScape 4000 SoftGates können dann nicht nur bei Ausfall der zentralen Steuerung, sondern auch bei Ausfall der WAN-Anbindung autonom betrieben werden.



LAN-/WAN-Szenario

11.1.1.3 Filialen- (WAN) Szenario

Bei der klassischen Filialstruktur sind viele, relativ kleine, aber räumlich weit verteilte Filialen über schlank dimensionierte WAN-Strecken an die Unternehmenszentrale angebunden. Hier kann es sinnvoll sein, den IPDA Access Point/das OpenScape 4000 SoftGate jeder einzelnen Filiale mit einer Survivability Unit auszustatten. Sie kann dann auch hier bei Ausfall der

zentralen Steuerung und bei Ausfall der WAN-Anbindung einen autonomen Betrieb der Filiale sicherstellen.

11.1.2 Access Point Emergency und Signaling Survivability

Das Leistungsmerkmal AP Emergency und Signaling Survivability schließen sich nicht gegenseitig aus. Sie ergänzen sich vielmehr. In allen Szenarien, die WAN-Strecken enthalten, lässt sich ein sinnvolles Stufenkonzept der Ausfallsicherheit implementieren.

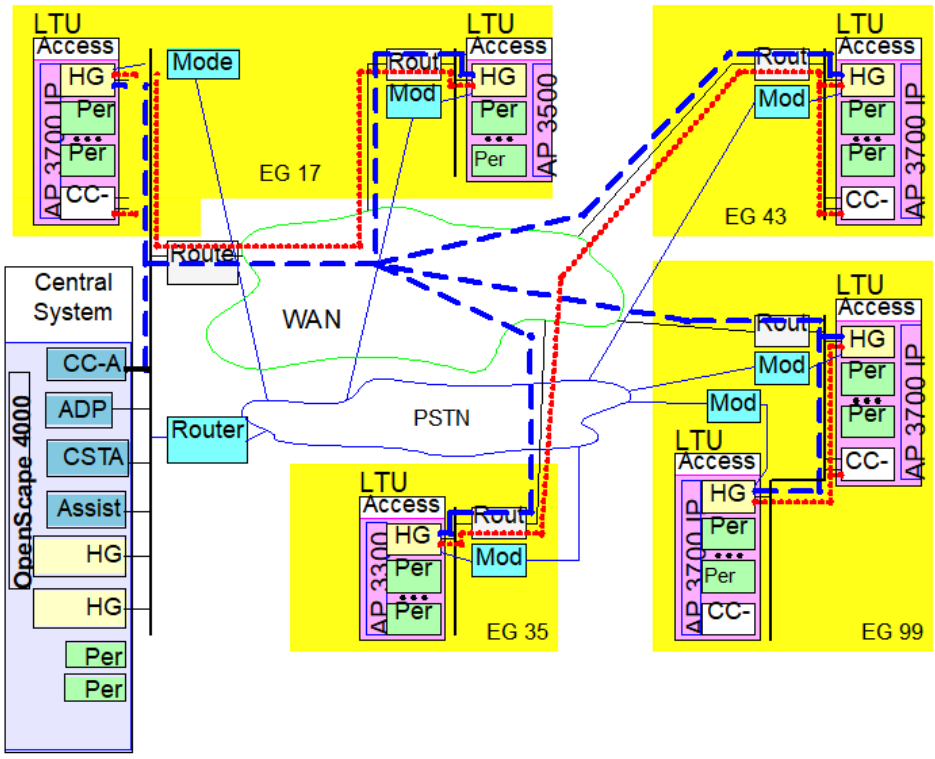
1) Signaling Survivabilty hält den Betrieb der Access Points/OpenScape 4000 SoftGates durch die zentrale Steuerung aufrecht, wenn es zu Störungen im WAN kommt. Die Umschaltung des Signalisierungspfades (Signaling Survivabilty) arbeitet unterbrechungsfrei.

2) AP Emergency übernimmt den Betrieb der Access Points/OpenScape 4000 SoftGates, wenn die zentrale Steuerung ausfällt.

Hinweise:

- Die HSR-Signalisierungs-Verbindung vom APE zum Access Point/ OpenScape 4000 SoftGate ist immer nur eine reine TCP/IP-Verbindung, keine „HSR über UDP“ - Verbindung (unabhängig von der SIGMODE Konfiguration im AMO UCSU).
- Zwischen APE und Access Point/OpenScape 4000 SoftGate existiert immer nur eine einzelne HSR-Signalisierungs-Verbindung über einen definierten Pfad und kein alternativer Survivability Pfad.

Bild 45 „AP Emergency Szenario“ zeigt ein Misch-Szenario, das im weiteren Verlauf des Handbuch herangezogen wird. Dieses Bild zeigt in blau gestrichelten Linien die Kommunikationswege zwischen der zentralen Steuerung und den Access Points/OpenScape 4000 SoftGates, in rot punktierten Linien die Kommunikation zwischen den Survivability Units und den ihnen zugeordneten Access Points/OpenScape 4000 SoftGates.



AP Emergency Szenario

11.1.3 Survivability Unit im AP 3700 IP

Die Survivability Unit kann nur in Access Points vom Typ AP 3700 IP eingesetzt werden. Dennoch kann sie IPDA Access Points aller möglichen Bauformen (AP 3300 IP, AP 3500 IP, AP 3700 IP) und OpenScape 4000 SoftGates steuern. Bei den Access Points spielt es keine Rolle, ob die Access Points mit NCUI2+ oder NCUI4 ausgestattet sind.

Die Survivability Unit besteht aus einer Kassette mit cPCI Backplane, DSCXL2 Prozessor, Stromversorgung und redundanten Lüftereinschüben.

Sie kann - abhängig vom Stromversorgungsmodul - aus 110/230V Wechselstrom oder 48 V Gleichstrom gespeist werden. Im AP 3700 IP besteht keinerlei elektrische Verbindung zwischen dem Access Point Anteil und der Survivability Unit.

Die Kommunikation zwischen Survivability Unit und NCUI2+/4 des selben Access Points/OpenScape 4000 SoftGates läuft ausschließlich über das IP-Netz.

11.1.4 Survivability Unit am OpenScape 4000 SoftGate

Im Falle des Leistungsmerkmals „Survivable OpenScape 4000 SoftGate“ wird die Survivability Unit als Software auf dem Rechner des OpenScape 4000 SoftGates realisiert.

11.1.5 Zuordnung von Access Points/OpenScape 4000 SoftGates zur Survivability Unit

Die Access Points/OpenScape 4000 SoftGates werden nicht unmittelbar einer Survivability Unit zugeordnet. Stattdessen werden sie einer Emergency Gruppe zugeordnet. Die Gruppe legt fest, welche Access Points/OpenScape 4000 SoftGates gleich zu behandeln sind.

So macht es zum Beispiel wenig Sinn, einen Access Point/OpenScape 4000 SoftGate ohne Amtszugang alleine von der Steuerung des Host Systems auf die Steuerung durch eine Survivability Unit umzuschalten. Sinnvoller ist es, gemeinsam eine ganze Gruppe umzuschalten, die auch einen Access Point/OpenScape 4000 SoftGate mit Amtszugang enthält. Die Regeln für die Umschaltung werden je Access Point/OpenScape 4000 SoftGate und je Gruppe definiert.

Durch Einführung der abstrakten Emergency Gruppen ist es möglich, mehrere Gruppen unabhängig von einer gemeinsamen Survivability Unit steuern zu lassen.

Die hierarchische Zuordnung ist einfach:

1) Ein Access Point/OpenScape 4000 SoftGates kann zu genau einer Emergency Gruppe gehören.

2) • Eine Emergency Gruppe kann von genau einer Survivability Unit gesteuert werden.

Betriebstechnisch sind alle Kombinationen mit 1 .. 83 Access Points/ OpenScape 4000 SoftGates in 1 .. 83 Emergency Gruppen an 1 .. 83 Survivability Units möglich. Eine einzige APE-Einheit kann alle 83 Access Points steuern.

Access Points/OpenScape 4000 SoftGates werden nach Verbindungsart unterschieden in „Direct Link“ (APDL) und „Networked Link“ (APNW). Details siehe „IP Distributed Architecture“, Abschnitt 2.2, „Access Point“.

Wichtig: Eine Survivability Unit in einem **APNW**-Access Point/OpenScape 4000 SoftGate kann keine **APDL**-Access Points/OpenScape 4000 SoftGates steuern. Eine Survivability Unit in einem **APDL**-Access Point/OpenScape 4000 SoftGate kann aber sowohl **APDL**- als auch **APNW**-Access Points/OpenScape 4000 SoftGate steuern.

11.1.6 Umschaltung in den Emergency-Betrieb

Wenn eine HG 3575/virtuelle HG 3575 die Unterbrechung der Signalisierungsverbindung zur zentralen Steuerung feststellt, meldet sie das der zugeordneten Survivability Unit.

Der Emergency-Betrieb, d.h. die Steuerung eines Access Points/OpenScape 4000 SoftGates durch eine Survivability Unit, ist ein Eskalationsschritt nach Signaling Survivability. Ist Signaling Survivability konfiguriert, wird bei Verbindungsverlust zuerst versucht, die Steuerung der Access Points/ OpenScape 4000 SoftGates über Modem aufzunehmen. Scheitert dies, z.B. weil die zentrale Steuerung nicht verfügbar ist, so wird der Emergency-Betrieb eingeleitet.

Die Survivability Unit entscheidet anhand vorkonfigurierter Regeln, ob sie die Steuerung eines Access Points/OpenScape 4000 SoftGates übernehmen soll, oder nicht.

1) Jedem Access Point/OpenScape 4000 SoftGate ist ein Gewicht zugeordnet.

2)
- Wenn die Summe der Gewichte aller Access Points/OpenScape 4000 SoftGates einer Emergency Gruppe, welche die Verbindung zur zentralen Steuerung verloren haben, größer ist als die für die Gruppe festgelegte Schwelle, übernimmt die Survivability Unit die Steuerung aller Access Points/OpenScape 4000 SoftGates, welche dieser Gruppe zugeordnet sind
- Access Points/OpenScape 4000 SoftGates können aber auch so konfiguriert werden, dass sie unabhängig von der Gewichtung immer auch einzeln in die Steuerung der Survivabilty Unit übernommen werden.
- Zusätzlich können Sie
- – einzelne Access Points/OpenScape 4000 SoftGates
  – alle Access Points/OpenScape 4000 SoftGates einer Emergency Gruppe
  – alle Access Points/OpenScape 4000 SoftGates aller Emergency Gruppen einer Survivability Unit oder
  – alle Access Points/OpenScape 4000 SoftGates des gesamten OpenScape 4000 Systems

  administrativ in die Steuerung durch die zugeordnete(n) Survivability Unit(s) zu schalten.

  Die Übernahme der Steuerung eines Access Points/OpenScape 4000 SoftGates durch die Survivability Unit erfolgt dadurch, dass die Survivability Unit die HG 3575/virtuelle HG 3575 anweist, einen Restart durchzuführen und danach mit der Survivability Unit hochzulaufen. Der Restart der HG 3575/virtuelle HG 3575 verursacht einen Restart aller peripheren Baugruppen im Access Point/OpenScape 4000 SoftGate.
- Alle Gespräche werden getrennt.
- Leistungsmerkmale mit aktiver Anmeldung z.B. mobiler Teilnehmer (PIN, Mobile-HFA) werden abgemeldet.
- Vom Anwender konfigurierbare Leistungsmerkmale wie z.B. Tastenbelegungen (Namenstasten, Direktruftasten), Anrufumleitung, Termine, etc., werden in dem Zustand aufgesetzt, wie sie zum Zeitpunkt der Datenübernahme aus dem Zentralsystem waren (siehe auch Abschnitt 1.8, „Konfigurationsdaten“).

11.1.7 Rückschaltung in den Normalbetrieb

Stellt eine HG 3575/virtuelle HG 3575 fest, dass die Signalisierungsverbindung zur zentralen Steuerung wiederhergestellt ist, meldet sie das der zugeordneten Survivability Unit.

Die Survivability Unit entscheidet anhand vorkonfigurierter Regeln, ob sie die Steuerung eines Access Points/OpenScape 4000 SoftGates an das Host System zurückgeben soll, oder nicht.

1) Jeder Access Point / jedes OpenScape 4000 SoftGate einer Emergency Gruppe muss für eine konfigurierbare Mindestzeit eine stabile Verbindung zur zentralen Steuerung haben

2)
- Die automatische Rückschaltung ist nur in einem konfigurierbaren Intervall der Tageszeit erlaubt. Das Intervall kann auf 24 Stunden eingestellt werden, so dass jederzeit automatisch zurückgeschaltet werden kann.
- Die automatische Rückschaltung kann abgeschaltet werden.
- Zusätzlich können Sie
- – einzelne Access Points/OpenScape 4000 SoftGates,
  – alle Access Points/OpenScape 4000 SoftGates einer Emergency Gruppe,
  – alle Access Points/OpenScape 4000 SoftGates aller Emergency Gruppen einer Survivability Unit oder
  – alle Access Points/OpenScape 4000 SoftGates des gesamten OpenScape 4000 Systems

  administrativ an die zentrale Steuerung zurückzuschalten.

  Die Übergabe der Steuerung eines Access Points/OpenScape 4000 SoftGates an die zentrale Steuerung erfolgt dadurch, dass die Survivability Unit die HG 3575/virtuelle HG 3575 anweist, einen Restart durchzuführen und danach mit der zentralen Steuerung hochzulaufen. Der Restart der HG 3575/virtuelle HG 3575 verursacht einen Restart aller peripheren Baugruppen im Access Point/OpenScape 4000 SoftGate.
- Alle Gespräche werden getrennt.
- Leistungsmerkmale mit aktiver Anmeldung z.B. mobiler Teilnehmer (PIN, Mobile-HFA) werden abgemeldet.
- Vom Anwender konfigurierbare Leistungsmerkmale wie z.B. Tastenbelegungen (Namenstasten, Direktruftasten), Anrufumleitung, Termine, etc., werden in dem Zustand aufgesetzt, der im Zentralsystem aktiv ist - d.h. in der Regel, wie er vor der Umschaltung aktiv war.

11.1.8 Konfigurationsdaten

Das gesamte OpenScape 4000 System mit all seinen Access Points/ OpenScape 4000 SoftGates und Survivability Units wird ausschließlich im Zentralsystem konfiguriert.

Eine lokale Administration des Leistungsmerkmals an der Survivability Unit ist nicht möglich. Ausnahme: OpenScape 4000 Assistant, Backup and Restore.

In konfigurierbaren Zeitabständen - typischerweise einmal täglich - wird eine spezielle Sicherung der Datenbasis des OpenScape 4000 Systems durchgeführt (OpenScape 4000 Assistant > Backup und Restore im Host System).

Die Survivability Units prüfen kontinuierlich (alle 10 Minuten), ob eine neue Sicherung der OpenScape 4000 Datenbasis verfügbar ist. Wenn die Survivability Unit keine Access Points/OpenScape 4000 SoftGates aktiv steuert (Emergency Betrieb), lädt sie die gesicherten Daten herunter und übernimmt sie durch einen Reload (OpenScape 4000 Assistant > Backup and Restore auf der Survivability Unit).

Die Sicherungsdaten werden auf einem File-Server abgelegt. Das kann ein File-Server im Rechenzentrum des Kunden sein. Es ist aber auch möglich die Plattform des OpenScape 4000 Managers als File-Server zu nutzen.

Auf dem File-Server wird die tägliche Sicherung so angelegt, dass sie immer das vollständige System mit Datenbasis, Patches und Software enthält.

Die Übertragung vom Host System zum File-Server und vom File-Server zur Survivability Unit erfolgt aber optimiert. Nur unterschiedliche Daten werden tatsächlich übertragen.

Mehr Informationen zur Applikation „Backup und Restore“ finden Sie in der Online-Hilfe.

11.1.9 Übernahme von Systemausgaben und Patches

Die Komplexität eines OpenScape 4000 Systems wird durch Survivability Units erheblich erhöht. Um den Betriebs- und Wartungsaufwand gering zu halten, erfolgt die Verteilung von Systemausgaben und Patches an die Survivability Units automatisch.

Dazu werden neue Systemausgaben und Patches in den Backup/Restore-Prozess für die Datenbasis mit eingeschlossen (siehe Abschnitt 1.8, „Konfigurationsdaten“).

11.1.10 Verbindung zwischen den Teilsystemen (Inseln)

Zerfällt ein OpenScape 4000 System im Emergency Betrieb in mehrere autonome Inseln, so stellt sich die Frage: Wie wird zwischen den Inseln kommuniziert? Dabei definiert sich die autonome Insel durch eine Survivability Unit und alle Access Points/OpenScape 4000 SoftGates, welche sie gerade aktiv steuert.

Innerhalb jeder einzelnen Insel bleibt alles beim alten:

- Gespräche zwischen Teilnehmern im selben Access Point/OpenScape 4000 SoftGate werden innerhalb des Access Points/OpenScape 4000 SoftGates geschaltet.
- Gespräche zwischen Teilnehmern an unterschiedlichen Access Points/ OpenScape 4000 SoftGates einer Insel werden über IP Verbindungen zwischen den Access Points/OpenScape 4000 SoftGates geschaltet.
- Kommende / gehende Amtsgespräche werden über die Amtsschnittstellen der Insel geführt.
- Kommende / gehende Gespräche in vernetzte Anlagen werden über die Querverbindungsschnittstellen der Insel geführt.

Was passiert mit Gesprächen, welche einen Teilnehmer in einer anderen Insel als Ziel haben?

Alle Survivability Units haben die selbe und vollständige Datenbasis des Zentralsystems. Daher kennt jede Insel jeden Teilnehmer der Gesamtkonfiguration, also auch alle Teilnehmer der anderen Inseln. Access Points/OpenScape 4000 SoftGates außerhalb der Insel sind konfiguriert, aber nicht erreichbar. Damit sind auch alle Baugruppen und die darauf befindlichen Teilnehmer-, Amts- und Querleitungssätze bekannt und hierarchisch gesperrt (UNACH).

Obwohl es vorkommen kann, dass die IP Infrastruktur zwischen manchen Inseln noch intakt ist, werden keine Insel-übergreifenden Gespräche zwischen den Access Points/OpenScape 4000 SoftGates über IP geschaltet.

Zur Insel-übergreifenden Kommunikation bleiben also noch die Amtsschnittstellen. Ein bekannter, aber nicht direkt erreichbarer Teilnehmer in einer anderen Insel kann also noch über Amt erreicht werden. Das

Leistungsmerkmal „Alternate Routing on Error“ ermöglicht speziell für den Emergency Betrieb eine regelbasierte Rufnummernmodifikation.

Für den Verkehr zwischen den Inseln ist damit die grundsätzliche Erreichbarkeit durch Basic Call sichergestellt.

Voraussetzung ist, dass die Amtsanschlüsse in den Inseln unterschiedliche Kennzahlen verwenden. Verwenden alle Amtsanschlüsse die selbe Kennzahl, muss vom Carrier ein gezieltes Routing an Hand der vollständigen gerufenen Nummer durchgefügt werden (**CENTREX**).

Sind die Inseln in ein übergreifendes OpenScape 4000 Netzwerk mit QSig-Trunks eingebunden, so muss die LCR-Konfiguration den Normal- und den Emergency-Fall berücksichtigen, da es ja nur eine Konfiguration der Anlage gibt. Auch in diesem Fall ist für kommenden, anlagenübergreifenden Verkehr zu einem Access Point/OpenScape 4000 SoftGate, der zu einer Transitverbindung führt, die grundsätzliche Erreichbarkeit durch Basic Call sichergestellt. Zur Unterstützung von netzweiten Leistungsmerkmalen sollen die Inseln als virtuelle Knoten eingerichtet werden.

Payload Survivabilty kann im Emergency Betrieb nicht greifen, da die betroffenen Inseln keine gemeinsame Steuerung mehr haben.

11.1.11 Zeitsynchronisation

Für viele Funktionen der OpenScape 4000 ist eine exakte Uhrzeit erforderlich (Gebührenerfassung, uhrzeitabhängige Wege, Nachtschaltung, etc.). Alle Uhren im System (bis zu 84) müssen synchron laufen.

Es gibt zwei Möglichkeiten, die Zeitsynchronisation durchzuführen:

1) Im IP-Netz steht ein Zeit-Server zur Verfügung, der die Zeitsynchronisation aller Prozessoren der OpenScape 4000 (Host System und alle Survivability Units) mittels Network Time Protocol unterstützt.

2) Im IP-Netz steht **kein** Zeit-Server zur Verfügung. Die OpenScape 4000 Plattform stellt dann ihre lokale Uhrzeit zur Synchronisation aller Survivability Units über das Netzwerk zur Verfügung.

11.1.12 Lizenzierung der Leistungsmerkmale

Für den Betrieb einer Survivability Unit in einem OpenScape 4000-System wird eine entsprechende Lizenz benötigt.

Alle Host-System-Lizenzen werden auch auf den Survivability Units im Notfallmodus verwendet. Die Survivability Units werden ohne Lizenzen betrieben. Aus diesem Grund beginnt nach einer Wiederherstellung eine 30-tägige Grace Period. Nach Ablauf dieser 30 Tage werden alle SWU-Leistungsmerkmale gesperrt.

Es wird empfohlen, mindestens einmal pro Monat ein APE-Backup auf dem Zentralsystem einzuplanen. Dies sorgt nicht nur für ein APE-Restore auf der Survivability Unit, durch das die 30-tägige Grace Period zurückgesetzt wird, sondern auch für die Konsistenz der Datenbanken der einzelnen Survivability Units mit dem Zentral-/Host-System im Fall von Konfigurationsänderungen.

Anmerkung: Wenn die 30-tägige Grace Period des Lizenzmanagement auf dem Zentralsystem bereits läuft und der Betrieb nur noch 10 Tage lang uneingeschränkt möglich ist, gilt diese Einschränkung auch für alle Survivability Units nach einer Wiederherstellung.

11.1.13 Unterstützung von Applikationen im Emergency-Betrieb

Die OpenScape CSTA wird von der AP Emergency-Funktion unterstützt, sodass einige Anwendungen sowohl auf dem Host-System als auch auf der Survivability Unit funktionieren können.

Voraussetzungen dafür sind aber:

- Die Anwendung hat eine funktionierende IP-Verbindung zur CSTA der Survivability Unit
- Die Anwendung kann nur Ressourcen überwachen/nutzen, die von derselben Survivability Unit gesteuert werden.

11.2 Einrichtung des Leistungsmerkmals APE (Access Point Emergency)

Zum Einrichten des Leistungsmerkmals AP Emergency ist ein gutes Verständnis der Arbeitsweise dieses Leistungsmerkmals erforderlich. Diesen Überblick gibt Kapitel 1, „Leistungsmerkmalbeschreibung Access Point Emergency“

Wichtig: Für den Emergency Betrieb ist meist eine Konfigurationen des Leistungsmerkmals „Alternate Routing on Error“ nötig, damit sich Teilnehmer unterschiedlicher „Emergency-Inseln“ erreichen können. Dies ist im Servicehandbuch „Kapitel 3 - Feature-Nutzungsbeispiele > Alternatives Routing im Fehlerfall“ beschrieben. In manchen Installationen müssen auch zusätzliche Amts-/Querverbind-ungssätze eingerichtet werden, um aus den „Inseln“ in ein HiPath 400/OpenScape 4000 Netz oder in das öffentliche Netz zu gelangen. Schließen Sie diesen Teil der Konfiguration ab, **bevor** Sie das Leistungsmerkmal AP Emergency einrichten. Sie können nicht verhindern, dass APE wirkt, wenn z.B. im Netzwerk eine Störung auftritt. Sind dann aber die oben genannten Voraussetzungen noch nicht erfüllt, kann es vorkommen, dass eine „Emergency-Insel“ in ihrer Kommunika-tionsfähigkeit eingeschränkt ist und z.B. Notrufe nicht mehr möglich sind.

Die Einrichtung des Leistungsmerkmals gliedert sich in die folgenden Schritte:

- Aktivitäten am OpenScape 4000 Zentralsystem
- – Einrichten oder Ändern eines CC-AP/Survivable OpenScape 4000 SoftGate in der OpenScape 4000
  – Einrichten/Ändern einer Emergency Gruppe
  – Einrichten von Access Points/OpenScape 4000 SoftGates für AP Emergency

  - Einrichten der Display-Anzeige für AP Emergency am Endgerät
  - Festlegen der Umschalteverzögerung
  - Zeitsynchronisation zwischen Host System und CC-AP/Survivable OpenScape 4000 SoftGate
- Aktivitäten an der Survivability Unit - CC-AP/Survivable OpenScape 4000 SoftGate
- – Erstinbetriebnahme des CC-AP/Survivable OpenScape 4000 SoftGate
  – Verifizieren / Abnahme der AP-Emergency Konfiguration

11.2.1 Einrichten oder Ändern eines CC-AP/Survivable OpenScape 4000 SoftGate in der OpenScape 4000

Der CC-AP/das Survivable OpenScape 4000 SoftGate wird immer mit der LTU-Nummer des Access Points/OpenScape 4000 SoftGates adressiert, in welchem er eingebaut ist.

Als Konfigurationsdaten werden nur die IP-Adresse für den IPDA-LAN-Anschluss des CC-AP/Survivable OpenScape 4000 SoftGate und die Betriebsart der Ethernet-Schnittstelle benötigt. Alle anderen für die IP-Kommunikation notwendigen Parameter werden aus der Konfiguration der HG 3575 des Access Points/OpenScape 4000 SoftGates übernommen.

Tabelle 67: Abgeleitete Konfigurationsparameter für CC-AP/Survivable OpenScape 4000 SoftGate

Parameter	„Network Link“ Access Point/OpenScape 4000 SoftGate	„Direct Link“ Access Point/ OpenScape 4000 SoftGate
IP address	direkt eingestellt	
Netmask	Netzmaske der HG 3575 APRT: TYP=APNET - NETMASK	Netzmaske des OpenScape 4000 LAN Segments SIPCO: TYP=LSNET - NETMASK
Default-Router	Default-Router im Netz des Access Points/OpenScape 4000 SoftGates UCSU: ART=AP - APRTADR	Default-Router im Netz des Access Points/OpenScape 4000 SoftGates UCSU: ART=AP - APRTADR das ist in der Regel der Default-Router des OpenScape 4000 LAN Segments SIPCO: TYP=LSNET - DEFRT
VLAN-Tagging	STMIB: MTYP=NCUI2 - TYP=IFDATA - VLAN	
VLAN-ID	STMIB: MTYP=NCUI2 - TYP=IFDATA - VLANID	

Parameter	„Network Link“ Access Point/OpenScape 4000 SoftGate	„Direct Link“ Access Point/ OpenScape 4000 SoftGate
TOS-Byte für die Signalisierung Verbindung	STMIB: MTYP=NCUI2 - TYP=IFDATA - TOSLAN	

Die Ethernet-Schnittstelle **muss** bei beiden beteiligten Schnittstellenpartnern (CC-AP/Survivable OpenScape 4000 SoftGate bzw. LAN-Switch, -Router) **identisch** eingestellt werden!

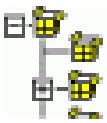
Wichtig: Die feste Einstellung eines Schnittstellenpartners führt zusammen mit der „Autonegotiate“-Einstellung des anderen Partners zu Problemen.

Wichtig: Fehlerhafte Einstellungen können vom System meist nicht erkannt und daher nicht gemeldet werden. Gerade wenn ein Gerät auf vollduplex, das andere auf halbduplex arbeitet, ist das nicht sofort bemerkbar. Unter hoher Last wird das auf halbduplex eingestellte Gerät verstärkt späte Kollisionen melden und die Paketverzögerung steigt stark an.

Wichtig: Unterstützt der LAN-Port, mit dem der CC-AP/das Survivable OpenScape 4000 SoftGate verbunden sind, keine Autonegotiation, oder funktioniert diese nicht zuverlässig, so muss die Ethernet-Schnittstelle des CC-AP/Survivable OpenScape 4000 SoftGate auf feste Werte eingestellt werden.

Im Beispiel wird der CC-AP/das Survivable OpenScape 4000 SoftGate im Access Point/OpenScape 4000 SoftGate 99 eingerichtet, bzw. geändert.

Die IP-Adresse ist 192.168.23.199, die Ethernet-Schnittstelle wird auf 10 MBit/s, halbduplex eingestellt.

	**Configuration Management > Anlagendaten > IPDA > IPDA - CC-Access Point** Auf **Suchen** klicken und CC-AP/Survivable OpenScape 4000 SoftGate auswählen oder über das Menü **Neu** neu anlegen. **IP-Adresse** sowie Übertragungsgeschwindigkeit (**Geschwindigkeit**) und Modus der Ethernet-Schnittstelle einstellen und auf **Sichern** klicken.

	`EINRICHTEN-`
	`APESU:DATEN=CCAP,CCAPNUM=99,IPADR=192.168.23.199;`
	oder
	`AENDERN-`
	`APESU:DATEN=CCAP,CCAPNUM=99,IPADR=192.168.23.199;`

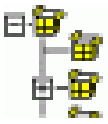
Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

Tabelle 68: Parameter AMO APESU im EINRICHTEN- oder AENDERN-Zweig, DATEN=CCAP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APESU	CCAPNUM	d	LTU-Nummer des Access Points/ OpenScape 4000 SoftGates, in welchem der CC-AP/das Survivable OpenScape 4000 SoftGate eingebaut ist.
	CCAPNO	e	Line/Trunk Unit Number of the access point/ OpenScape 4000 SoftGate, where the CC-AP/Survivable OpenScape 4000 SoftGate is installed.
	IPADR	d	IP Adresse des CC-AP/Survivable OpenScape 4000 SoftGate.
	IPADDR	e	IP Address of the CC-AP/Survivable OpenScape 4000 SoftGate

11.2.2 Löschen eines CC-AP/Survivable OpenScape 4000 SoftGate in der OpenScape 4000

Beim Löschen eines CC-AP/Survivable OpenScape 4000 SoftGate werden automatisch auch alle ihm zugeordneten Emergency Gruppen und die AP-Emergency Konfiguration der zugeordneten Access Points/ OpenScape 4000 SoftGates gelöscht. Sollen Emergency Gruppen weiter bestehen bleiben, müssen sie vorher einem anderen CC-AP/ Survivable OpenScape 4000 SoftGate zugeordnet werden (`AENDERN-APESU:DATEN=APEGRP,EGRPNUM=xx,CCAPNUM=yy;`).

	**Configuration Management > Anlagendaten > IPDA > IPDA - CC-Access Point** Auf **Suchen** klicken und den CC-AP/Survivable OpenScape 4000 SoftGate auswählen, dann auf **Löschen** klicken.
	`LOESCHEN-APESU:CCAPNUM=99;`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

11.2.3 Einrichten/Ändern einer Emergency Gruppe

Die Emergency Gruppe dient als logisches Bindeglied zwischen Access Point/ OpenScape 4000 SoftGate und CC-AP/Survivable OpenScape 4000 SoftGate.

Ein Access Point/OpenScape 4000 SoftGate ist Mitglied in genau einer Emergency Gruppe. Eine Emergency Gruppe wird von genau einem CC-AP/ Survivable OpenScape 4000 SoftGate bedient.

Die Emergency Gruppe wurde eingeführt, um komplette Gruppen von Access Points/OpenScape 4000 SoftGates gemeinsam und gleichzeitig aus der Steuerung des Zentralsystems in die Steuerung des CC-AP/Survivable OpenScape 4000 SoftGate zu überführen - und umgekehrt.

Auch wenn sich das Leistungsmerkmal AP Emergency primär um den Totalausfall der zentralen Steuerung kümmern soll, liegt die Komplexität in der angemessenen Handhabung von beliebigen Teil-Ausfällen der IP-Kommunikation.

Eine Emergency Gruppe fasst typischerweise Access Points/OpenScape 4000 SoftGates zusammen, welche miteinander eine überlebensfähige Einheit bilden. Das kann z. B. ein über WAN angebundener Außenstandort sein.

Durch Störungen im Routing kann es vorkommen, dass nur ein Teil der Access Points/OpenScape 4000 SoftGates einer Gruppe den Kontakt zur zentralen Steuerung verliert. Es wäre jetzt möglich, nur die betroffenen Access Points/OpenScape 4000 SoftGates in die Steuerung des CC-AP/Survivable OpenScape 4000 SoftGate zu überführen. Damit ist die Kommunikation zwischen den Access Points/OpenScape 4000 SoftGates der Gruppe aber unterbrochen. Gespräche gingen dann nur noch über Amt. Hat aber jeder Access Point/jedes OpenScape 4000 SoftGate einen eigenen Amtsanschluss? Wo hängen zentrale Ressourcen wie Ansagen, Server etc. ?

Es wird also häufig Sinn machen, eine Gruppe nur als Ganzes umzuschalten. Dann bleiben alle Access Points/OpenScape 4000 SoftGates unter **einer** Steuerung, die Kommunikation zwischen den Access Points/OpenScape 4000 SoftGates läuft über IP. Alle Access Points/OpenScape 4000 SoftGates können über einen gemeinsamen Amtsanschluss mit dem Rest der Anlage kommunizieren. In solchen Fällen werden die Access Points/OpenScape 4000 SoftGates **einer** Emergency Gruppe auch **einer** Source Group für Source Dependent Routing (siehe „IP Distributed Architecture (IPDA)“, Abschnitt 2.8, „Source Dependent Routing“) angehören.

Eine Emergency Gruppe wird durch eine frei wählbare Nummer identifiziert. Je nach Installation kann es von Vorteil sein, die Nummer der Emergency Gruppe an der Nummerierung der beteiligten Source Group oder der CC-AP/Survivable OpenScape 4000 SoftGate-Nummer zu orientieren.

Da Klartext mehr sagt, als jede noch so klug gewählte Nummer, kann jede Emergency Gruppe mit einem Namen versehen werden.

Jede eingerichtete Emergency Gruppe muss einem CC-AP/Survivable OpenScape 4000 SoftGate zugewiesen werden. Die Zuweisung kann geändert werden.

Ob alle Access Points/OpenScape 4000 SoftGates einer Emergency Group zum CC-AP/Survivable OpenScape 4000 SoftGate umgeschaltet werden, wird durch eine Gewichtung bestimmt. Jedem Access Point/OpenScape 4000 SoftGates ist eine Gewichtung zugeordnet. Jedem Access Point/ OpenScape 4000 SoftGate wird ein Gewicht zugeordnet, das er bei Ausfall

seiner Verbindung zur zentralen Steuerung in die Umschaltebewertung einbringt. Für die Gruppe kann ein Grenzwert definiert werden. Wird dieser Wert überschritten, erfolgt eine Umschaltung.

Durch höhere Gewichtung können Access Points/OpenScape 4000 SoftGates mit Amtsanschlüssen, zentralen Ressourcen oder VIP-Teilnehmern eher eine Umschaltung auslösen als Access Points/OpenScape 4000 SoftGates mit „Standard-Bestückung“.

Bei der Gewichtung muss sichergestellt sein, dass die Gewichte aller Access Points/OpenScape 4000 SoftGates, die einer Emergency Gruppe zugewiesen sind, den Grenzwert der Gruppe auch erreichen können. Das kann insbesondere bei Konfigurationsänderungen leicht übersehen werden.

Sind die IP-Verbindungen aller Access Points/OpenScape 4000 SoftGates zur zentralen Steuerung wieder verfügbar, gilt es die Rückschaltung auf die zentrale Steuerung zu organisieren. Es wird Kunden geben, welche eine sofortige Rückschaltung auf die zentrale Steuerung fordern, obwohl dabei Gespräche getrennt werden. Häufig wird aber die Rückschaltung zu bestimmten Zeiten verboten werden. Oder es wird von vorn herein ausschließlich eine administrative Umschaltung erlaubt.

AP Emergency bietet die Möglichkeit, eine automatische Rückschaltung zu aktivieren, oder ausschließlich die manuelle Rückschaltung zu erlauben. Die Parametrisierung der automatische Rückschaltung basiert auf der Ebene der Emergency Gruppen.

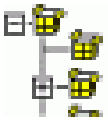
Für die Gruppe - und damit für alle Access Points/OpenScape 4000 SoftGates der Gruppe - kann bestimmt werden, wie lange die Verbindung zwischen jedem Access Point/OpenScape 4000 SoftGate und der zentralen Steuerung wieder ununterbrochen stabil sein muss, um eine Rückschaltung zu erwägen.

Ist die Stabilitätszeit erreicht, wird geprüft, ob es zum aktuellen Zeitpunkt erlaubt ist, zurückzuschalten. Hierfür werden Zeitfenster eingerichtet, innerhalb derer zurückgeschaltet werden darf. Das Zeitfenster wird durch Angabe einer Stunde (des Tages) begonnen und durch eine weitere Stundenangabe beendet. Um die Netzlast zeitgesteuerter Aktivitäten von der vollen Stunde weg zu verlegen, ist es üblich, einen zeitlichen Offset einzurichten. Hiermit kann bestimmt werden, wieviele Minuten nach der vollen Stunde das Rückschaltefenster geöffnet bzw. geschlossen wird. Ist z.B. der Rückschalte-Beginn auf 20, das Rückschalte-Ende auf 6 eingestellt bedeutet das bei einem Offset von 13, dass innerhalb der Zeit von 20:13 bis 06:13 automatisch rückgeschaltet werden kann. Trat in dieser Konfiguration eine Netzwerkstörung auf, die von 9:05 bis 9:15 die IP-Verbindung zwischen zentraler Steuerung und den Access Points/OpenScape 4000 SoftGates unterbrochen hat, so wird die automatische Rückschaltung um 20:13 erfolgen. Tritt die Störung innerhalb des Rückschaltefensters auf, erfolgt die Rückschaltung sofort, nachdem die IP-Verbindungen zwischen zentraler Steuerung und Access Points/OpenScape 4000 SoftGates wieder die Mindestzeit stabil sind.

Die manuelle Rückschaltung ist jederzeit möglich. Hier muss der Administrator sicherstellen, dass die Randbedingungen stimmen (ist die Rückschaltung erwünscht? - haben alle Access Points/OpenScape 4000 SoftGates wieder Verbindung mit der zentralen Steuerung?).

Fällt ein CC-AP/Survivable OpenScape 4000 SoftGate aus, während er aktiv Access Points/OpenScape 4000 SoftGates steuert, so ergibt sich folgendes Verhalten:

- Ist das Zentral-System verfügbar und hat es Kontakt zu einem betroffenen Access Point/OpenScape 4000 SoftGate, so übernimmt das Host System den Access Point/das OpenScape 4000 SoftGate wieder in seine Kontrolle, ohne die Stabilitätszeit und die eingestellte Umschaltezeit zu berücksichtigen.
- – Dies gilt nur, wenn automatische Rückschaltung eingerichtet ist.
  – Ist manuelle Rückschaltung eingerichtet, so wird ein Access Point/ OpenScape 4000 SoftGate bei Ausfall des CC-AP/Survivable OpenScape 4000 SoftGate während des Emergency-Betriebs **nicht** automatisch vom Host System übernommen.
- Ist das Zentral-System nicht verfügbar, so ist keine Steuerung mehr für den Access Point/das OpenScape 4000 SoftGate verfügbar. Er setzt sich immerhalb der konfigurierten Zeit zurück wartet darauf, dass eine Steuerung Kontakt mit ihm aufnimmt.

	**Configuration Management > Anlagendaten > IPDA > AP-Notfallgruppe** Auf **Suchen** klicken und Emergency Gruppe auswählen oder über das Menü **Neu** neu anlegen. Konfigurationsparameter einstellen und auf **Sichern** klicken.

	`EINRICHTEN-APESU:DATEN=APEGRP,EGRPNUM=2,CCAPNUM=99,SCHWELLE=100,RS-MODE=AUTO,NAME=„BERLIN“,STABIL=10,RSBEGIN=20,RSENDE=6,RSOFFSE`
	oder
	`AENDERN-APESU:DATEN=APEGRP,EGRPNUM=2,CCAPNUM=99,SCHWELLE=100,RS-MODE=AUTO,NAME=„BERLIN“,STABIL=10,RSBEGIN=20,RSENDE=6,RSOFFSE`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

Tabelle 69: Parameter AMO APESU im EINRICHTEN- oder AENDERN-Zweig, DATEN=APEGRP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APESU	EGRPNUM	d	Identifikations-Nummer der Emergency Gruppe. Wertebereich [1 .. 99]
	EGRPNO	e	Identification number of the Emergency Group. Range [1 .. 99]
	CCAPNUM	d	Nummer des CC-AP/Survivable OpenScape 4000 SoftGate, dem die Emergency Gruppe zugeordnet ist.

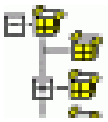
AMO	Parameter	Sprache/ Language	Beschreibung/Description
	CCAPNO	e	Number of the CC-AP/Survivable OpenScape 4000 SoftGate, to which the Emergency Group is assigned.
	SCHWELLE	d	Grenzwert für den Gewichtungsalgorithmus. Bei Erreichen bzw. Überschreiten werden die Access Points/OpenScape 4000 SoftGates der Emergency Gruppe in die Steuerung des CC-AP/Survivable OpenScape 4000 SoftGate umgeschaltet. Wertebereich [0 .. 1000]
	THRSHLD	e	Threshold for the weighing alogrithm. When reached or exceeded, the access points/OpenScape 4000 SoftGates of the Emergency Group are switched over into control of the CC-AP/Survivable OpenScape 4000 SoftGate. Range [0 .. 1000]
	RSMODE	d	Rückschaltemodus Bestimmt, ob die Access Points/OpenScape 4000 SoftGates der Emergency Gruppe automatisch, oder ausschließlich manuell zur zentralen Steuerung zurückgeschaltet werden dürfen. Werte: AUTO: Automatische Rückschaltung MAN: Manuelle Rückschaltung
	SBMODE	e	Switch-Back Mode Specifies if the access points/OpenScape 4000 SoftGates of the Emergency Group may be switched back to the central control automatically or only manually. Values: AUTO: Automatical Switch-Back MAN: Manual Switch-Back
	NAME	d	Name der Emergency Gruppe (maximal 22 Zeichen)
	NAME	e	Name of the Emergency Group (maximum 22 characters)

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	STABIL	d	Stabilitätszeit Minimale Zeitdauer, über welche alle Access Points/OpenScape 4000 SoftGates der Emergency Gruppe eine stabile Verbindung zur zentralen Steuerung haben müssen, bevor automatisch rückgeschaltet werden darf. Wertebereich [0 .. 255] Minuten
	STABLE	e	Stability time Minimum amount of time, during which all access points/OpenScape 4000 SoftGates of the Emergency Group must have a stable connection to central control, before they may be switched back. Range [0 .. 255] Minutes
	RSBEGIN	d	Beginn des täglichen Zeitintervalls für die automatische Rückschaltung. Die Rückschaltung ist erlaubt in der Zeit zwischen RSBEGIN:RSOFFSET und RSENDE:RSOFFSET.
	SBBEGIN	e	Begin of the daily time interval for the automatic switch-back. Switch-back is allowed during the time between SBBEGIN:SBOFFEST and SBEND:SBOFFEST.
	RSENDE	d	Ende des täglichen Zeitintervalls für die automatische Rückschaltung. Ist RSENDE gleich RSBEGIN gesetzt, darf jederzeit automatisch rückgeschaltet werden.
	SBEND	e	End of the daily time interval for the automatic switch-back. If SBEND is set identically to SBBEGIN, automatic switch-back is allowed at any time.
	RSOFFSET	d	Offsetwert [in Minuten] zum täglichen Zeitintervall für die automatische Rückschaltung.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	RSOFFSET	e	Offset value [in minutes] to the daily time interval for the automatic switch-back.

11.2.4 Löschen einer Emergency Gruppe

Beim Löschen einer Emergency Gruppe wird automatisch auch die AP-Emergency Konfiguration der ihr zugeordneten Access Points/OpenScape 4000 SoftGates gelöscht. Soll die Konfiguration der Access Points/des OpenScape 4000 SoftGates erhalten bleiben, müssen diese vorher einer anderen Emergency Gruppe zugeordnet werden (`AENDERN-APESU:DATEN=AP,APNUM=xx,EGRPNUM=yy;`),

	**Configuration Management > Anlagendaten > IPDA > AP-Notfallgruppe** Auf **Suchen** klicken und CC-AP/Survivable OpenScape 4000 SoftGate auswählen, dann auf **Löschen** klicken.
	`LOESCHEN-APESU:EGRPNUM=99;`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

11.2.5 Einrichten von Access Points/OpenScape 4000 SoftGates für AP Emergency

Um einen Access Point/OpenScape 4000 SoftGate für das Leistungsmerkmal AP Emergency einzurichten, muss er einer bereits existierenden Emergency Gruppe zugewiesen werden. Der Großteil der AP Emergency spezifischen Konfiguration wird auf Ebene der Emergency Gruppe erledigt.

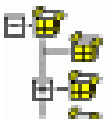
Access Points/OpenScape 4000 SoftGates mit Verbindungsart „Direct Link“ (APDL) - siehe „IP Distributed Architecture (IPDA)“, Abschnitt 2.2, „Access Point“- können ausschließlich Emergency Gruppen zugewiesen werden, deren CC-AP/Survivable OpenScape 4000 SoftGate in einem Access Point/ OpenScape 4000 SoftGate mit Verbindungsart **APDL** sitzt. Für Access Points/ OpenScape 4000 SoftGates mit Verbindungsart „Networked“ (**APNW**) gibt es keine Einschränkung bezüglich der Verbindungsart des Access Points/ OpenScape 4000 SoftGates, der den CC-AP/das Survivable OpenScape 4000 SoftGate enthält.

Für einen Access Point/OpenScape 4000 SoftGate ist festzulegen, zu welcher Emergency Gruppe dieser Access Point/OpenScape 4000 SoftGate gehört und was sein „Gewicht“ ist, d.h. sein Beitrag im Gewichtungsalgorithmus für die Umschaltung.

Zusätzlich kann für einen Access Point/OpenScape 4000 SoftGate festgelegt werden, dass er auch unabhängig von der Gewichtung in der Emergency Gruppe bei Verlust der Verbindung zur zentralen Steuerung sofort in die Steuerung durch den der Emergency Gruppe zugeordneten CC-AP/Survivable OpenScape 4000 SoftGate übernommen wird. Diese Ausnahme vom Gruppenverhalten kann sinnvoll sein, wenn zum Beispiel ein Access Point/ OpenScape 4000 SoftGate mit VIP-Teilnehmern so ausgerüstet ist, dass er einen eigenen Amtszugang hat und damit unabhängig von der Verfügbarkeit der restlichen Gruppenmitglieder ist.

Wichtig: Access Points/OpenScape 4000 SoftGates, die unabhängig von der Gruppe zum CC-AP/Survivable OpenScape 4000 SoftGate umgeschaltet werden und keinen eigenen Amts-/ Quer-Verbindungen besitzen, erlauben nur noch die Access Point/OpenScape 4000 SoftGate interne Kommunikation. **Damit wird verhindert, dass z.B. Notrufe über Amt abgesetzt werden können.**

Diese Ausnahme gilt nur für den Fall, dass der Grenzwert für die Gewichtung innerhalb der Emergency Gruppe noch nicht erreicht ist. Der Gewichtungsbeitrag eines Access Points/OpenScape 4000 SoftGates mit Einzelumschaltung wird in der Gewichtung für das Gruppenverhalten immer mit berücksichtigt. Der Access Point/das OpenScape 4000 SoftGate wird immer mit umgeschaltet, wenn die Gewichtung dies für die Emergency Gruppe fordert. Auch die Rückschaltung erfolgt im Rahmen der Gruppe.

	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken und Access Point/OpenScape 4000 SoftGate auswählen. Auf der Registerkarte **AP-Notfall** die Konfigurationsparameter einstellen und auf **Sichern** klicken.

	`EINRICHTEN-APESU:DATEN=AP,APNUM=99,EGRPNUM=2,GEWICHT=70,UMSCHALT=GRUPPE;`
	oder
	`AENDERN-APESU:DATEN=AP,APNUM=99,EGRPNUM=2,GEWICHT=70,UMSCHALT=GRUPPE;`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

Tabelle 70: Parameter AMO APESU im EINRICHTEN- oder AENDERN-Zweig, DATEN=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APESU	APNUM	d	LTU-Nummer des Access Points/OpenScape 4000 SoftGates
	APNO	e	Line/Trunk Unit Number of the access point/ OpenScape 4000 SoftGate
	EGRPNUM	d	Identifikations-Nummer der Emergency Gruppe.
	EGRPNO	e	Identification number of the Emergency Group.
	GEWICHT	d	Gewichtsbeitrag des Access Points/ OpenScape 4000 SoftGates für den Gewichtungsalgorithmus. Verliert der Access Point/OpenScape 4000 SoftGate die Verbindung zur zentralen Steuerung, so wird sein Gewichtsbeitrag in die Gewichtung der Emergency Gruppe eingebracht. Wertebereich [0 .. 1000]
	WEIGHT	e	Weight share of the access point/ OpenScape 4000 SoftGate to the weighing alogrithm. When the access point/OpenScape 4000 SoftGate loses the connection with the central control, itâs weight share is brought into the weighing of the Emergency Group. Range [0 .. 1000]
	UMSCHALT	d	Umschaltemodus Bestimmt, ob ein Access Point/OpenScape 4000 SoftGate ausschließlich zusammen mit der gesamten Emergency Gruppe umgeschaltet wird, oder ob er auch unabhängig von der Gewichtung sofort vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wird, wenn er die Verbindung zur zentralen Steuerung verloren hat. Werte: GRUPPE: Umschaltung nur mit gesamter Gruppe EINZEL: Einzelbehandlung bei der Umschaltung

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SWMODE	e	Switch-Over Mode Specifies if the access point/OpenScape 4000 SoftGate may be switched over only together with the complete Emergency Group, or if it may be taken over by the CC-AP/Survivable OpenScape 4000 SoftGate independently to the weighing, as soon as it loses connection with central control. Values: GROUP: Switch-Over only together with Group SINGLE: Individual handling at Switch-Over

11.2.6 Beispiele für die Dimensionierung der Gewichtung

Das Wechselspiel aus der Gewichtung der Access Points/OpenScape 4000 SoftGates, der Schwelle für die Umschaltung der Gruppe und gegebenenfalls der Ausnahme aus der Gruppenregel mittels Einzelumschaltung stellen ein sehr mächtiges Instrument zur Konfiguration der automatischen Umschaltung in den Emergency Betrieb dar. Zwei Beispiele sollen die Orientierung in diesem Zahlenspiel erleichtern.

- Reine IP-Anlage (keine Shelves 1-15), Communication Server steht im Rechenzentrum, 30 Access Points/OpenScape 4000 SoftGates, 1 CC-AP/ Survivable OpenScape 4000 SoftGate im Reserve-Rechenzentrum, mehrere Amtszugänge mit gleicher Kennzahl auf vier Access Points/OpenScape 4000 SoftGates verteilt.
- Konfigurationsvorschlag 1 (Emergency Betrieb ausschließlich bei Ausfall des Communication Servers, d.h. **alle** Access Points/OpenScape 4000 SoftGates haben die Verbindung dorthin verloren)
  - 1 Emergency Gruppe, Schwelle = 300
  - Alle 30 Access Points/OpenScape 4000 SoftGates bekommen Gewicht = 10

  Nachteil: Ist auch nur ein Access Point/OpenScape 4000 SoftGate außer Betrieb - z.B. durch Stromausfall, so kann dieser nicht in die Bewertung eingehen, da er keinen Kontakt zum CC-AP/Survivable OpenScape 4000 SoftGate hat. In diesem Fall kann die Schwelle **nicht** erreicht werden.

  Konfigurationsvorschlag 2 (Hat mehr als die Hälfte der Access Points/ OpenScape 4000 SoftGates die Verbindung mit dem Communication Server verloren, soll der Emergency Betrieb beginnen. Das soll auch für die Hälfte der Amtszugänge gelten).
  - 1 Emergency Gruppe, Schwelle = 150
  - Access Points/OpenScape 4000 SoftGates ohne Amtsanschluss: Gewicht = 10
  - Access Points/OpenScape 4000 SoftGates mit Amtsanschluss: Gewicht = 75

- Klassische Anlage am Hauptstandort, Nebenstandort 1 mit 3 Access Points/ OpenScape 4000 SoftGates, einer davon hat Amtszugang; Nebenstandort 2 mit 6 Access Points/OpenScape 4000 SoftGates, zwei davon haben Amtszugang; Nebenstandort 3 mit 1 Access Point/OpenScape 4000 SoftGate, dieser hat auch Amtszugang; Nebenstandort 4 hat 4 Access Points/OpenScape 4000 SoftGates, einer davon hat den allgemeinen Amtszugang, einer enthält die Anschlüsse der Geschäftsleitung mit eigenem Amtszugang. Für die Nebenstandorte ist die Erreichbarkeit über die lokalen Amtszugänge sehr wichtig. Der „Ausfall“ eines einzelnen Access Points/OpenScape 4000 SoftGates ohne Amtszugang soll noch nicht zur Umschaltuder Gruppe führen. Sind aber zwei oder mehr Access Points/ OpenScape 4000 SoftGates betroffen, so ist in jedem Fall umzuschalten. Jeder Standort hat einen Access Point/ein OpenScape 4000 SoftGate mit CC-AP/Survivable OpenScape 4000 SoftGate ausgestattet.
- Konfigurationsvorschlag Nebenstandort 1 (3 Access Points/OpenScape 4000 SoftGates)
  - 1 Emergency Gruppe, Schwelle = 200
  - Access Points/OpenScape 4000 SoftGates ohne Amtsanschluss: Gewicht = 100
  - Access Point/OpenScape 4000 SoftGate mit Amtsanschluss: Gewicht = 200

  Nebenstandort 2 (6 Access Points/OpenScape 4000 SoftGates)
  - 1 Emergency Gruppe, Schwelle = 200
  - Access Points/OpenScape 4000 SoftGates ohne Amtsanschluss: Gewicht = 100
  - Access Points/OpenScape 4000 SoftGates mit Amtsanschluss: Gewicht = 100

  Nebenstandort 3
  - 1 Emergency Gruppe, Schwelle = 100
  - Access Points/OpenScape 4000 SoftGates: Gewicht = 100

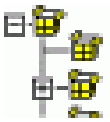
  Nebenstandort 4
  - 1 Emergency Gruppe, Schwelle = 200
  - Access Points/OpenScape 4000 SoftGates ohne Amtsanschluss: Gewicht = 100
  - Access Point/OpenScape 4000 SoftGate mit Amtsanschluss: Gewicht = 200
  - Access Point/OpenScape 4000 SoftGate der Geschäftsleitung: Gewicht = 100, Einzelumschaltung aktiv Der CC-AP/das Survivable OpenScape 4000 SoftGate sollte in diesem Access Point/OpenScape 4000 SoftGate eingebaut sein.

11.2.7 Access Points/OpenScape 4000 SoftGates aus AP Emergency Konfiguration entfernen

Ein Access Point/OpenScape 4000 SoftGate kann jederzeit aus der AP Emergency Konfiguration entfernt werden.

Wichtig: Wird ein Access Point/OpenScape 4000 SoftGate aus der AP Emergency Konfiguration gelöscht, entfällt auch

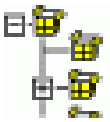
sein möglicher Gewichtsbeitrag im Gewichtungsalgorithmus der Emergency Gruppe, welcher er angehört hat. Prüfen Sie, ob der Grenzwert „SCHWELLE“ der Emergency Gruppe noch auf einem sinnvollen Wert steht.

	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken und Access Point/OpenScape 4000 SoftGate auswählen. Auf der Registerkarte **AP-Notfall** die **Nummer der Notfallgruppe** löschen und auf **Sichern** klicken .
	`LOESCHEN-APESU:APNUM=99;`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

11.2.8 Löschen der gesamten AP Emergency Konfiguration

Soll die gesamte AP Emergency Konfiguration eines OpenScape 4000 Systems gelöscht werden, so geht das recht einfach auf Systemebene. Alle CC-APs, alle Emergency Gruppen und die AP Emergency Konfiguration aller Access Points/ OpenScape 4000 SoftGates wird komplett entfernt.

	**Configuration Management > Anlagendaten > IPDA > IPDA - CC-Access Point** Auf **Suchen** klicken und die Ansicht **Objektliste** auswählen. Alle CC-AP/Survivable OpenScape 4000 SoftGate-Objekte auswählen und auf **Löschen** klicken.
	`LOESCHEN-APESU;`

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

11.2.9 Einrichten der Display-Anzeige für AP Emergency am Endgerät

Wird ein Access Point/OpenScape 4000 SoftGate aktiv von einer Survivability Unit, d.h. einem CC-AP/Survivable OpenScape 4000 SoftGate gesteuert, ergeben sich für den Anwender Veränderungen, über welche er informiert werden soll.

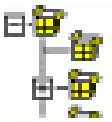
Diese Information wird auf dem Ruhe-Display der angeschlossenden Endgeräte in der zweiten Zeile ausgegeben. **Der auszugebende Text muss mit dem Kunden abgestimmt werden.**

Der ausgegebene Text ersetzt die LOGO-Information, die im Normalbetrieb ausgegeben werden kann.

Der Text hat maximal 22 Stellen, welche mit Zahlen und Buchstaben in Groß- und Kleinschreibung besetzt werden können.

Wichtig: Bitte besetzen Sie alle Positionen der zweiten Display-Zeile, auf denen im Ruhe-Display Informationen ausgegeben werden, mit Leerzeichen und lassen Sie genügend Platz, damit die Informationen lesbar sind. Wird z.B. auf den ersten 5 Stellen des Ruhe-Displays die Rufnummer des Telefons angezeigt, müssen Sie den AP Emergency Hinweistext mit mindestens 6 Leerzeichen beginnen.

Dies Einstellung erfolgt mit dem AMO ZANDE.

	Die Einstellung mit dem AMO ZANDE kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Open** ...<IP> mittels AMO (siehe AMO Kommando)
	`AENDERN-ZANDE:TYP=DATENALL,APEDTXT=„ Notbetrieb“;` Der Text sollte genau 22 Zeichen lang sein.

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

11.2.10 Festlegen der Umschalteverzögerung

Ist ein Ausfall des OpenScape 4000 Host System oder des IP Netzwerks erkannt und hat ein CC-AP anhand seiner konfigurierten Regeln entschieden, dass Access Points/OpenScape 4000 SoftGates umgeschaltet werden sollen, gibt es noch einen Punkt zu beachten:

Wie soll das Gesamtsystem reagieren, falls das OpenScape 4000 Host System einen RELOAD durchführt?

Hier gibt es zwei Möglichkeiten:

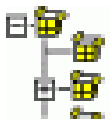
1) So schnell wie möglich reagieren, d.h. sofort umschalten. Im Fall eines RELOAD wird dann **immer** in den Emergency-Betrieb umgeschaltet.

2) Die Umschaltung so lange verzögern, dass ein RELOAD **nicht** zum Emergency-Betrieb führt.

Entsprechend dieser Entscheidung muss die AP Emergency Umschalteverzögerung entweder

1) auf Null (sofortiges umschalten) oder

2) • auf die Zeitdauer, welche das OpenScape 4000 System für die komplette Ausführung eines RELOAD benötigt, eingestellt werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf den Registerkarten **Anlagendaten** unter **Zeitverhalten (TIMING)** die Umschalteverzögerung für AP Emergency eingeben und auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=TIMING,APESWDLY=5;` Stellt die Umschalteverzögerung auf 5 Minuten -> d.h. der RELOAD der Anlage dauert 5 Minuten und soll abgewartet werden.

Die geänderten Daten werden erst wirksam, nachdem die Datenbasis mittels OpenScape 4000 Assistant Backup & Restore auf den CC-AP/das Survivable OpenScape 4000 SoftGate gebracht und vom CC-AP/Survivable OpenScape 4000 SoftGate übernommen wurde.

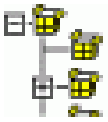
Tabelle 71: Parameter APESWDLY des AMO SIPCO im AENDERN-Zweig, TYP=TIMING

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
SIPCO	APESWDLY	d	APE Umschalteverzögerung Das Umschalten eines Access Points/ OpenScape 4000 SoftGates in den Emergency Mode kann um eine konfigurierbare Zeit verzögert werden. Der Wert wird in Minuten angegeben. Wertebereich [0 .. 99]. „0“ sollte nicht konfiguriert werden, weil damit würde der APE auch im Falle eines RMX Restarts des Hostsystems (CCA/CCB) übernehmen. Konfigurationsempfehlung und AMO Defaultwert: 5 (Minuten)

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	APESWDLY	e	APE Switch Over Delay The switch-over of an Access Point/ OpenScape 4000 SoftGate to Emergency Mode can be delayed for a configurable amount of time. The value is entered in minutes. Range [0 .. 99]. „0“ should not be configured because then a switch over to the APE is performed even in case of a restart of the RMX of the host system (CCA/CCB). Recommendation configuration and AMO default: 5 (minutes)

11.2.11 Abfragen der Verbindungsdaten

11.2.11.1 Abfragen der Verbindungsdaten über Configuration Management



Configuration Management > Anlagendaten > Wartung

> IPDA - CC-Access- Point-Wartung

Auf SUCHEN klicken und CC-AP/Survivable OpenScape 4000 SoftGate auswählen.

Die daraufhin erzeugte Tabelle zeigt die Verbindungszustände aller Access Points/OpenScape 4000 SoftGates welche zu Emergency Gruppen der ausgewählten CC-APs/Survivable OpenScape 4000 SoftGates gehören...

11.2.11.2 Abfragen der Verbindungsdaten über AMO



Die Abfrage der Konfiguration von AP-Emergency schließt auch die Ausgabe der aktuellen Verbindungszustände ein. Menge und Inhalt der ausgegebenen Daten hängt davon ab, auf welcher logischen Ebene die Abfrage läuft - und ob sie im OpenScape 4000 Host System oder auf einem CC-AP/Survivable OpenScape 4000 SoftGate durchgeführt wird.

ABFRAGEN-APESU;

1) an OpenScape 4000 Host System

2) **a)** alle CC-APs

b)
- alle Emergency Gruppen
- alle Access Points/OpenScape 4000 SoftGates

- lokal an einem CC-AP/Survivable OpenScape 4000 SoftGate
- – lokaler CC-AP/Survivable OpenScape 4000 SoftGate
  – alle Emergency Gruppen des CC-AP/Survivable OpenScape 4000 SoftGate
  – alle Access Points/OpenScape 4000 SoftGates der Emergency Gruppen des CC-AP/Survivable OpenScape 4000 SoftGate

  ABFRAGEN-APESU:CCAPNUM=xx; **bzw.** ABFRAGEN-APESU:xx;
- an OpenScape 4000 Host System
- – ausgewählter CC-AP/Survivable OpenScape 4000 SoftGate
  – alle Emergency Gruppen des ausgewählten CC-AP/Survivable OpenScape 4000 SoftGate
  – alle Access Points/OpenScape 4000 SoftGates der Emergency Gruppen des ausgewählten CC-AP/Survivable OpenScape 4000 SoftGate
- lokal an einem CC-AP/Survivable OpenScape 4000 SoftGate

falls der lokale CC-AP/Survivable OpenScape 4000 SoftGate ausgewählt ist

a) lokaler CC-AP/Survivable OpenScape 4000 SoftGate

b)
- alle Emergency Gruppen des CC-AP/Survivable OpenScape 4000 SoftGate
- alle Access Points/OpenScape 4000 SoftGates der Emergency Gruppen des CC-AP/Survivable OpenScape 4000 SoftGate

falls nicht der lokale CC-AP/Survivable OpenScape 4000 SoftGate ausgewählt ist: Hinweismeldung

ABFRAGEN-APESU:EGRPNUM=xx; **bzw.** ABFRAGEN-APESU:,xx;

- OpenScape 4000 Host System
- – ausgewählte Emergency Gruppe
  – alle Access Points/OpenScape 4000 SoftGates der ausgewählten Emergency Gruppe
- lokal an einem CC-AP/Survivable OpenScape 4000 SoftGate

falls eine Emergency Gruppe des lokalen CC-AP/Survivable OpenScape 4000 SoftGate ausgewählt ist

a) ausgewählte Emergency Gruppe

b)
- alle Access Points/OpenScape 4000 SoftGates der ausgewählten Emergency Gruppe

sonst: Hinweismeldung

ABFRAGEN-APESU:APNUM=xx; **bzw.** ABFRAGEN-APESU:,,xx;

- OpenScape 4000 Host System
- – ausgewählter Access Point/ausgewähltes OpenScape 4000 SoftGate
- lokal an einem CC-AP/Survivable OpenScape 4000 SoftGate

falls ein Access Point/OpenScape 4000 SoftGate einer Emergency Gruppe des lokalen CC-AP/Survivable OpenScape 4000 SoftGate ausgewählt ist

a) ausgewählter Access Point/ausgewähltes OpenScape 4000 SoftGate

sonst: Hinweismeldung

CC-AP/Survivable OpenScape 4000 SoftGate spezifischer Block:

```
+-------------------------------------------------------------------
+
| CC-AP: 99 IP ADRESSE: 192.168.23 .199 |
| GESCHWINDIGKEIT/ARBEITSMODUS(IPDA): 100MBFD |
+-------------------------------------------------------------------
+
```

Emergency Group spezifischer Block:

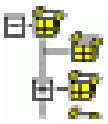
```
+-------------------------------------------------------------------
+
| AP EMERGENCY GRUPPE: 2 CC-AP: 99 NAME: BERLIN |
| SCHWELLE: 100 RSMODE: AUTO |
| STABIL: 10 MIN RSBEGIN: 20 H RSENDE: 6 H RSOFFSET: 13 MIN
 |
+-------------------------------------------------------------------
+
```

Access Point/OpenScape 4000 SoftGate spezifischer Block:

```
+-------------------------------------------------------------------
+
| AP: 99 AP EMERGENCY GRUPPE: 2 CC-AP: 99 GEWICHT: 70
 UMSCHALT: GRUPPE |
| KONTROLL-EINHEIT: HOST-CC SIGNAL-PFAD: LAN |
| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG: |
| |
| HOST-CC: VERBUNDEN: JA VERBUNDEN SEIT: 08-06-2004 18:20 |
| CC-AP: VERBUNDEN: JA VERBUNDEN SEIT: 18-06-2004 23:01 |
+-------------------------------------------------------------------
---------------+
```

11.2.12 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates

11.2.12.1 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates über Configuration Management



Configuration Management > Anlagendaten > Wartung > IPDA - CC-Access Point-Wartung

Auf **Suchen** klicken und CC-AP/Survivable OpenScape 4000 SoftGate auswählen.

Im Hauptmenü die Menüpunkte -> **Aktion** -> **Ausführen** auswählen.

In der daraufhin erzeugten Maske kann eingestellt werden

- ob in den Normal-, oder Notfall-Modus gewechselt werden soll,
- ob ein bestimmter Access Point/bestimmtes OpenScape 4000 SoftGate, alle Access Points/OpenScape 4000 SoftGates einer bestimmten Emergency Gruppe, alle Access Points/ OpenScape 4000 SoftGates aller Emergency Gruppen des ausgewählten CC-AP/Survivable OpenScape 4000 SoftGate, oder das gesamte System umgeschaltet werden soll.

11.2.12.2 Administrative Umschaltung von Access Points/OpenScape 4000 SoftGates über AMO

Die administrative Umschaltung von Access Points/OpenScape 4000 SoftGates von der zentralen Steuerung zum CC-AP/Survivable OpenScape 4000 SoftGate oder umgekehrt ist jederzeit möglich.

Der Auftrag wird an das OpenScape 4000 Host System per AMO abgesetzt. Von dort wird er über einen betroffenen Access Point/betroffenes OpenScape 4000 SoftGate zu dem betroffenen CC-AP/Survivable OpenScape 4000 SoftGate gesendet. Letztlich weist der CC-AP/Survivable OpenScape 4000 SoftGate die HG 3575 der betroffenen Access Points/OpenScape 4000 SoftGates an, durchzustarten und mit der gewünschten Steuerung (zentrale Steuerung (Host) oder CC-AP/Survivable OpenScape 4000 SoftGate) hochzufahren. Ist mehr als ein CC-AP/Survivable OpenScape 4000 SoftGate betroffen, wird dieser Vorgang für jeden CC-AP/Survivable OpenScape 4000 SoftGate durchgeführt.

Die Kommunikation vom OpenScape 4000 Host System über Access Point/ OpenScape 4000 SoftGate zu CC-AP/Survivable OpenScape 4000 SoftGate setzt voraus, dass mindestens ein Access Point/OpenScape 4000 SoftGate sowohl eine Verbindung zur zentralen Steuerung, als auch zum CC-AP/ Survivable OpenScape 4000 SoftGate hat. Ist dies nicht der Fall, kann keine Umschaltung eingeleitet werden.

Die Umschaltung kann auf unterschiedlichen Ebenen erfolgen:

- alle Access Points/OpenScape 4000 SoftGates aller Emergency Gruppen aller CC-APs im System
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=SYSTEM;` schaltet zum CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=SYSTEM;` schaltet zur zentralen Steuerung

- alle Access Points/OpenScape 4000 SoftGates aller Emergency Gruppen eines CC-AP/Survivable OpenScape 4000 SoftGate
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=CCAP,NUMMER=99;` schaltet zum CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=CCAP,NUMMER=99;` schaltet zur zentralen Steuerung
- alle Access Points/OpenScape 4000 SoftGates einer Emergency Gruppe (eines CC-AP/Survivable OpenScape 4000 SoftGate)
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=APEGRP,NUMMER=2;` schaltet zum CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=APEGRP,NUMMER=2;` schaltet zur zentralen Steuerung
- ein Access Point/OpenScape 4000 SoftGate (einer Emergency Gruppe (eines CC-AP/Survivable OpenScape 4000 SoftGate))
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=AP,NUMMER=99;` schaltet zum CC-AP/Survivable OpenScape 4000 SoftGate `EXEC-APESU:SYSMODE=NORMAL,LEVEL=AP,NUMMER=99;` schaltet zur zentralen Steuerung

---

Wichtig: Die Umschaltung wird unabhängig von Gruppenregeln immer für alle ausgewählten Access Points/ OpenScape 4000 SoftGates durchgeführt, welche Kontakt zu der gewünschten Steuerung haben. Haben einige Access Points/OpenScape 4000 SoftGates innerhalb einer Auswahl (SYSTEM, CC-AP/Survivable OpenScape 4000 SoftGate, APEGRP) keinen Kontakt zur gewünschten Steuerung, so werden diese **nicht** umgeschaltet. Der AMO meldet dann „teilweise durchgeführt“. Die teilweise Umschaltung kann dazu führen, dass betriebswichtige Ressourcen (z.B. Amtsanschlüsse) für eine Gruppe nicht zur Verfügung stehen! Vor einer manuellen Umschaltung **muss** daher der Verbindungsstatus abgefragt und überprüft werden. Siehe Abschnitt 2.11, „Abfragen der Verbindungsdaten“.

Wichtig: Access Points/OpenScape 4000 SoftGates, die unabhängig von der Gruppe umschaltet werden und keinen eigenen Amts-/Quer-Verbindungen besitzen, erlauben nur noch die Access Point-/OpenScape 4000 SoftGate-interne Kommunikation. **Damit wird verhindert, dass z.B. Notrufe über Amt abgesetzt werden können.**

Tabelle 72: Parameter des AMO APESU im EXEC-Zweig

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APESU	SYSMODE	d	Gibt an, welche Steuerung übernehmen soll. Werte: NORMAL: zentrale Steuerung (Host) EMERG: Emergency Steuerung (CC-AP/ Survivable OpenScape 4000 SoftGate)

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SYSMODE	e	Identifies, which control shall take over. Values: NORMAL: Central Control (Host) EMERG: Emergency Control (CC-AP/ Survivable OpenScape 4000 SoftGate)
	LEVEL	d	Gibt an, auf welcher System-Ebene umgeschaltet werden soll. Werte: SYSTEM: gesamtes System (alle Access Points/OpenScape 4000 SoftGates, APEGRPs, CC-APs) CCAP: ein CC-AP/Survivable OpenScape 4000 SoftGate (alle Access Points/ OpenScape 4000 SoftGates, APEGRPs) APEGRP: eine Emergency Gruppe (alle Access Points/OpenScape 4000 SoftGates) AP: ein Access Point/OpenScape 4000 SoftGate
	LEVEL	e	Identifies on which system level the switch over shall be executed. Values: SYSTEM: complete system (all access points/OpenScape 4000 SoftGates, APEGRPs, CC-APs) CCAP: one CC-AP/Survivable OpenScape 4000 SoftGate (all access points/ OpenScape 4000 SoftGates, APEGRPs) APEGRP: one Emergency Group (all access points/OpenScape 4000 SoftGates) AP: one access point/OpenScape 4000 SoftGate
	NUMMER	d	Gibt die Nummer des betroffenen CC-AP/ Survivable OpenScape 4000 SoftGate, der Emergency Gruppe oder des Access Point/ OpenScape 4000 SoftGate an.
	NO	e	Identifies the number of the affected CC-AP/Survivable OpenScape 4000 SoftGate, Emergency Group or access point/OpenScape 4000 SoftGate

11.2.13 Zeitsynchronisation zwischen Host System und CC-AP/Survivable OpenScape 4000 SoftGate

Für viele Funktionen der OpenScape 4000 ist eine exakte Uhrzeit erforderlich (Gebührenerfassung, uhrzeitabhängige Wege, Nachtschaltung, etc.). Alle Uhren im System (bis zu 84) müssen synchron laufen.

Es gibt zwei Möglichkeiten, die Zeitsynchronisation durchzuführen:

1) Im IP-Netzwerk steht ein Zeitserver zur Verfügung, der die Zeitsynchronisation aller OpenScape 4000-Prozessoren (Zentralrechner und alle Survivability-Einheiten) über das Network Time Protocol unterstützt.
2) Im IP-Netz steht **kein** Zeit-Server zur Verfügung. Die OpenScape 4000 Plattform stellt dann ihre lokale Uhrzeit zur Synchronisation aller Survivability Units über das Netzwerk zur Verfügung.

Mehr Informationen zur Einstellung von Datum und Zeit und zum Thema „Zeitsynchronisation“ finden Sie im Abschnitt 1.11, „Zeitsynchronisation“.

11.2.14 Erstinbetriebnahme des CC-AP/Survivable OpenScape 4000 SoftGate

11.2.14.1 Vorbereitung

Bei der Erstinbetriebnahme muss sichergestellt werden, dass die Festplatte des CC-AP/Survivable OpenScape 4000 SoftGate mit der gleichen APS-Version läuft, wie sie aktuell im Host System läuft.



AB-APS;

Diese Abfrage an der OpenScape 4000 Host System gibt die Sachnummern der geladenen Programmsysteme aus. Interessant ist dabei die Sachnummer des **Y0**-APS.

PROGRAMMSYSTEM	:Y0-EN0YC
VERSIONSNUMMER	:10
KORREKTURVERSIONSNUMMER	: 001
SACHNUMMER	: **P30252x**xxxxxxxxxx
PROGRAMMSYSTEM MIT CODESUBSYSTEMEN	
SCHNITTSTELLENVERSION:	
PROGRAMMSYSTEM ENTHAELT KEINE SCHNITTSTELLENVERSION	

11.2.14.2 CC-AP

Siehe entsprechendes „How To“ in der Release Note zu OpenScape 4000.

11.2.14.3 Survivable OpenScape 4000 SoftGate

Siehe entsprechendes „How To“ in der Release Note zu OpenScape 4000.

11.2.15 Verifizieren / Abnahme der AP-Emergency Konfiguration

Der Kunde nutzt die AP Emergency-Funktion, um in Notsituationen, in denen die zentrale Steuerung und/oder wesentliche Komponenten der IP-Infrastruktur nicht zur Verfügung stehen, Telefonate zu ermöglichen.

Diese Notfallsituation wird in der Regel sehr selten eintreten. Daher ist es um so wichtiger, dass die Notfallmassnahmen dann, wenn sie tatsächlich einmal gebraucht werden, auch wie beabsichtigt funktionieren.

Es ist zwingend erforderlich, dass die Funktionalität der AP-Emergency Konfiguration nach der Erstinbetriebnahme, bzw. nach wesentlichen Modifikationen durch einen Abnahme/Übergabetest verifiziert wird.

Dazu muss jede Emergency Gruppe einmal administrativ zum CC-AP/ Survivable OpenScape 4000 SoftGate umgeschaltet werden. Im Emergency-Betrieb muss dann geprüft werden, ob Notrufe, die Kommunikation ins Amt, zu anderen Anlagen im Netz und auch die Kommunikation zwischen Emergency Gruppen an unterschiedlichen CC-APs wie geplant funktioniert. Beziehen Sie gegebenenfalls auch installierte Applikationen, die den Emergency-Betrieb unterstützen, mit in den Test ein.

Prüfen Sie auch die Kommunikationsfähigkeit von Access Points/OpenScape 4000 SoftGates, die unabhängig von der Emergency Gruppe zum CC-AP/ Survivable OpenScape 4000 SoftGate geschaltet werden können, wenn die Gruppe im Normalbetrieb läuft.

Die Tests können in betriebsschwachen Zeiten durchgeführt werden.

11.3 Backup & Restore

11.3.1 Konfiguration von OpenScape 4000 Assistant Backup & Restore im OpenScape 4000 Host System

Um die Backup- und Restore-Prozesse für das Leistungsmerkmal AP-Emergency zu unterstützen, repliziert die Applikation OpenScape 4000 Assistant Backup & Restore die Software sowie die Konfigurationsdaten vom Zentralsystem zu den CC-APs/Survivable OpenScape 4000 SoftGates.

Es muss zwischen zwischen HOST und APE unterschieden werden.

- HOST
- OpenScape 4000 Platform mit den virtuellen Maschinen ADP/CCA, OpenScape 4000 Assistant und OpenScape 4000 CSTA.
- APE

- OpenScape 4000 Platform mit den virtuellen Maschinen CCAP, OpenScape 4000 Assistant und OpenScape 4000 CSTA.

  Daher gibt es vier Systeme, die synchronisiert werden müssen. Im Moment ist aber nur die Synchronisation von CC-AP auf dem APE und ADP/CCA auf dem Host System möglich. Diese Funktionalität wird durch OpenScape 4000 Assistant Backup & Restore gewährleistet.

  Wichtig: Mehr Informationen zum Backup & Restore finden Sie in der Online-Hilfe.

Zeitliche Rahmenbedingungen

Ein Backup kann nur durchgeführt werden, wenn der AP Backup-Server frei, d.h. nicht gerade von Restore-Prozessen belegt ist. Die Zahl der gleichzeitig erlaubten Restore-Prozesse kann eingestellt werden, um die Server bzw. Netzwerklast zu begrenzen.

Die Zeit zwischen zwei Backup-Terminen muss also ausreichen, um den Backup durchzuführen und die Restore-Abläufe aller CC-AP/Survivable OpenScape 4000 SoftGate im System auszuführen.

Ist die Anzahl der CC-APs größer als die Zahl der gleichzeitig unterstützten Restore-Operationen, so müssen einige CC-APs mit dem Restore warten, bis Kapazität am AP Backup-Server frei ist. Das führt dann zu einer Vervielfachung der benötigten Restore-Zeit, die im Gesamt-Ablauf berücksichtigt werden muss.

Der Zeitbedarf wird bestimmt durch das zu transportierende Datenvolumen und die verfügbare Übertragungsbandbreite. Das maximale Datenvolumen (im Falle einer System Maintenance Release) wird mit 100 MByte angesetzt. Die durchschnittliche Größe wird unter 10% des Maximums liegen.

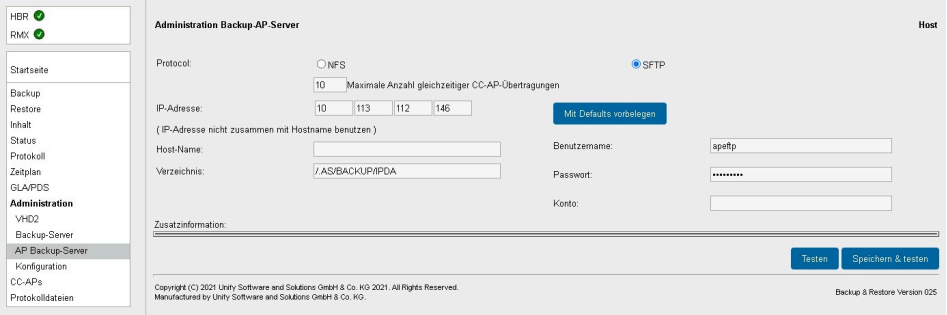
Wird für den Restore-Prozess am CC-AP/Survivable OpenScape 4000 SoftGate sehr viel Zeit benötigt (niedrige verfügbare Übertragungsbandbreite), so muss dafür gesorgt werden, dass der Restore aller CC-APs gleichzeitig stattfinden kann.

Der Startzeitpunkt für den Backup bestimmt indirekt auch den Inhalt der Datenbasis. Ist es z.B. beim Kunden üblich, vor Verlassen des Büros am Telefon die feste Anrufumleitung zu aktivieren und wird der Backup außerhalb der Bürozeiten durchgeführt, so enthält die gesicherte Datenbasis die aktivierten Anrufumleitungen. Tritt nun während des Tages ein Problem auf, welches den Emergency Betrieb einleitet, so startet der Emergency Betrieb mit den gesicherten Anrufumleitungen.

11.3.1.1 Einrichten eines AP Backup-Servers mit OpenScape 4000 Assistant Backup & Restore

Im ersten Konfigurationsschritt wird festgelegt, wo die Daten des OpenScape 4000 Backup abgelegt werden sollen. Hierzu muss der Rechner angegeben werden, der als File-Server (AP Backup-Server) agieren soll, das Verzeichnis, wo die Daten abgelegt werden sollen, sowie die Login-Daten für den Zugang. Die Einrichtung auf dem File-Server (Verzeichnis anlegen, Kennung einrichten) sollte vor der Konfiguration im OpenScape 4000 Assistant Backup & Restore erfolgen.

- Über Web-Browser die Startseite des OpenScape 4000 Assistant anzeigen und mit der Â«rstaÂ»-Kennung einloggen.
- In der linken Menüleiste den Funktionsbereich **Software Management** auswählen.
- Als Unterpunkt des **Software Management** die Applikation **Backup & Restore** auswählen.
- In der Bedienoberfläche von Backup & Restore die Funktion **Administration AP Backup-Server** auswählen.



Backup & Restore: Einrichten eines AP Backup-Servers

Die folgenden Felder müssen nun ausgefüllt werden:

- Auswahl des **Protokolls** (**SFTP** oder **NFS**) - typisch: **SFTP**

Für den Fall, dass der AP Backup-Server auf dem OpenScape 4000 Zentralsystem eingerichtet werden soll, muss **SFTP** als Protokoll ausgewählt werden.

- **Maximale Anzahl gleichzeitiger CC-AP/Survivable OpenScape 4000 SoftGate Transfers**

Im Maximalausbau können sich 83 CC-APs gleichzeitig am AP Backup-Server anmelden und das aktuelle Backup-Set herunterladen wollen. Unterstützt der Server diese hohe Zahl gleichzeitig angemeldeter System nicht, oder sollen mögliche Lastspitzen am Server verringert werden, so kann die maximale Anzahl gleichzeitig angemeldeter CC-APs entsprechend eingestellt werden. Die Abhängigkeiten sind im Abschnitt 3.1, „Zeitliche Rahmenbedingungen“ dargestellt.

- Eingabe der **IP- Adresse** oder des **Host-Namens** des AP Backup-Servers

Die Eingabe des Host-Namens ist nur möglich, wenn dieser entweder direkt in UBA konfiguriert ist oder Namensauflösung mit DNS eingerichtet ist.

- Eingabe des **Verzeichnisses** auf dem AP Backup-Server, welches für Backup & Restore verwendet werden soll.

Für den Fall, dass der AP Backup-Server auf dem OpenScape 4000 Zentralsystem eingerichtet werden soll, muss das hierfür vorgeleistete Verzeichnis „`/.AS/BACKUP/IPDA`“ gewählt werden.

Das Verzeichnis muss etwa 100 MByte an Daten aufnehmen können.

- Wurde **SFTP** als Protokoll gewählt, so muss noch der Login-Name für die **Anmeldung** und das **Passwort** für den Zugriff auf den AP Backup-Server (SFTP-Server) eingerichtet werden. Falls der SFTP-Server einen **Account** benötigt, ist dieser ebenfalls einzugeben.

Für den Fall, dass der AP Backup-Server auf dem OpenScape 4000 Zentralsystem eingerichtet werden soll, sollte aus Sicherheitsgründen die

Anmeldung unter `apeftp` eingerichtet werden. Ein Account wird in diesem Fall nicht eingerichtet.

Wichtig: Bitte beachten Sie, dass das Passwort für die Anmeldung am AP Backup-Server auf dem Backup-Server sowie in der OpenScape 4000 Assistant Backup & Restore-Konfiguration des OpenScape 4000 Zentralsystems und aller CC-APs gepflegt werden muss!

Die Einrichtung des Backup der Konfigurationsdaten wird abgeschlossen durch

- **Speichern & testen** - Sichern der Konfiguration und Test des Zugriffs auf den AP Backup-Server.

  Diese Option sollte immer verwendet werden, wenn der File-Server zum Zeitpunkt der Einrichtung im Netz bereits verfügbar ist.
- **Testen** der Konfiguration ohne Sicherung.

  Diese Option ist für Diagnosezwecke gedacht.

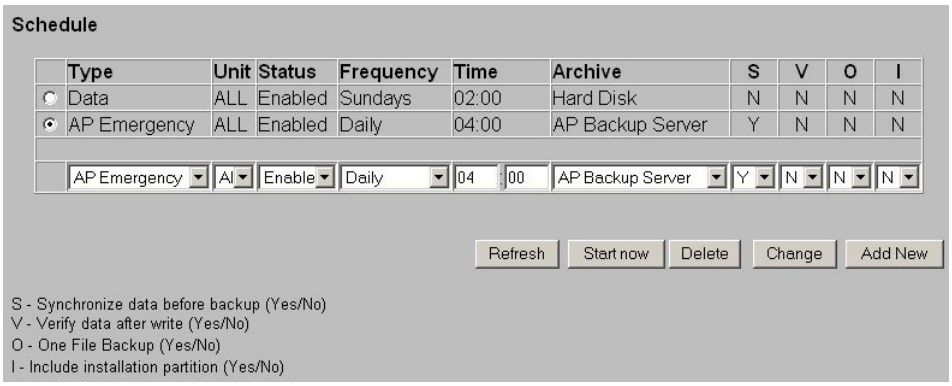
11.3.1.2 Einrichten eines Zeitplans für den Backup

Als zweiter Konfigurationsschritt muss nun festgelegt werden, wann OpenScape 4000 Assistant Backup & Restore einen Backup auf den eingerichteten AP Backup-Server durchführt. Typisch ist ein Backup täglich in einer betriebsschwachen Zeit.

Bei der Auswahl der Startzeit für den Backup muss berücksichtigt werden, dass damit indirekt auch die Startzeit für den Restore auf den CC-APs festgelegt wird. Der Restore auf dem CC-AP/Survivable OpenScape 4000 SoftGate startet, sobald der CC-AP/das Survivable OpenScape 4000 SoftGate einen neuen vollständigen Backup vorfindet. Die Abhängigkeiten sind im Abschnitt 3.1, „Zeitliche Rahmenbedingungen“ dargestellt.

Voraussetzung:

- Über Web-Browser im OpenScape 4000 Assistant unter Â«`rsta`Â»-Kennung angemeldet.
- **Software Management** -> **Backup & Restore** gestartet.
- In der Bedienoberfläche von Backup & Restore die Funktion **Zeitplan** auswählen.



Backup & Restore: Einrichten eines Zeitplans für den Backup

Die folgenden Felder müssen nun ausgefüllt werden:

Tabelle 73: Eingabefelder des Zeitplans im OpenScape 4000 Assistant Backup & Restore

Feldname	Wert	Erklärung
Typ	AP Emergency	nur dieser Wert zulässig.
Einheit	Alle	nur dieser Wert zulässig.
Status	Aktiviert	hiermit kann ein konfigurierter Zeitplan ein- bzw. aus-geschaltet werden.
Frequenz	Täglich (Wochentags, Montags, Dientags, Mittwochs,...)	Typischerweise sollte täglich ein Backup durchgeführt werden.
Zeit	Stunde: Minute	Uhrzeit, zu welcher der Backup beginnen soll
Archiv	AP Backup-Server	nur dieser Wert zulässig - AP Backup-Server muss vorher eingerichtet worden sein.
S	**JA**	Vor Backup synchronisieren, d.h. UPDATe durchführen. Muss auf **Ja** stehen, damit der aktuellste Stand der Datenbasis gesichert wird.
V	Ja/**Nein**	Verifizieren der Backup Daten
O	Ja/**Nein**	Backup einer einzelnen Datei
I	Ja/**Nein**	Installationspartition inkludieren

Soll häufiger als einmal am Tag ein Backup durchgeführt werden, so können weitere tägliche Backups im Zeitplan eingetragen werden, z.B. ein Backup um 12:00 Uhr und ein weiteres um 18:00 Uhr.

Die Einrichtung des Backup der Konfigurationsdaten wird abgeschlossen durch

- **Neuen Eintrag hinzufügen** - Der neue Eintrag im Zeitplan wird gespeichert. Ein Backup wird entsprechend der Konfiguration ausgeführt.

Hiermit ist die Konfiguration am OpenScape 4000 Zentralsystem abgeschlossen.

Die Dauer des Backup-Vorgangs hängt stark von der zu übertragenden Datenmenge und von der zwischen Zentralsystem und AP Backup-Server verfügbaren Übertragungsbandbreite ab. Der Vorgang dauert mindestens eine Stunde.

11.3.1.3 Durchführen des ersten Backup

Es kann zweckmäßig sein, außerhalb des eingerichteten Zeitplans sofort einen Backup anzustoßen, um möglichst wenig Zeit zu verlieren, bis die CC-APs die Daten abholen können.

Hierzu einen Zeitplan für AP Emergency auswählen und **Jetzt starten** anklicken.

Der erste Backup des Systems dauert am längsten, da alle gesicherten Daten erstmalig auf den AP Backup-Server übertragen werden müssen (ca. 100 MByte). Die erforderliche Zeit hängt auch sehr wesentlich von der verfügbaren Bandbreite im IP-Netz zwischen OpenScape 4000 Host System und AP Backup-Server ab.

11.3.1.4 Handhabung von OpenScape 4000 Assistant Backup & Restore bei größeren Änderungen am System

Sollen größere Änderungen am System durchgeführt werden, oder wird eine neue Systemausgabe eingespielt, so können folgende Anforderungen auftreten:

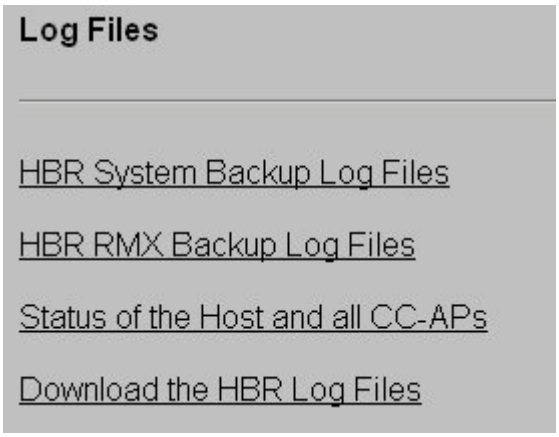
- Größere Konfigurationsänderungen sollen so schnell wie möglich auf alle CC-AP/Survivable OpenScape 4000 SoftGate verteilt werden
- – Sie sollten sofort nach Abschluss der Änderungen einen „außerplanmäßigen“ Backup anstoßen. Prüfen Sie aber, ob zu diesem Zeitpunkt ausreichend Übertragungsbandbreite im Netzwerk zur Verfügung steht, um den Backup und die foglenden Restore Operationen der CC-APs abzuwickeln. Bedenken Sie, dass Sie gerade aktive Backup und auch Restore-Vorgänge nicht abbrechen können. Eventuell macht es Sinn, vor der Durchführung der Änderungen den Backup-Prozess auszusetzen. -> Siehe zweiter Punkt. Gehen Sie in OpenScape 4000 Assistant Backup & Restore auf den Zeitplan für den Backup-Typ „AP Emergency“ und klicken Sie auf **Jetzt starten**. Gehen Sie besser nicht über „Backup“, denn hier müssen Sie selber daran denken, vorher einen EXEC-UPDAT durchzuführen.
- Neue Software (egal ob Vorabkorrektur einer LW oder eine neuen Systemausgabe) soll erst am Zentralsystem verifiziert werden, bevor es auf alle CC-APs verteilt wird
- – *Bevor neue Software eingespielt wird:* Gehen Sie in OpenScape 4000 Assistant Backup & Restore auf den Zeitplan für den Backup-Typ „AP Emergency“ und ändern Sie den Status von „**aktiviert**“ auf „**deaktiviert**“. Falls mehrere Einträge im Zeitplan für den Backup-Typ „AP Emergency“ vorhanden sind, müssen Sie alle Einträge deaktivieren, die für den geplanten Zeitraum in Frage kommen.
  – *Nach erfolgreicher Prüfung der Software:* Gehen Sie in OpenScape 4000 Assistant Backup & Restore auf den Zeitplan für den Backup-Typ „AP Emergency“ und ändern Sie den Status von „**deaktiviert**“ auf „**aktiviert**“ zurück. Falls mehrere Einträge im Zeitplan für den Backup-Typ „AP Emergency“ vorhanden sind, müssen Sie alle Einträge aktivieren, die Sie vorher deaktiviert haben. Sofern die Netzwerkgegebenheiten es erlauben, kann es sinnvoll sein, ein außerplanmäßiges Backup anzustoßen. -> Siehe erster Punkt.

11.3.1.5 Prüfen der regelmäßigen Aktivitäten von OpenScape 4000 Assistant Backup & Restore

Zusätzlich zu den „üblichen“ Methoden (Log-Files etc.) gibt es für die Kommunikation mit dem AP Backup-Server die Möglichkeit abzufragen, wann welcher Prozessor zuletzt in Kontakt mit dem AP-Backup-Server war.

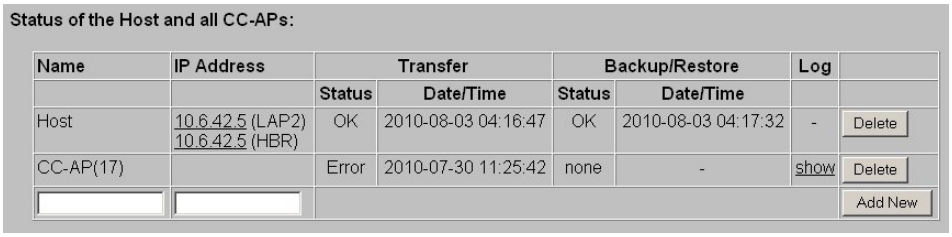
Voraussetzung:

- Über Web-Browser im OpenScape 4000 Assistant unter Â«rstaÂ»-Kennung angemeldet.
- **Software Management** -> **Backup & Restore** gestartet.
- In der Bedienoberfläche von Backup & Restore die Funktion Protokolldateien ausgewählt.



Backup & Restore - Auswahl „Protokolldateien“

- Wählen Sie in der Liste „Status des Hosts und aller CC-APs“ aus



Backup & Restore - Status Host und CC-APs

Die Datum/Zeit-Angaben sind wie folgt zu interpretieren:

Host:	Abschluss des letzten Backup-Vorgangs
CC-AP/Survivable OpenScape 4000 SoftGate:	Zeitpunkt der letzten Nachfrage am AP Backup-Server (fragt in der Regel alle 10 Minuten einmal nach)

11.3.2 Konfiguration von OpenScape 4000 Assistant Backup & Restore am CC-AP/Survivable OpenScape 4000 SoftGate

11.3.2.1 Einrichten des AP Backup-Servers am CC-AP/Survivable OpenScape 4000 SoftGate

Für den automatischen Restore der gesicherten Daten muss festgelegt werden, wo die Daten des OpenScape 4000 Backup abgeholt werden sollen. Hierzu müssen Rechner, Verzeichnis und Login-Daten genau so eingerichtet werden, wie es für den AP Backup-Server am OpenScape 4000 Zentralsystem eingerichtet wurde (siehe Abschnitt 3.1.1, „Einrichten eines AP Backup-Servers mit OpenScape 4000 Assistant Backup & Restore“).

- In der Bedienoberfläche von **Backup & Restore** die Funktion **Administration AP Backup-Server** auswählen.

Die folgenden Felder müssen nun identisch zur Einstellung am OpenScape 4000 Zentralsystem ausgefüllt werden:

- **Protokoll** (SFTP oder NFS) - typisch: **SFTP**
- **IP-**Adresse **oder** Host-Name des AP Backup-Servers.
- **Verzeichnis** auf dem AP Backup-Server.
- Wurde **SFTP** als Protokoll gewählt, so muss noch der Login-Name für die **Anmeldung** und das **Passwort** für den Zugriff auf den AP Backup-Server (SFTP-Server) eingerichtet werden. Falls der SFTP-Server einen **Account** benötigt, ist dieser ebenfalls einzugeben.

  Wichtig: Wenn als Backup-Verzeichnis **/.AS/BACKUP/IPDA** verwendet wird, sollte aus Sicherheitsgründen als ftp-User „apeftp“ verwendet werden.

- Durch Aktivieren der Auswahl „**Automatischer Restore gesperrt**“ kann der Restore-Prozess ausgesetzt werden. Aktivieren Sie diesen Schalter nur vorübergehend und vergessen Sie nie, den Schalter für den Routinebetrieb wieder auszuschalten.

Die Einrichtung des Backup der Konfigurationsdaten wird abgeschlossen durch:

- Testen und Sichern der Konfiguration und Test des Zugriffs auf den AP Backup-Server.

  Mit dieser Option wird getestet, ob die Installation funktioniert, d.h.:

  – Verbindung zum AP Backup-Server kann aufgebaut werden
  – Login mit den konfigurierten Daten ist möglich
  – Zugriff auf das konfigurierte Verzeichnis ist möglich
- Testen der Konfiguration ohne Sicherung.

  Diese Option ist für Diagnosezwecke gedacht.

Damit ist der Zugriff auf den AP Backup-Server eingerichtet. Die OpenScape 4000 Assistant Backup& Restore Applikation am CC-AP/Survivable OpenScape 4000 SoftGate wird nun ab sofort alle 10 Minuten Kontakt zum AP Backup-Server aufnehmen, prüfen, ob ein neues, vollständiges Backup-Set vorliegt, und die veränderten Teile des Backup-Sets herunterladen und aktivieren.

Wichtig: Vor dem ersten Restore führt OpenScape 4000 Assistant Backup & Restore einen kompletten Backup auf die Harddisk durch. Dieser Backup wird als Referenz für die Bestimmung der geänderten Dateien genutzt, welche beim

Restore vom AP Backup-Server geholt werden müssen. Der Backup muss nicht extra angestoßen werden. Er kann aber auch nicht verhindert werden. Für diesen Vorgang wird etwa eine Stunde benötigt.

Die Dauer des Restore-Vorgangs hängt stark von der zu übertragenden Datenmenge und von der zwischen AP Backup-Server und CC-AP/Survivable OpenScape 4000 SoftGate verfügbaren Übertragungsbandbreite ab. Der Vorgang dauert mindestens eine halbe Stunde.

11.3.2.2 Einrichten eines regelmäßigen Backup der Konfigurationsdaten auf Harddisk

Der CC-AP/das Survivable OpenScape 4000 SoftGate bezieht zwar die wesentlichen Konfigurationsdaten durch Restore vom Zentralsystem. Trotzdem lohnt es sich, auch die spezifische lokale Konfiguration des CC-AP/Survivable OpenScape 4000 SoftGate regelmäßig zu sichern. Da Änderungen der lokalen Konfiguration eher selten sind, ist ein wöchentlicher Backup ausreichend. Beachten Sie beim Festlegen der Startzeit, dass dieser Backup sinnvoll nach dem Backup des Zentralsystems und dem folgenden Restore am CC-AP/Survivable OpenScape 4000 SoftGate laufen sollte.

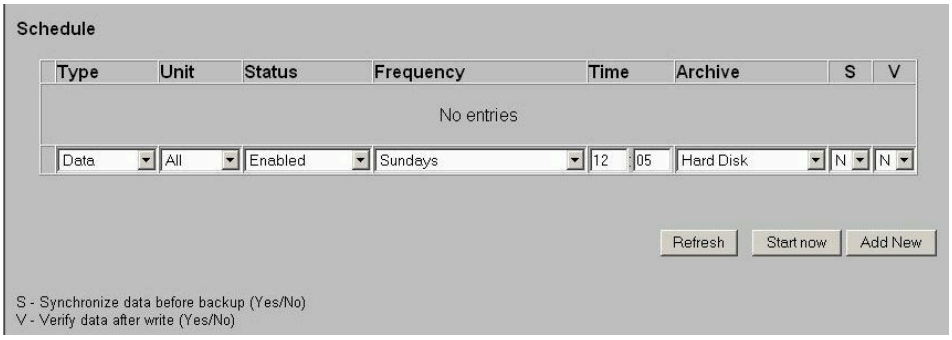
Dem Beispiel liegt folgender Plan zu Grunde:

1) Start Backup des Zentralsystems: täglich 22:05

2) • Abschluss Restore des CC-AP/Survivable OpenScape 4000 SoftGate: spätestens 06:30
• Lokaler Backup auf Harddisk: Sonntags 12:05

Voraussetzung für die Einrichtung:

- Über Web-Browser im OpenScape 4000 Assistant unter Â«rstaÂ»-Kennung angemeldet.
- **Software Management** -> **Backup & Restore** gestartet.
- In der Bedienoberfläche von Backup & Restore die Funktion **Zeitplan** auswählen.



Backup & Restore: Einrichten eines Zeitplans für den Backup der Konfigurationsdaten

Folgende Felder müssen ausgefüllt werden:

Tabelle 74: Eingabefelder des Zeitplans für den Backup der Konfigurationsdaten

Feldname	Wert	Erklärung
Typ	Daten	nur dieser Wert zulässig.
Einheit	Alle	nur dieser Wert zulässig.
Status	Aktiviert	hiermit kann ein konfigurierter Zeitplan ein- bzw. aus-geschaltet werden.
Frequenz	z.B. Sonntags	Typischerweise sollte wöchentlich ein Backup durchgeführt werden, z.B. Sonntags.
Zeit	Stunde: Minute	Uhrzeit, zu welcher der Backup beginnen soll
Archiv	Festplatte	nur dieser Wert zulässig.
S	Ja/**Nein**	Vor Backup synchronisieren, d.h. UPDATe durchführen. - Ist hierfür nicht erforderlich.
V	Ja/**Nein**	Verifizieren der Backup Daten

Die Einrichtung des Backup der Konfigurationsdaten wird abgeschlossen durch

- **Neuen Eintrag hinzufügen** - Der neue Eintrag im Zeitplan wird gespeichert. Ein Backup wird entsprechend der Konfiguration ausgeführt.

Die Dauer des Backup-Vorgangs liegt bei etwa 10 Minuten.

11.4 Service-Szenarien

11.4.1 Hochrüstung des AP-Emergency Servers (neues Fix Release/Minor Release)

Ablauf

Der AP-Emergency-Server schaut regelmäßig in seinen Backup-Bereich, ob dort ein aktualisiertes Software-Paket liegt. Wenn dort ein neues Software-Paket liegt, dann wird dieses auf den AP-Emergency-Server kopiert.

Hinweise

- Erfolgte eine Hochrüstung mittels Software Transfer/Software Aktivierung (Hotfix/FixRelease/MinorRelease-Upgrade), dann werden alle Patches zur Verfügung gestellt und das gesamte System wird hochgerüstet (OpenScape 4000 Plattform, ADP/CCA/CCB, OpenScape 4000 Assistant, OpenScape 4000 CSTA). In diesem Fall werden die Patche mit Hilfe von OpenScape 4000 Backup & Restore zum APE übertragen und durch die OpenScape 4000 Software Aktivierung aktiviert.
- Erfolgte eine RMX-Hochrüstung über einen HD-Austausch innerhalb des selben Major Release, dann übernimmt der APE sowohl die RMX-Software als auch die OpenScape 4000 Assistant Software. Damit das funktioniert

wird ein Backup benötigt, der auch die Dateien der Installations-Partition enthält. Dieses Backup erstellen Sie im **OpenScape 4000 Assistant > Software Management > Backup & Restore > Zeitplan** (Backup Zeitplan für AP Emergency) und wählen in der letzten Spalte **I=J**. Für eine Software-Hochrüstung zu einem nächsten Major Release ist diese Funktionalität nicht gewährleistet!

- Erfolgte eine RMX-Hochrüstung über einen HD-Austausch (Wechsel des Major Release), dann entspricht die Vorgehensweise einer Neuinstallation und der APE übernimmt nur die RMX-Software. Es erfolgt keine Hochrüstung der OpenScape 4000 Assistant Software.
- **Die APE-Funktionalität ist allerdings nicht von der OpenScape 4000 Assistant Version abhängig und daher entsprechend gewährleistet!**

11.4.2 DSCXL2-Austausch im AP-Emergency Server

Bei einem Defekt der DSCXL2 gehen Sie wie folgt vor.

1) Defekte DSCXL2 entfernen.
2) Neue DSCXL2 einbauen.
3) Software neu installieren (siehe How Tos zur APE-Installation)

Wichtig: Bitte achten Sie darauf, dass der Softwarestand, der am AP Emergency Server installiert wird, dem Softwarestand des Host-Systems entspricht (gleiches Minor- bzw. Fix-Release).

---

1) Restore mit Hilfe von OpenScape 4000 Assistant „Backup & Restore“ einspielen.

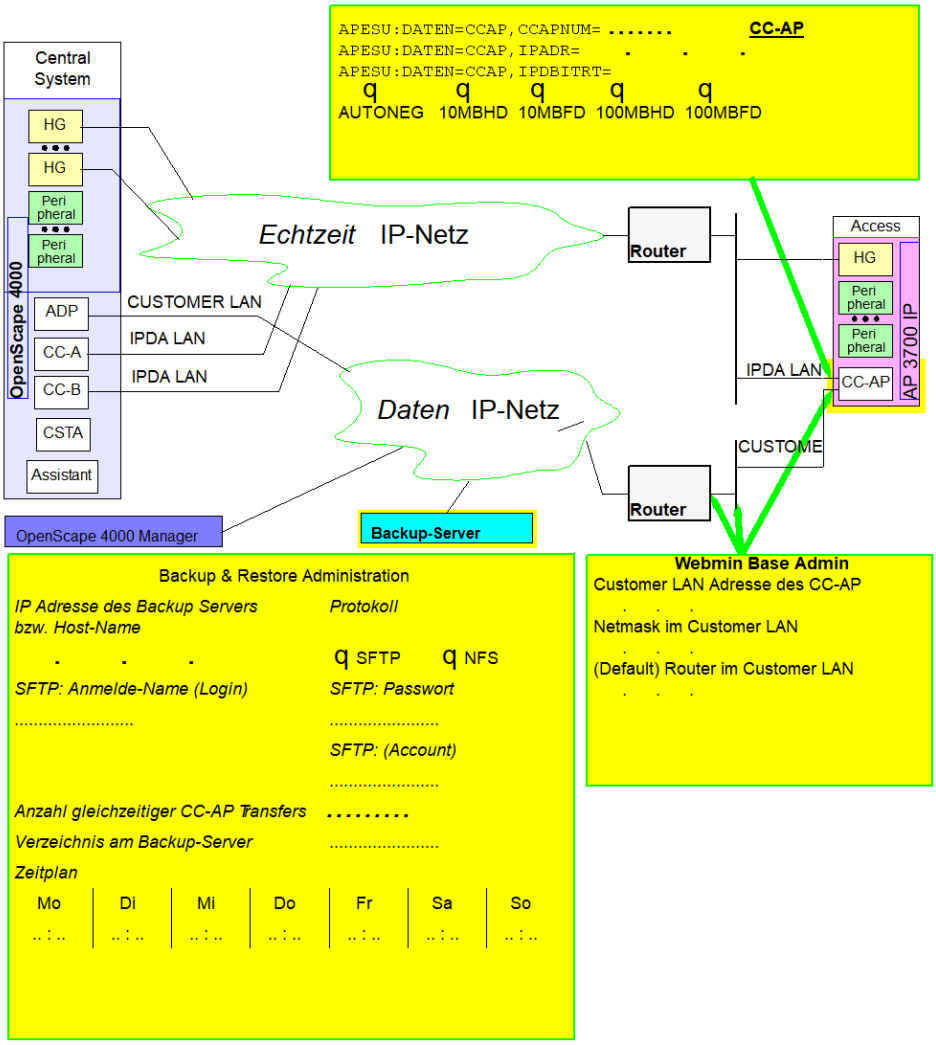
11.5 Arbeitsblätter - APE-Konfiguration

Die folgenden Arbeitsblätter sollen bei den ersten Schritten zu einer APE-Konfiguration helfen. Sie sind so angelegt, dass sich auf der Vorderseite jeweils ein Konfigurationsbild und AMO-Template zum Ausfüllen befindet, auf der Rückseite das ausgefüllte Beispiel aus dem Servicehandbuch.

Die folgenden Arbeitsblätter (mit Beispiel) werden zur Verfügung gestellt:

- Arbeitsblatt AP-Emergency: Einrichtung eines CC-AP
- Arbeitsblatt AP-Emergency: Emergency Gruppe

Arbeitsblatt AP-Emergency: Einrichtung eines CC-AP



Im Arbeitsblatt sind zwei getrennte Netze für Echtzeit- bzw. Daten-Kommunikation dargestellt. Wird für beide Kommunikationsarten ein gemeinsames Netz verwendet, so sind die beiden Router identisch.

Arbeitsblatt AP-Emergency: Emergency Gruppe

Arbeitsblatt: Emergency Gruppe							
	EGRPNUM		NAME				
Nummer		Name					CC
Umschaltung in Emergency Mode					**Zugeordnete Access Po**		
		SCHWELLE			LTU	**GEWICHT**	**UM**
Schwellwert der Gewichtung					APNUM		**EI**
							q

Rückschaltung in Normal Mode							q
	SBMODE	**AUTO**matisch	**MAN**uell				q
Rückschaltemodus		q	q				q
		STABIL					q
Stabilitätszeit			[Minuten]				q
							q
Zeitraum für automatische Umschaltung							q
	Stunde	Minute (Offset)					q
Beginn							q
Ende							q
	RSBEGINN	RSOFFSET					q
	RSENDE						q
							q
							q
							q
							q
							q
							q
							q
							q
							q
		Summe der Gewichte					

11.6 Hinweise für Netzwerkadministratoren

11.6.1 Survivability Unit für AP-Emergency

Mit der Survivability Unit wird ein Steuerungsprozessor in einen Access Point gebracht. Bei maximal 83 Access Points je System können maximal 83 Survivability Units ins System eingebracht werden.

Der Prozessor der Survivability Unit benötigt 2 LAN-Anschlüsse in das IP-Netz.

Details finden Sie im „Band 2 - Systemkomponenten (Harwdare & Software) > OpenScape 4000 im LAN des Kunden > AP 3700 IP/OpenScape 4000 SoftGate mit Survivability Unit im LAN des Kunden“.

Eine Schnittstelle „IPDA“ wird für die Signalisierungsverbindung mit den zugeordneten Access Points benötigt.

PHY	10/100 Base T - autosensing bzw. fest einstellbar
MAC-Adresse	fest programmiert, ->Aufkleber (höhere der 2 Adressen)
IP-Adresse	Im OpenScape 4000 System konfiguriert, frei einstellbar
IEEE 802.1p/q VLAN-Tagging	Konfigurierbar, wenn aktiv werden immer die Prioritätsbits gesetzt. Siehe Tabelle 3 „TOS-Werte“ in Dokument „Gateways HG 3500 und HG 3575“. Die VLAN-ID ist frei einstellbar. Konfiguration im OpenScape 4000 System.
TOS / DiffServ	Die 6 höchstwertigen Bits der TOS-Bytes sind frei einstellbar. Siehe Tabelle 3 „TOS-Werte“ in Dokument „Gateways HG 3500 und HG 3575“. Konfiguration im OpenScape 4000 System.
Protokolle / Ports	Siehe Kapitel 21, „IP-Ports“ im Dokument „Gateways HG 3500 und HG 3575“.
Routing	den Access Point wird die Default-Host-Route benutzt, welche für die HG 3575 im selben Shelf eingerichtet ist.
Firewall	Der Zentralprozessor erlaubt nur Verbindungen zu ihm bekannten Adressen, d.h. den Access Points, bzw. denen zugeordnete Service PCs.
Verbindungszahl	maximal 83 TCP/IP Verbindungen (1 je zugeordnetem Access Point)

Eine weitere Schnittstelle „CUSTOMER“ wird für Remote-Zugriff vom OpenScape 4000 Manager und für den Zugriff auf den File-Server benötigt, über den Software und Daten des OpenScape 4000 Zentralsystems verteilt werden.

PHY	10/100 Base T - autosensing
MAC-Adresse	fest auf programmiert, ->Aufkleber (niedrigere der 2 Adressen)
IP-Adresse	Im OpenScape 4000 Assistant konfigurierbar

Routing	konfigurierbar
Verbindungszahl	Bei Bedarf TCP/IP-Verbindung zum File-Server. Administration über OpenScape 4000 Assistant
Security	Wie für OpenScape 4000 Assistant

11.7 Kurzanleitung zum Einrichten eines AP Emergency (IPDA)

11.7.1 Einleitung

In diesem Kapitel wird ein AP Emergency Konfigurationsbeispiel und dessen Generierung mittels AMOs und OpenScape 4000 Assistant aufgezeigt. Es wird auf einer vorhandenen IPDA-Konfiguration aufgesetzt.

Fallunterscheidung:

Bei AP Emergency wird zwischen Direct Link und Networked-Konfiguration unterschieden.

Direct Link bedeutet, dass sich der AP Emergency und das OpenScape 4000 Host System im gleichen Netzsegment (OpenScape 4000 LAN Segment) befinden.

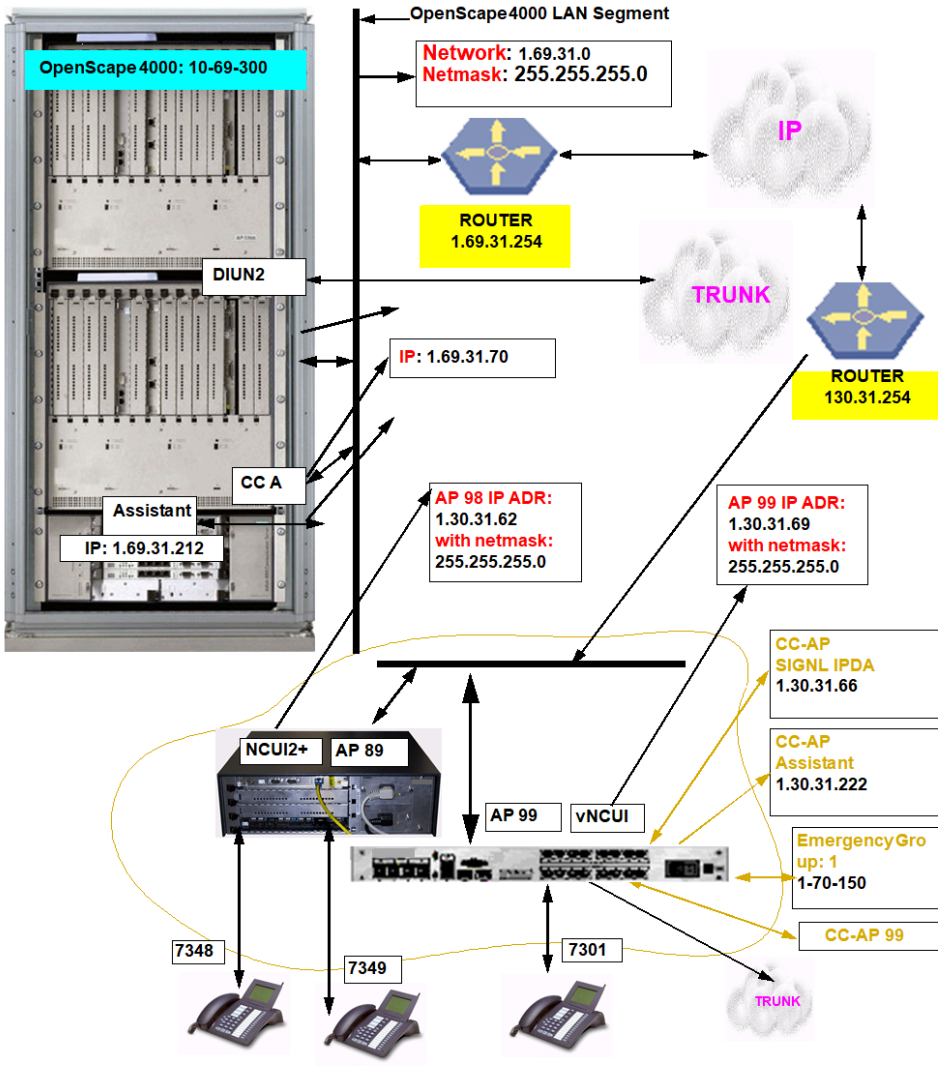
Networked-Konfiguration bedeutet, dass sich der AP Emergency und das OpenScape 4000 Host System in unterschiedlichen Netzsegmenten befinden.

Dabei ist folgendes zu beachten:

- Sind die IPDA-Shelfs einer Emergency Gruppe direct link angeschaltet, so muss ihr zugehöriger Emergency Prozessor ebenfalls direct link angeschaltet werden.
- Sind IPDA-Shelfs networked angeschaltet, so kann der zugehörige Emergency Prozessor direct link oder networked sein.

Die Einrichtung eines direct link Emergency Prozessors unterscheidet sich nur geringfügig von einer Networked-Konfiguration. Bei networked ist lediglich darauf zu achten, dass in den OpenScape 4000 Assistants von Host und APE die jeweiligen Routereinträge stimmen.

Das folgende Generierungsbeispiel entspricht der folgenden Konfiguration und IP-Situation:



11.7.2 Voraussetzung

Das Leistungsmerkmal IPDA ist schon installiert. Die relevanten Parameter sind:

OpenScape 4000 LAN Segment	1.69.31.0, Netzmaske 255.255.255.0
CC-A	1.69.31.70
CC-B	nicht vorhanden
HG3575 - AP98	1.30.31.62, 255.255.255.0
vHG3575 - AP99	1.30.31.69, 255.255.255.0
Assistant- Customer LAN	1.69.31.212

Default Router - OpenScape 4000 Host-System	1.69.31.254
Default Router - AP-LAN	1.30.31.254

Für das Leistungsmerkmal Access Point Emergency braucht man neue IP-Adressen:

eth0 - SLES	1.30.31.220
Portal Access 500	1.30.31.221
Assistant Customer APE	1.30.31.222
CC-C (IPDA-Signaling)	1.30.31.66

Für den Einsatz von AP Emergency müssen im Codewort Lizenzen vorhanden sein.

Wichtig: Survivability und AP Emergency müssen gekauft werden, um es nutzen zu können

```
ABFRAGEN-CODEW;
  ------------------------------------------+-------
+-------+-------+-------+

|                     EINHEIT                | GE-   |
 VER-  | FREI  | GE-   |

|                                            | KAUFT |
 WENDET|       | SPERRT|

+-------------------------------------------+-------
+-------+-------+-------+

|  OPENSCAPE 4000 V6 FLEX                    | 12000 |
 89 | 11911 |       |

|  SIGNALING SURVIVABILITY                   |    83 |
 0 |    83 |       |

|  CC-AP FUER AP EMERGENCY                   |    83 |
 1 |    82 |       |

+-------------------------------------------+-------
+-------+-------+-------+
```

11.7.3 Einrichtungsschritte in OpenScape 4000

Schritt 1: Signaling IP-Adresse des CC-APs einstellen

Voraussetzung: `EINRICHTEN-DIMSU:TYP=SYSTEM,CCAP=xx;`
`EINRICHTEN-APESU:DATEN=CCAP,CCAPNUM=99,IPADR=1.30.31.66;`

Wichtig: Die CC-AP Nummer muss eine der AP (LTU) Nummern sein, die im System eingerichtet sind (normalerweise die AP Nummer, in welcher der CC-AP eingebaut ist).

Schritt 2: AP-Emergency-Gruppe einrichten

Voraussetzung: `EINRICHTEN-DIMSU:TYP=SYSTEM,APEGRP=xx;`
`EINRICHTEN-`
`APESU:DATEN=APEGRP,EGRPNUM=1,`**`CCAPNUM`**`=99,`**`SCHWELLE`**`=0,`**`RSMODE`**`=AUTO,N`
`AME``="HPA MUC",`**`STABIL`**`=10,`**`RSBEGIN`**`=20,`**`RSENDE`**`=6,`**`RSOFFSET`**`=15;`

Parameter	Beschreibung
CCAPNUM	Nummer des CC-AP, der die Emergency-Gruppe steuert
NAME	Name der Emergency-Gruppe
RSMODE	Rückschaltemodus: manuell oder automatisch (bei manueller Rückschaltung ist das Umschalteintervall nicht relevant)
RSBEGIN	Umschalteintervall: Beginn (Stunde) für eine automatische Rückschaltung
RSENDE	Umschalteintervall: Zeitende (Stunde) für eine automatische Rückschaltung
RSOFFSET	Umschalteintervall: Minuten für RSBEGIN und RSENDE
STABIL	Stabilitätszeit der LAN-Verbindung in Minuten
SCHWELLE	Grenzwert für den Gewichtungsalgorithmus Jeder AP bekommt mit dem AMO APESU ein „Gewicht“ zugeordnet. Wird der Grenzwert in der Emergency-Gruppe überschritten, wird auf den CC-AP dieser Gruppe umgeschaltet.

Schritt 3: AP 98 und 99 für AP-Emergency einrichten

```
EINRICHTEN-
APESU:DATEN=AP,APNUM=98,EGRPNUM=1,GEWICHT=0,UMSCHALT=GRUPPE;
EINRICHTEN-
APESU:DATEN=AP,APNUM=99,EGRPNUM=1,GEWICHT=0,UMSCHALT=GRUPPE;
```

Schritt4: Display-Anzeige im Emergency-Mode am Systemtelefon einrichten

```
AENDERN-ZANDE:TYP=DATENALL,APEDTXT="            AP
 EMERGENCY";
```

Schritt 5: Umschaltverzögerung festlegen

z.B.: soll ein RELOAD der Anlage (OpenScape 4000) nicht zum Emergency-Betrieb führen, kann eine Umschaltverzögerung (in Minuten) eingerichtet werden.

```
ABFRAGEN-SIPCO:TYP=TIMING;
H500:  AMO SIPCO GESTARTET
  TIMING :



 ---------------------------------------------------------------

  PINGTIME ( UEBERW.-ZEIT FUER PAYLOAD PATH QUALITY ) :
 60 SEK

  RESTIME  ( RESET ZEIT BEI SIGNALING VERB. VERLUST ) :
 60 SEK

  SUPVTIME ( UEBERW.-ZEIT FUER SUPERVISORY VERB. )    :
 4 SEK

  APESWDLY ( APE UMSCHALTEVERZOEGERUNG. )             :
 0 MIN

  ALVTIME  ( UEBERW.-ZEIT FUER SIGNALING VERBINDUNG ) :
 60 SEK


AENDERN-SIPCO:TYP=TIMING,APESWDLY=<MIN>;
```

Schritt 6: AP Emergency-Konfiguration abfragen

```
ABFRAGEN-APESU:;
+-------------------------------------------------------------------
+

| AKTUELLE SYSTEMZEIT  : 22-06-2012   09:35:47
                     |

+-------------------------------------------------------------------
+



+-------------------------------------------------------------------
+

| CC-AP: 99                          IP ADRESSE: 1
  .30 .31 .66                 |

+-------------------------------------------------------------------
+

+-------------------------------------------------------------------
+
```

```
| AP EMERGENCY GRUPPE: 1    CC-AP: 99          NAME: HPA
 MUC                  |

| SCHWELLE: 0       RSMODE: AUTO
                     |

| STABIL: 10  MIN     RSBEGIN: 20 H     RSENDE: 6  H
 RSOFFSET: 15 MIN      |

+-------------------------------------------------------------------
+

| AP: 98  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0
  UMSCHALT: GRUPPE  |

| KONTROLL-EINHEIT: UNBEKANNT   SIGNAL-PFAD: KEIN
                     |

| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                     |

|
                     |

|     HOST-CC:  VERBUNDEN: NEIN       GETRENNT SEIT:
 00-00-0000  00:00         |

|     CC-AP:    VERBUNDEN: NEIN       GETRENNT SEIT:
 00-00-0000  00:00         |

+-------------------------------------------------------------------
+

| AP: 99  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0
  UMSCHALT: GRUPPE  |

| KONTROLL-EINHEIT: UNBEKANNT   SIGNAL-PFAD: KEIN
                     |

| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                     |

|
                     |

|     HOST-CC:  VERBUNDEN: NEIN       GETRENNT SEIT:
 00-00-0000  00:00         |

|     CC-AP:    VERBUNDEN: NEIN       GETRENNT SEIT:
 00-00-0000  00:00         |

+-------------------------------------------------------------------
+
```

Schritt 7: BP-Datenbasis updaten und lokale HG3575 Datenbasis synchronisieren

```
EXEC-USSU:ART=UPDATAP,LTU=98;
EXEC-USSU:ART=UPDATAP,LTU=99;
EXEC-UPDAT:MODUL=BP,SUSY=ALL;
```

Schritt 8: Synchronität des Configuration Management überprüfen

Nach dem Abschluss der Einrichtung mit AMO APESU verbindet man sich mit dem OpenScape 4000 Assistant im Host (z.B. http://1.30.11.212). Dort vergewissert man sich zunächst, ob das Configuration Management synchron ist zum RMX-System. Ist das nicht der Fall, muss ein Upload durchgeführt werden.

Dazu geht man auf **Configuration Management > Netzwerk > Anlage**, klickt auf der angezeigten Seite auf **Suchen** und startet ggf. den Upload mit **Aktion** / **Upload**.

Schritt 9: Zeitserver im Host (Zentrale) einstellen

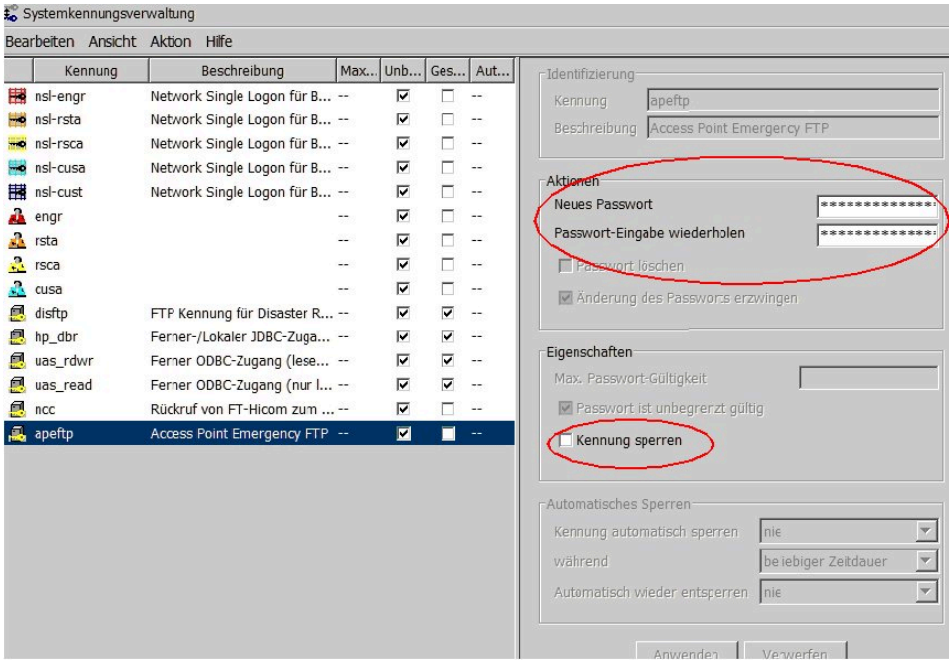
Für viele Funktionen der OpenScape 4000 ist eine exakte Uhrzeit erforderlich. Die OpenScape 4000 sollte daher an einen Zeitserver angebunden werden. Man geht dabei folgendermaßen vor:

1) Aufbau einer ssl-Verbindung zum SLES (z.B. mit putty), hier zu 1.30.31.210.
2) Anmeldung mit root/hicom und Aufruf von yast.
3) In yast auf System / Date and Time gehen.
4) Region (z.B. Europe) und Time Zone (z.B. Germany) einstellen. **Hardware Clock Set To UTC** aktivieren, dann mit **Change** auf die Seite **Change Date and Time** wechseln. Dort unter **Synchronize with NTP Server** die IP-Adresse des Zeitservers eintragen (hier 1.50.100.2). **Save NTP Configuration** ankreuzen und auf **Configure** gehen.
5) Bei **Advandced NTP Configuration > Now and on Boot** ankreuzen. Nach Drücken auf **Ok** startet der NTP Dienst neu und yast kann wieder verlassen werden.
6) Über AENDERN-DATE:; wird die Uhrzeit im RMX aktualisiert.

Schritt 10: Systemkennung apeftp konfigurieren

Anstelle einer herkömmlichen Systemkennung sollte die spezielle Systemkennung apeftp für den Transport des APE Backup Sets verwendet werden. Um apeftp verwenden zu können, muss er explizit freigegeben werden. Dazu geht man im OpenScape 4000 Assistant auf **Zugangsverwaltung > Kennungsverwaltung > Systemkennungsverwaltung**, entsperrt dort den User apeftp und gibt ihm anschließend ein Passwort.

Dasselbe muss später auch im OpenScape 4000 Assistant des APE-Prozessors durchgeführt werden, da die Kennungen und Passwörter nicht über den APE Backup synchronisiert werden.



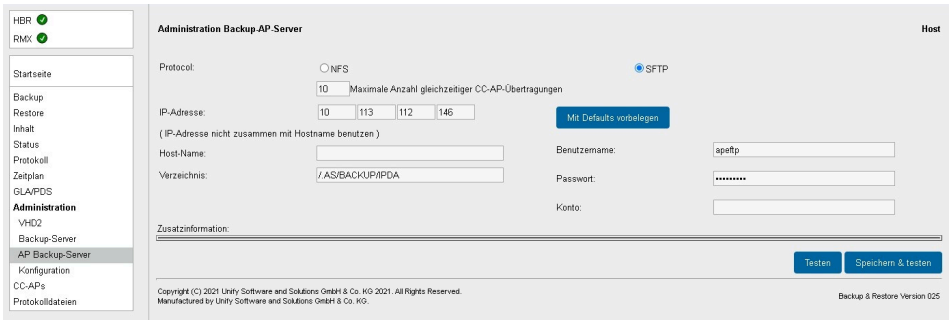
Systemkennung apeftp im Host konfigurieren

Schritt 11: AP Backup Server einrichten

OpenScape 4000 Assistant:

Software Management > Backup & Restore > AP Backup-Server

In diesem Beispiel ist die OpenScape 4000 selbst der Backup-Server. Das Verzeichnis /.AS/BACKUP/IPDA ist im System vorgeleistet. Abschließend Testen drücken (enthält auch Konfigurieren).

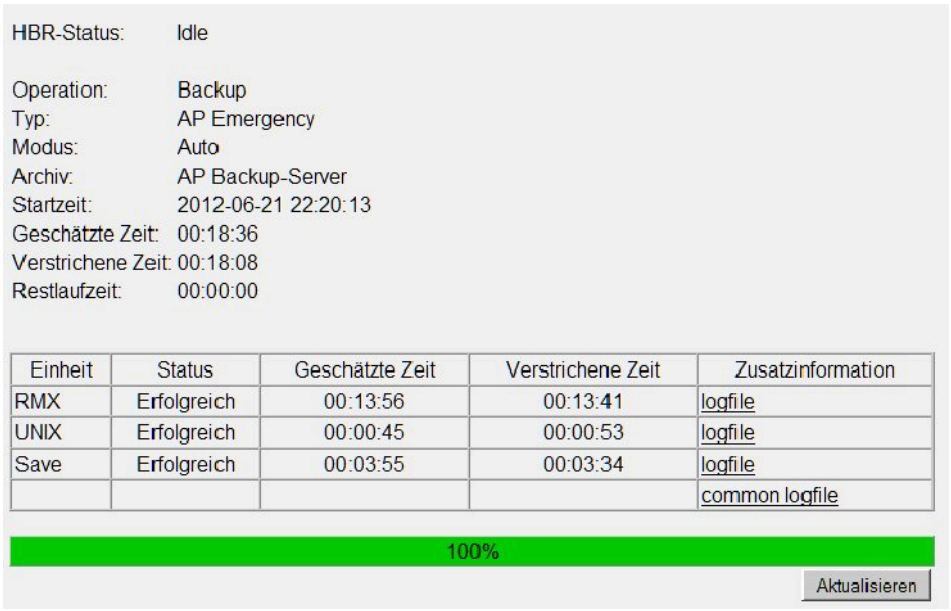


AP Backup Server im Host einrichten

Durch die Festlegung des Zeitplans für den Backup, wird indirekt der Transfer-zeitpunkt zu den CC-APs definiert. Maximal 10 Minuten (nicht steuerbar) nach dem Backup, erkennen die CC-APs, dass ein neueres Backup-Set zur Verfügung steht und holen sich das Delta automatisch.

Bei der Erstinstallation ist der erste Backup manuell zu starten (Schritt 2), um das Leistungsmerkmal komplett einrichten zu können.

Nach dem manuellen Backup den Status prüfen:



Backup-Status prüfen

11.7.4 Einrichtungsschritte im CC-AP

Schritt 1: AP Emergency auf DSCXL2 oder OpenScape 4000 SoftGate/ OpenScape Access 500 installieren

1) USB Installation des DSCXL2s (Deployment AP Emergency) oder OpenScape 4000 SoftGate / OpenScape Access 500 (Deployment Survible SoftGate).

2) Monitor/Tastatur anschließen oder über Standard-IP Adresse (192.168.0.2) mit der Anlage verbinden. Passwort für root (hicom) ändern. In YaST IP-Adresse von SLES (default 192.168.0.2) einstellen, Zeitserver in gleicher Weise wie in Host einstellen, eventuell Keyboard von englich auf deutsch umstellen (wegen Sonderzeichen im Passwort).

3) Verbindung zur OpenScape 4000 Plattform Administration (Portal) über YaST. Dort den LAN Assistenten aufrufen. Der LAN Wizard enthält die Initial Config für IPDA:

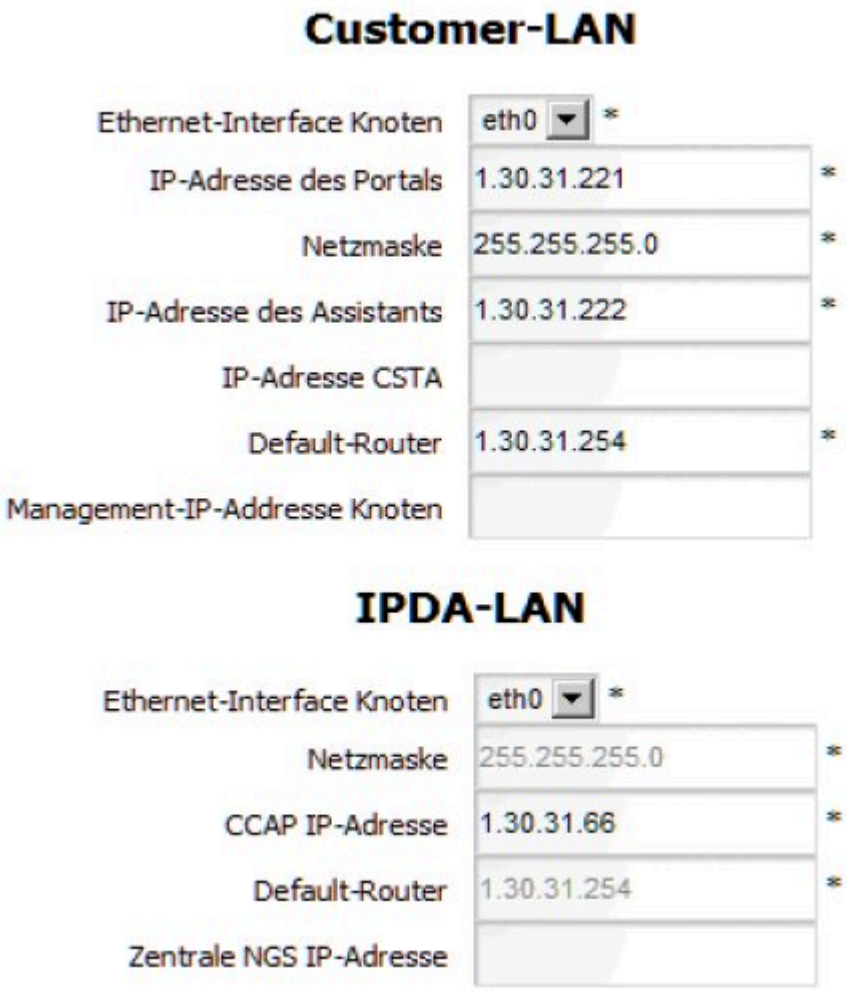


LAN Assistent - Deployment auswählen für AP Emergency Installation

Dann Im LAN Assistent die IP-Adresse des Portals und des OpenScape 4000 Assistants konfigurieren. Bitte beachten, dass es sich hierbei um Adressen des APEs handelt und nicht etwa um Adressen des Hosts.

Falls erforderlich, Default Router konfigurieren.

Unter IPDA-LAN wird die IP-Adresse des APEs eingetragen.



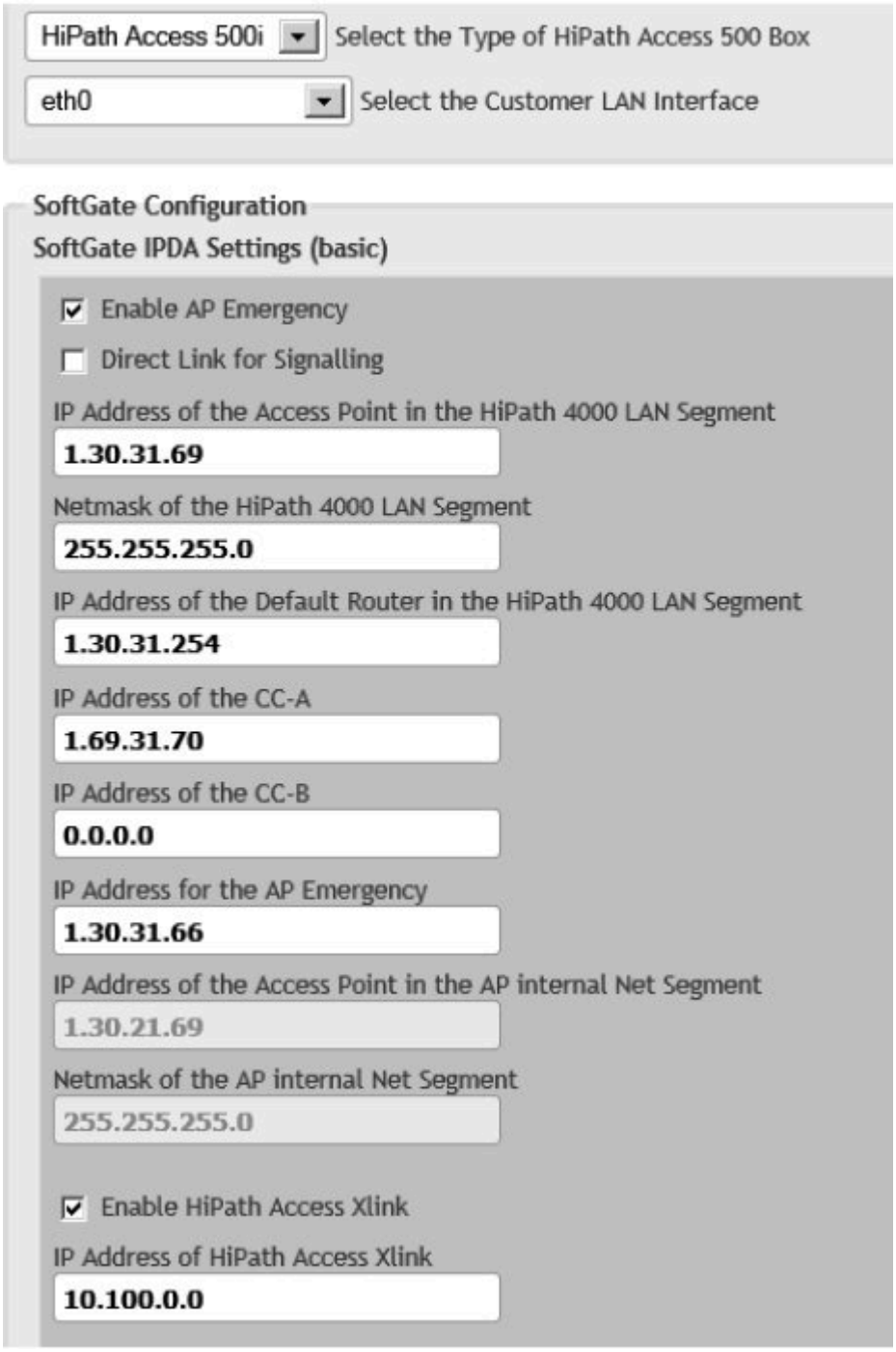
LAN Assistent - Customer LAN und IPDA LAN Adressen eingeben

Im Abschnitt **Internes LAN** muss darauf geachtet werden, dass die Checkbox **AMO-Initialisierungs-Kommandos senden** angekreuzt ist. Es werden dadurch die RMX-Konfigurations-AMOs automatisch konfiguriert.



LAN Assistent - AMO-Initialisierungs-Kommandos senden

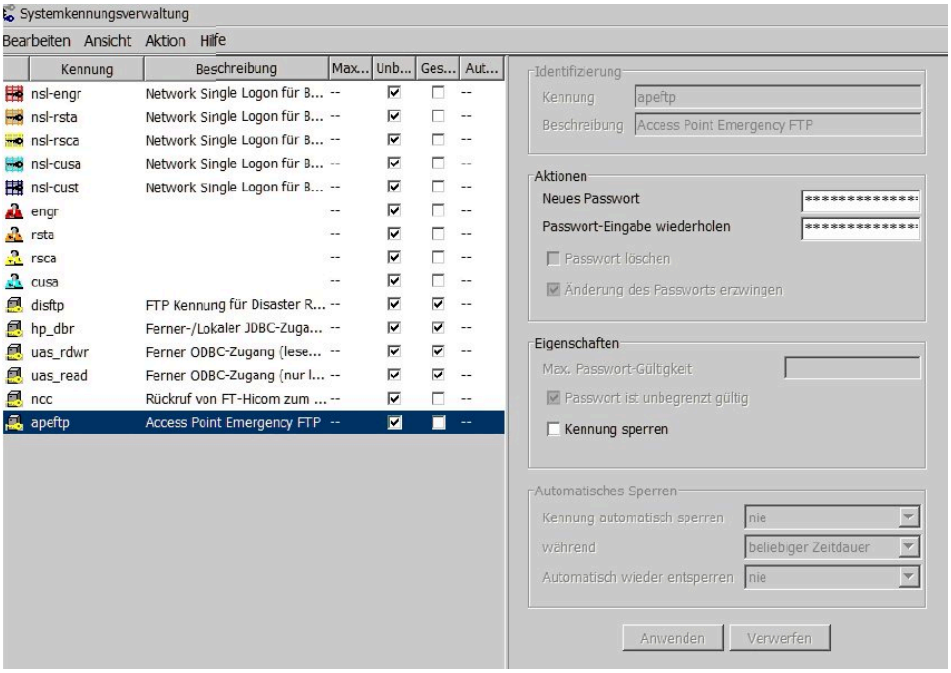
Dann den IPDA-Rahmen (hier als OpenScape 4000 SoftGate im Access 500) konfigureren.



IPDA Rahmen konfigurieren

Schritt 2: Benutzerkennung des FTP-Users einrichten (apeftp)

Der User für den FTP Transport (apeftp) muss auch im CC-AP aktiviert und mit dem gleichen Passwort wie im Host konfiguriert werden.

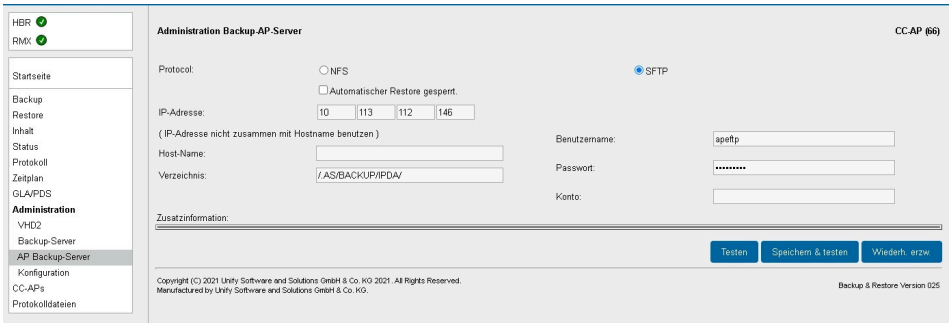


Systemkennung apeftp im CC-AP konfigurieren

Schritt 3: Im CC-AP FTP Backup für APE konfigurieren

Im OpenScape 4000 Assistant vom CC-AP den FTP-Server für den APE-Backup konfigurieren. Die Einträge sind dieselben wie im Host.

Mit **Speichern & testen** wird die Synchronisation des CC-APs sofort gestartet.



AP Backup Server im CC-AP einrichten

Schritt 4: Status abfragen

Den Fortschritt sieht man auf der Statusseite des HBRs. Bei der Erstinstallation startet der CC-AP mit einem Backup, damit er einen Vergleich zum Backup des Hosts hat. Sofort im Anschluss beginnt der CC-AP mit einem Restore, der dann mit einem Reload abgeschlossen wird. Anschließend geht der CC-AP automatisch in Betrieb. Im Normalbetrieb führt der CC-AP nur noch Restores durch. Dazu nimmt der CC-AP alle 10 Minuten Kontakt zum AP Backup-Server auf, und prüft, ob ein neues, vollständiges Backup-Set vorliegt, um dann die veränderten Teile des Backup-Sets herunterzuladen und zu aktivieren.

Die Dauer des Restore-Vorgangs hängt stark von der zu übertragenden Datenmenge und von der zwischen AP Backup-Server und CC-AP verfügbaren Übertragungsbandbreite ab. Der Vorgang dauert eine halbe Stunde, kann aber auch kürzer sein, wenn nur Änderungen im RMX erfolgten.

HBR-Status: Idle

Operation: Restore
Typ: AP Emergency
Modus: Auto
Archiv: AP Backup-Server
Startzeit: 2012-06-21 22:40:37
Geschätzte Zeit: 00:44:59
Verstrichene Zeit: 00:13:25
Restlaufzeit: 00:00:00

Einheit	Status	Geschätzte Zeit	Verstrichene Zeit	Zusatzinformation
Fetch	Erfolgreich	00:30:25	00:01:44	
RMX	Erfolgreich	00:13:41	00:09:14	logfile
UNIX	Erfolgreich	00:00:53	00:02:27	logfile
Retr	Erfolgreich	---	---	(Restore Gesamt-Status)
				common logfile

Backup-Status prüfen

Schritt 5: APE-Status ausgeben

```
ABFRAGEN-APESU;
```

H500: AMO APESU GESTARTET

```
+------------------------------------------------------------------
+

| AKTUELLE SYSTEMZEIT  : 22-06-2012 10:38:14
                   |

+------------------------------------------------------------------
+



+------------------------------------------------------------------
+

| CC-AP: 99
         IP ADRESSE: 1
.30 .31 .66                |


+------------------------------------------------------------------
+

+------------------------------------------------------------------
+

| AP EMERGENCY GRUPPE: 1    CC-AP: 99          NAME: HPA
 MUC                    |

| SCHWELLE: 0          RSMODE: AUTO
                     |
```

```
| STABIL: 5   MIN     RSBEGIN: 20 H     RSENDE: 6  H
 RSOFFSET: 15 MIN      |

+-------------------------------------------------------------------
+

| AP: 98  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0
  UMSCHALT: GRUPPE  |

| KONTROLL-EINHEIT: HOST-CC     SIGNAL-PFAD: LAN
                    |

| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                    |

|
                    |

|     HOST-CC:  VERBUNDEN: JA        VERBUNDEN SEIT:
 22-06-2012  10:07         |

|     CC-AP:    VERBUNDEN: JA        VERBUNDEN SEIT:
 22-06-2012  10:07         |

+-------------------------------------------------------------------
+

| AP: 99  AP EMERGENCY GRUPPE: 1   CC-AP: 99  GEWICHT: 0
  UMSCHALT: GRUPPE  |

| KONTROLL-EINHEIT: HOST-CC     SIGNAL-PFAD: LAN
                    |

| LETZTE AUFGEZEICHNETE VERBINDUNGS-STATUS-AENDERUNG:
                    |

|
                    |

|     HOST-CC:  VERBUNDEN: JA        VERBUNDEN SEIT:
 22-06-2012  10:08         |

|     CC-AP:    VERBUNDEN: JA        VERBUNDEN SEIT:
 22-06-2012  10:08         |

+-------------------------------------------------------------------
+
```

11.7.5 Verifizieren / Abnahme der AP-Emergency Konfiguration

Es ist unbedingt erforderlich, dass die Funktionalität der AP-Emergency Konfiguration nach der Erstinbetriebnahme, bzw. nach wesentlichen Modifikationen durch einen Abnahme/Übergabetest verifiziert wird.

Dazu muss jede Emergency Gruppe einmal administrativ zum CC-AP umgeschaltet werden. Im Emergency-Betrieb muss dann geprüft werden, ob die Kommunikation ins Amt, zu anderen Anlagen im Netz und auch die Kommunikation zwischen Emergency Gruppen an unterschiedlichen CC-APs wie geplant funktioniert. Beziehen Sie gegebenenfalls auch installierte Applikationen, die den Emergency-Betrieb unterstützen, mit in den Test ein.

Prüfen Sie auch die Kommunikationsfähigkeit von Access Points, die unabhängig von der Emergency Gruppe zum CC-AP geschaltet werden können, wenn die Gruppe im Normalbetrieb läuft.

Die Tests können in betriebsschwachen Zeiten durchgeführt werden.

Folgende manuelle Schaltmöglichkeiten stehen zur Verfügung:

- alle Access Points aller Emergency Gruppen aller CC-APs im System
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=SYST;` schaltet zum CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=SYST;` schaltet zur zentralen Steuerung
- alle Access Points aller Emergency Gruppen eines CC-APs
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=CCAP,NUMMER=17;` schaltet zum CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=CCAP,NUMMER=17;` schaltet zur zentralen Steuerung
- alle Access Points einer Emergency Gruppe (eines CC-APs)
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=APEGRP,NUMMER=1;` schaltet zum CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=APEGRP,NUMMER=1;` schaltet zur zentralen Steuerung
- ein Access Point (einer Emergency Gruppe (eines CC-APs)
- `EXEC-APESU:SYSMODE=EMERG,LEVEL=AP,NUMMER=17;` schaltet zum CC-AP

  `EXEC-APESU:SYSMODE=NORMAL,LEVEL=AP,NUMMER=17;` schaltet zur zentralen Steuerung

11.8 FAQ - Häufig gestellte Fragen

1) **Frage:** Ein OpenScape 4000 System mit IPDA und AP-Emergency zerfällt bei Ausfall der Zentralanlage in 5 Inseln. Jede Insel wird von einer Survivability Unit gesteuert. Kann die Kommunikation zwischen den Inseln über IP erfolgen, solange das IP-Netz das hergibt?

2) **Antwort:** Nein. Jede Insel stellt im Emergency Mode eine eigenständige Anlage dar. Diese Anlagen kommunizieren ausschließlich über Amts- bzw. Querleitungen.

   Nachfrage: Wenn ich also IP-Trunking zwischen den Inseln einrichte, geht das also.

   Antwort: Im Prinzip ja, aber Sie können IP-Trunking nicht ausschließlich für den Emergency Fall einrichten. Es muss in der Zentralanlage konfiguriert werden und ist dann auch während der Normalbetriebs vorhanden. Hier müssen Sie besonders darauf achten, dass es sich im Normalbetrieb dann um Querverbindungen innerhalb einer Anlage handelt, was bezüglich LCR nur sehr schwer in Griff zu kriegen ist. Daher wird von solchen Szenarien ausdrücklich abgeraten.
3) **Frage**: Ist das Survivable OpenScape 4000 SoftGate (OpenScape Access 500 a/i) in der Lage die Steuerung für die lokale OpenScape 4000 SoftGate Maschine zu übernehmen (Survival Mode) im Falle eines lokalen LAN Ausfalls (L1/eth0 down)?
4) **Antwort**: Ja. Auf einer OpenScape Access 500 Hardware kann das Routing der Signalisierung (HSR) über einen internen Weg gehndhabt werden (Rückwand), d.h. es wird kein externes LAN benötigt. Wenn OpenScape Access Module über Xlink angeschlossen sind, werden auch diese weiterarbeiten.
5) **Frage**: Können Minor/Fixed Release-Upgrades mit APEs und Survivable OpenScape 4000 SoftGates per Festplattenwechsel durchgeführt werden?
6) **Antwort**: Beachten Sie, dass beim Upgrade eines Systems im Hauptsystem per Festplattenwechsel die OpenScape 4000 Plattform Administration (Portal), OpenScape 4000 CSTA und OpenScape 4000 Assistant[4] an APEs und Survivable OpenScape 4000 SoftGates nicht automatisch aufgerüstet werden.

   Unter diesen Umständen sind zwei Vorgehensweisen möglich, um sicherzustellen, dass die APEs und die Survivable OpenScape 4000 SoftGates hinterher die richtige Software erhalten:

   a) Die neue Hostsystem-Festplatte für das Kunden-Upgrade sollte mit der Version des vorhandenen Kunden-Softwarestands vorbereitet und anschließend per SWA/SWT auf die vom Kunden benötigte Version aufgerüstet werden. Dadurch ist gewährleistet, dass der Upgrade-Verlauf auf der neuen Festplatte vorhanden ist und beim nächsten HBR für das APE/Survivable OpenScape 4000 SoftGate die richtigen Pakete übertragen und die OpenScape 4000 Plattform Administration (Portal), OpenScape 4000 CSTA und OpenScape 4000 Assistant[4] automatisch auf die richtigen Versionen aktualisiert werden.

   Nach der Installation der neuen Festplatte mit einer neueren Version durch die Erstinstallation würde RMX lediglich auf den APEs/Survivable OpenScape 4000 SoftGates aufgerüstet. Die vorhandenen Versionen von OpenScape 4000 Plattform Administration (Portal), OpenScape 4000 CSTA und OpenScape 4000 Assistant 1 hingegen werden aufgrund des fehlenden Upgrade-Verlaufs nicht aktualisiert. Nachdem das Fix Release/Maintenance Release übertragen und per SWT/SWA auf den einzelnen APEE/Survivable

[4] Hinweis: Das OpenScape 4000 Assistant-Upgrade kann mit Option I in HBR erzwungen werden. Dies wird allerdings nicht als Standard empfohlen und bewirkt, wie im Servicehandbuch bereits angemerkt, kein Upgrade der OpenScape 4000 Plattform Administration (Portal) oder OpenScape 4000 CSTA.

OpenScape 4000 SoftGates individuell aktiviert wurde, werden alle weiteren Hot Fixes automatisch mit dem nächsten HBR aktiviert.

Wichtig: Linux-Host OpenScape 4000 Plattform Administration (Portal) (PLT) und OpenScape 4000 CSTA sind in diesem Backup nicht enthalten. Wenn das Hostsystem durch Wechseln der Systemfestplatte aktualisiert wird, müssen die einzelnen angeschlossenen APEs/ Survivable OpenScape 4000 SoftGates daher entweder neu installiert oder mit RLC derselben Version als neue Hostfestplatten aktualisiert werden.

Wichtig: Dies gilt natürlich nicht für Upgrades bei denen eine Neuinstallation erforderlich ist. Nach der Installation des zentralen Hosts mit der OpenScape 4000-Software würde nur RMX auf OpenScape 4000 APEs/Survivable OpenScape 4000 SoftGates repliziert, OpenScape 4000 Plattform Administration (Portal), OpenScape 4000 Assistant und OpenScape 4000 CSTA jedoch nicht aktualisiert. Deshalb müssen die APEs/Survivable OpenScape 4000 SoftGates neu installiert und anschließend mit dem zentralen Host synchronisiert werden.

---

7) **Frage**: Sollten Hot Fixes auf APEs und Survivable OpenScape 4000 SoftGates aktiviert werden?
8) **Antwort**: Gemäß den Hinweisen zur Aktivierung der grafischen SWA-Benutzeroberfläche:

   Achtung: Hot Fixes und FR/MR sollten nicht direkt auf APE-Knoten aktiviert werden.

   Vielmehr sollten Software-Updates auf dem Hostsystem aktiviert und bei der nächsten APE-Wiederherstellung auf die APE-Knoten gespiegelt werden.

   Eine direkte Aktivierung auf APE sollte nur in seltenen Fällen bei der Erstinstallation oder einem manuellen Upgrade durchgeführt werden.

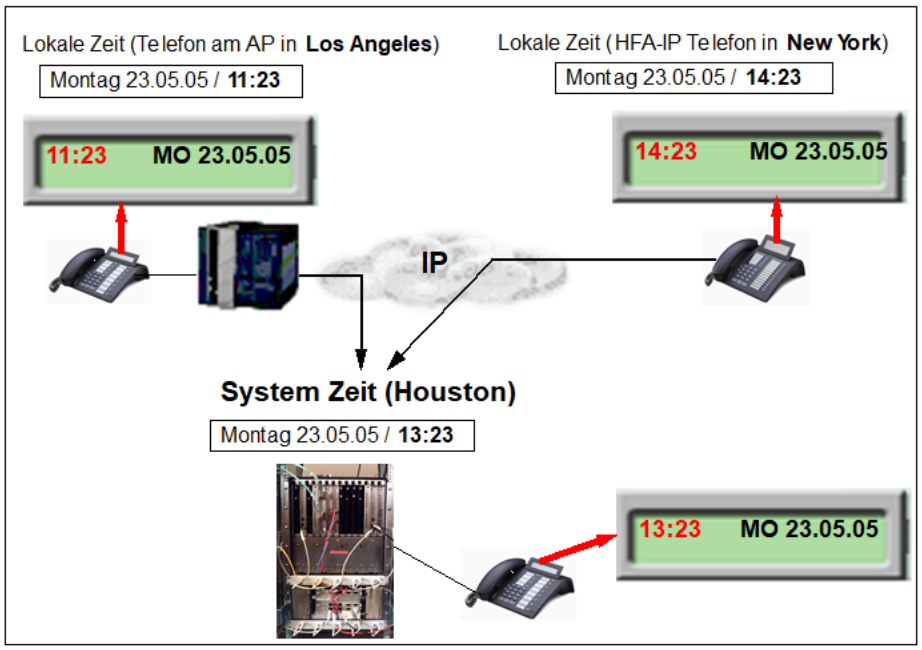
12 Verschiedene Zeitzonen - Different Time Zones (DTZ)

12.1 Leistungsmerkmalbeschreibung

Das Leistungsmerkmal „IPDA Different Time Zones (DTZ)“ berücksichtigt die Situation, dass sich ein IPDA-Shelf bzw. Access Point (AP-IP) oder HFA-IP Telefone in anderen Zeitzonen als das Host-System befinden können. In diesen Fällen soll statt der Systemzeit die lokale Tageszeit im Display der digitalen Telefone, die mit dem Remote-AP verbunden sind, bzw. im Display der HFA-IP Telefone angezeigt werden.

Beispiel für die Anzeige der lokalen Zeit:

Ein OpenScape 4000 System in Houston (Texas) hat einen Remote-AP in Los Angeles (Kalifornien). Ferner befindet sich ein HFA-IP Telefon in New York (New York). Alle Telefone sollen jeweils die lokale Uhrzeit anzeigen.



Beispiel für verschiedene Zeitzonen

Die lokale Zeit wird für folgende Funktionen unterstützt:

1) Datum und Tageszeit im Ruhe-Display

2)
- Sommer- und Winterzeit
- Anrufliste
- Rückrufe
- Datum/Zeit Taste
- Datum-Wechsel um Mitternacht

12.2 Service Information

In der OpenScape 4000 können bis zu 50 Zeitklassen über den AMO SIPCO eingerichtet werden. Die lokalen Zeiten haben einen festen Offset (in Minuten: West oder Ost) zur System Zeit.

Mit dem AMO UCSU kann einem IPDA-Shelf eine Zeitklasse zugeteilt werden. Damit benutzen alle Digites mit Display, die an diesem Shelf konfiguriert sind, diese Zeitklasse.

Mit dem AMO SDAT wird einem HFA Teilnehmer eine Zeitklasse zugewiesen. Wenn ein HFA Teilnehmer an einem IPDA-Shelf konfiguriert ist und keine Zeitklasse mit dem AMO SDAT zugewiesen bekommen hat, wird die Zeitklasse des IPDA-Shelfs benutzt. Sobald dieser HFA Teilnehmer mit dem AMO SDAT eine Zeitklasse erhält, wird die Zeitklasse des IPDA Shelfs für diesen Teilnehmer ignoriert.

Das Netz muss auch in AMO SIPCO definiert sein, wenn nur HFA-Teilnehmer in einer anderen Zeitzone konfiguriert sind.

- Zuvor müssen die Zeitzonen im IPDA-Wizard in OpenScape 4000 Assistant im folgenden Menü konfiguriert werden: Configuration Management > Anlagendaten > IPDA > IPDA-Daten
- Die Zeitklasse (TCLASS) in AMO SDAT kann nur bei HFA-Teilnehmern geändert werden.

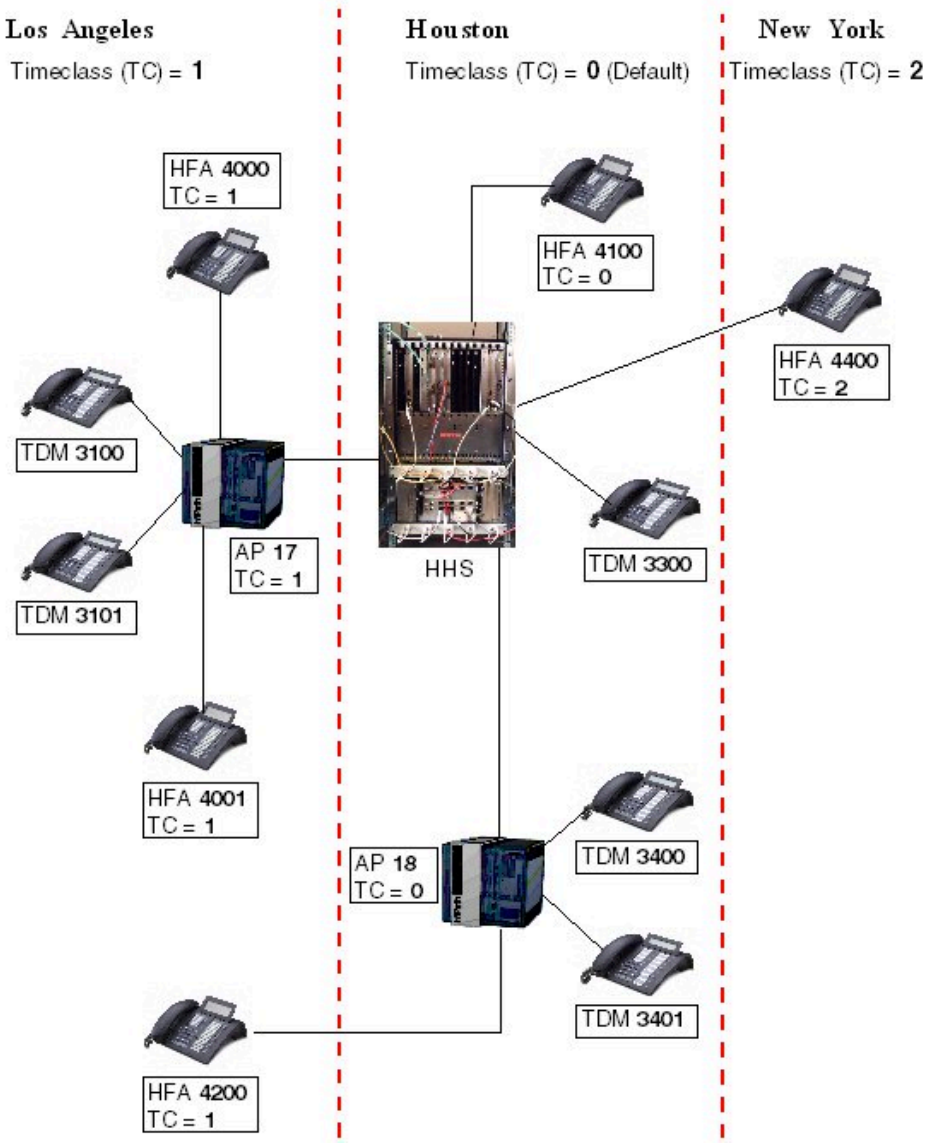
Einschränkungen

- „HFA Mobile User“ wird nicht vollständig unterstützt. Ein Benutzer erhält im Display die Zeit der Zeitzone, die der Rufnummer beim Einrichten zugewiesen wurde - auch wenn er sich in einer anderen Zeitzone angemeldet hat.
- Termine werden für Telefone mit Zeitklasse /= 0 nicht unterstützt. Wenn ein Telefon keine lokale Zeitklasse konfiguriert hat, ist die Terminfunktion blockiert.
- Die Gebührenerfassung erfolgt in Systemzeit.
- Fehlermeldungen werden in Systemzeit ausgegeben.
- Im Falle ein APE (CCAP) übernimmt die Kontrolle, so agiert er anstelle des Rechners im Hostsystem (CCA/CCB) mit einer Kopie der Datenbasis des OpenScape 4000 Host-Systems. Ist das Leistungsmerkmal „Verschiedene Zeitzonen“ (AMO TCLASS) konfiguriert bzw. sind OpenScape 4000 Host-System & Access Points über verschiedenen Zeitzonen verteilt, so muss der APE (CCAP) die selbe Zeit wie der OpenScape 4000 Host-System (CCA/CCB/ADP) eingestellt haben, um eine korrekte Zeitanzeige im Falle von APE-Emergency (CC-AP hat die Kontrolle übernommen) zu gewährleisten.

12.3 Generierungsbeispiel

- Das folgende Beispiel deckt verschiedene DTZ-Konfigurationsmöglichkeiten ab:
- – Das HHS steht in Houston, Texas, und hat zwei AP-Shelfs konfiguriert. Die HFA-Teilnehmer 4000 und 4001 sind im AP-Shelf 17 konfiguriert, welches sich in Los Angeles befindet und der Zeitklasse 1 zugeordnet ist. Aufgrund der verschiedenen Zeitzonen bekommt das AP-Shelf 17 die Zeitklasse 1, welche eine Verschiebung von zwei Stunden nach Westen vorsieht.

  - Der HFA-Teilnehmer 4100 befindet sich in Houston und ist direkt auf dem HHS konfiguriert. Das AP-Shelf 18 befindet sich ebenfalls in Houston (Direct Link). Weder das AP-Shelf 18, noch der direkt auf dem HHS konfigurierte Teilnehmer benötigen eine spezielle Zeitklasse - die Defaulteinstellungen reichen vollkommen aus.
  - Der HFA-Teilnehmer 4400 ist zwar im HHS auf einer Baugruppe in Houston konfiguriert, befindet sich räumlich aber in New York. Dieser Teilnehmer bekommt die Zeitklasse 2, welche eine Zeitverschiebung von einer Stunde in östlicher Richtung bedeutet.
  - Der HFA-Teilnehmer 4200 ist zwar im AP-Shelf 18 in Houston konfiguriert, befindet sich räumlich jedoch in Los Angeles. Somit ist es nötig, dem Teilnehmer 4200 die Zeitklasse 1 zuzuweisen. Befände sich der Teilnehmer in New York, müsste ihm die Zeitzone 2 zugewiesen werden.
  - Alle TDM-Teilnehmer bekommen die Zeitklasse entsprechend ihrer Anschlußkonfiguration. Teilnehmer 3100, 3101, 3400 und 3401 erhalten die Zeitklasse aus der AP-Shelf-Konfiguration (AMO UCSU). Der Teilnehmer 3300 bekommt die Systemzeit.
  - Weiters könnte ein HFA-Teilnehmer auch im AP 17 (in Los Angeles) konfiguriert sein, sich aber räumlich in New York befinden. Dann müsste für diesen Teilnehmer im AMO SDAT die Zeitklasse 2 konfiguriert werden. Diese Konfiguration wird in diesem Beispiel nicht mehr weiterverfolgt.
- Übersichtsbild der Konfiguration:



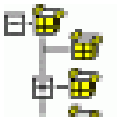
12.3.1 Einrichten der Zeitklassen

- Die für das Beispiel nötigen Zeitklassen werden im AMO SIPCO konfiguriert.

- Zeitklasse 1, Los Angeles, mit automatischer Sommer-Normalzeitumschaltung minus 2 Stunden relativ zu Houston (Systemzeit).

  In dieser Zeitklasse erfolgt die Umschaltung zwischen Sommer- und Normalzeit automatisch am letzten Sonntag im März um 2:30 nachts bzw. am letzten Sonntag im Oktober um 3:30.

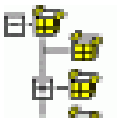
  Die Zeitklasse und die automatische Sommerzeitumschaltung wird folgendermaßen konfiguriert:

	Configuration Management -> Anlagendaten -> IPDA -> IPDA - Anlagendaten
	AENDERN- SIPCO:TYP=TCLASS,TCLASS=1,OFFSET=120,RICHT=WEST, TEXT=â##TIME ZONE: -2H L.A.â##,SONUS=AUTO,MONATSZ=3, WOTAGSZ=SO,TAGNRSZ=LETZTER,STUNDESZ=2,MINSZ=30, MONATNZ=10,WOTAGNZ=SO,TAGNRNZ=LETZTER, STUNDENZ=3,MINNZ=30;

  Zeitklasse 2, New York, mit manueller Sommer-Normalzeitumschaltung plus 1 Stunde relativ zu Houston (Systemzeit).

  In dieser Zeitklasse erfolgt die Umschaltung zwischen Sommer- und Normalzeit am 27. März um 2:00 nachts bzw. am 30. Oktober um 3:00.

  Die Zeitklasse und die manuelle Sommerzeitumschaltung wird folgendermaßen konfiguriert:

	Configuration Management -> Anlagendaten -> IPDA -> IPDA - Anlagendaten
	AENDERN- SIPCO:TYP=TCLASS,TCLASS=2,OFFSET=60,RICHT=OST, TEXT=â##TIME ZONE: +1H N.Y.â##,SONUS=MAN,MONATSZ=3, TAGSZ=27,STUNDESZ=2,MINSZ=0,MONATNZ=10,TAGNZ=30, STUNDENZ=3,MINNZ=0;

- Die Konfiguration der Zeitklassen sieht nun folgendermaßen aus:
- ABFRAGEN-SIPCO:TYP=TCLASS;

```
TIME CLASS DATUM:

 ---------------------------------------------------------------
```

```
  +------+-----------+-----------+-------------------
+--------+

  |INDEX |   OFFSET   |    RICHT   |        TEXT
 | SONUS  |

  +------+-----------+-----------+-------------------
+--------+

  |   1  |     120    |    WEST    |TIME ZONE: -2H L.A.
 | AUTO   |

  +------+-----------+-----------+-------------------
+--------+

  |   2  |      60    |     OST    |TIME ZONE: +1H N.Y.
 |  MAN   |

  +------+-----------+-----------+-------------------
+--------+

  +------+-----+-------+----------+----------+--------
+--------+

  |INDEX |     | MONAT | WOCHENTAG | TAGNUMMER | STUNDE
 | MINUTE |

  +------+-----+-------+----------+----------+--------
+--------+

  |   1  |SZ:  |   3   |    SO     |  LETZTER  |    2
 |   30   |

  |   1  |NZ:  |  10   |    SO     |  LETZTER  |    3
 |   30   |

  +------+-----+-------+----------+----------+--------
+--------+

  +------+-----+----------+-----------+-----------
+-----------+

  |INDEX |     |   MONAT   |     TAG    |   STUNDE   |
 MINUTE   |

  +------+-----+----------+-----------+-----------
+-----------+

  |   2  |SZ:  |     3     |     27     |      2     |
   0     |

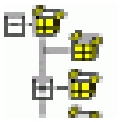
  |   2  |NZ:  |    10     |     30     |      3     |
   0     |

  +------+-----+----------+-----------+-----------
+-----------+
```

12.3.2 Zuweisen der Zeitklassen zu einem AP-Shelf

- Das im Beispiel konfigurierte AP-Shelf 17 benötigt eine Zeitklasse, da an ihr Teilnehmer konfiguriert sind, die ihre Zeitklasse vom AP-Shelf beziehen.
- **Zuweisen der Zeitklasse 1 zum AP-Shelf 17.**

  Die Zeitklasse wird über den neuen Parameter TCLASS im AMO UCSU konfiguriert:

	Configuration Management -> Anlagendaten -> IPDA -> IPDA Access Point

	`EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=17,`
	
	`LTSACHNR=âQ2305-X40`
	`",SRCGRP=17,FRAMETYP=INCH19,`
	
	`VERBART=APDL,LSRTADR=198.16.16.63,`
	
	`APRTADR=198.16.16.150,STANDOID=017,`
	
	`STANDORT=âLOS`
	`ANGELESâ,TEL=3140,FAX=3141,PLCHECK=JA,`
	
	`ANZBKAN=120,KONVLAW=NEIN,TCLASS=1;`

- Das AP-Shelf 18 bekommt keine eigene Zeitklasse zugewiesen, daher wird der Parameter TCLASS nicht angegeben. Das AP18 arbeitet somit mit der Default-Zeitklasse 0 (keine zusätzliche Berechnung der Display-Anzeige bzgl. Zeitzonen).

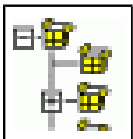
Wichtig: Soll die Zeitklasse des Shelfs geändert werden, so muss dieses vorher mit dem AMO USSU ausgeschaltet und nach dem Ändern wieder eingeschaltet werden.

12.3.3 Zuweisen der Zeitklassen zu einem HFA-Teilnehmer

- Den im Beispiel konfigurierten HFA-Teilnehmern 4200 und 4400 muss eine Zeitklasse zugewiesen werden.

- Zuweisen einer Zeitklasse für HFA-Teilnehmer mit AMO SDAT.

  Nachdem die HFA-Teilnehmer mittels AMO SBCSU (OPTIIP) eingerichtet wurden, wird die Zeitklasse über den neuen Parameter TCLASS im AMO SDAT konfiguriert:

	Configuration Management -> Anschluss -> Teilnehmeranschluss
	AENDERN- SDAT:TLNNU=4400,TYP=DATEN1,KNNR=1-1-100,TCLASS=2; AENDERN- SDAT:TLNNU=4200,TYP=DATEN1,KNNR=1-1-100,TCLASS=1;

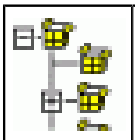
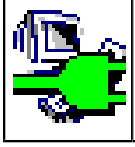
- Die HFA-Teilnehmer 4000, 4001 und 4100 bekommen keine Zeitklasse mit dem AMO SDAT zugewiesen.
- – Für HFA-Teilnehmer 4000 wird die Berechnung über die Zeitklasse des AP-Shelfs gesteuert, in der sie aktuell angemeldet sind (hier AP 17, daher Zeitklasse 1)
  – HFA-Teilnehmer 4100 ist direkt beim angemeldet und benötigt daher keine Zeitklasse. Das Display ist immer an die HHS-Zeit angepasst.
- Teilnehmer 4200 ist in AP-Shelf 18 (Systemzeit) konfiguriert. Teilnehmer 4200 ist in Zeitklasse 1, die von AMO SDAT zugeordnet wurde.
- HFA-Teilnehmer 4400 ist auf dem Host konfiguriert und ihm wurde mit AMO SDAT Zeitklasse 2 zugeordnet.
- Die konfigurierten Zeitklassen werden immer auf Teilnehmerebene von AMOs SDAT und SBCSU angezeigt.
- Nur einem HFA-Teilnehmer kann eine Zeitklasse mittels AMO SDAT zugewiesen werden. Wenn einem HFA-Teilnehmer mit AMO SDAT die Zeitklasse 0 zugeordnet ist, gilt für diesen Teilnehmer die Zeitklasse des AP-Shelf.

12.3.4 Löschen einer Zeitklasse

- Eine Zeitklasse kann gelöscht werden, indem der Zeitoffset und die Richtung auf die Initialisierungswerte gesetzt werden.

- Löschen der Zeitklasse 1.

  Der Offset und die Richtung werden zurückgesetzt, um die Zeitklasse zu löschen:

	Configuration Management -> Anlagendaten -> IPDA -> IPDA - Anlagendaten
	AENDERN- SIPCO:TYP=TCLASS,TCLASS=1,OFFSET=0,RICHT=KEINE;

  Wichtig: Alle Teilnehmer mit Zeitklasse 1 benutzen jetzt Systemzeit!

- Die Konfiguration der Zeitklassen sieht nun folgendermaßen aus:
- ABFRAGEN-SIPCO:TYP=TCLASS;

```
TIME CLASS DATUM:

 ---------------------------------------------------------------------

  +------+------------+------------+--------------------
+--------+

  |INDEX |   OFFSET   |    RICHT   |        TEXT
 | SONUS  |

  +------+------------+------------+--------------------
+--------+

  |   2  |      60    |     OST    |TIME ZONE: +1H N.Y.
 |  MAN   |

  +------+------------+------------+--------------------
+--------+

  +------+-----+----------+-----------+-----------
+-----------+

  |INDEX |     |   MONAT   |     TAG    |   STUNDE   |
 MINUTE   |

  +------+-----+----------+-----------+-----------
+-----------+

  |   2  |SZ:  |     3     |     27     |      2     |
    0    |

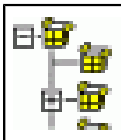
  |   2  |NZ:  |    10     |     30     |      3     |
    0    |

  +------+-----+----------+-----------+-----------
+-----------+
```

12.3.5 Löschen der Sommerzeitumschaltung

- Mit einem AMO-Parameter können Sie die Berücksichtigung der Sommerzeit in der Zeitklasse deaktivieren.
- Deaktivieren Sie die Berechnung der Sommerzeit in der Zeitklasse 2.

  Der Offset und die Richtung werden zurückgesetzt, um die Zeitklasse zu löschen.

	Configuration Management -> Anlagendaten -> IPDA -> IPDA - Anlagendaten
	`CHANGE-SIPCO:TYPE=TCLASS,TCLASS=2,DSTSW=OFF;`

- Die Konfiguration der Zeitklassen sieht nun folgendermaßen aus:
- `ABFRAGEN-SIPCO:TYP=TCLASS;`

```
TIME CLASS DATUM:

 ------------------------------------------------------------------

  +------+------------+------------+--------------------
+--------+

  |INDEX |   OFFSET   |    RICHT   |        TEXT
 | SONUS  |

  +------+------------+------------+--------------------
+--------+

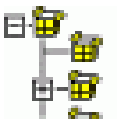
  |   2  |      60    |     OST    |TIME ZONE: +1H N.Y.
 |  AUS   |

  +------+------------+------------+--------------------
+--------+
```

12.3.6 Ändern von System-Zeit/Datum mit AMO DATE

Wichtig: Der Parameter Mode (SZ/ NZ) muss für DTZ angegeben werden, da es sonst bei den Telefonen zu falschen Zeitanzeigen kommen kann.

Ändern von System-Zeit/Datum

	Basis Administration -> Unix Basis Administration -> Datum/ Uhrzeit Kommentar: Derzeit kann der Parameter MODE nur über RMX eingegeben werden.
	`AENDERN-` `DATE:JAHR=2005,MONAT=7,TAG=20,STUNDE=14,MINUTE=30,MODE=SZ;`

- Anzeige von System-Zeit/Datum:
- `ABFRAGEN-DATE;`

```
+-----------------------------+
| MITTWOCH                    |
| DATUM:           UHRZEIT:   |
| 2005-07-20       14:30:34   |
|                             |
| LAUFENDE TAGESNUMMER: 201   |
| SOMMERZEIT                  |
| GMTRTG:       ZEITDIFF:0    |
+-----------------------------+
```

12.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
DATE	MODE	d	Zeit-Modus
	MODE	e	Mode of time
	SZ	d	Sommerzeit
	DST	e	Daylight Saving Time
	NZ	d	Normalzeit
	NT	e	Normal Time
UCSU	TCLASS	d	Zeitklasse des AP-Shelfs
	TCLASS	e	Time class of the AP shelf
SDAT	TCLASS	d	Zeitklasse des Teilnehmers
	TCLASS	e	Time class of the subscriber
SIPCO	TCLASS	d	Zeitklasse
	TCLASS	e	Time class
	OFFSET	d	Zeit-Offset (Minuten)
	OFFSET	e	Time offset (minutes)

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	RICHT	d	Richtung (WEST/OST/KEINE)
	DIRECT	e	Direction (WEST/EAST/NONE)
	TEXT	d	Beschreibung der Zeitklasse
	TEXT	e	Time class description
	SONUS	d	Sommer-/Normalzeit-Umschaltung (AUTO/MAN/AUS)
	DSTSW	e	Daylight savings time switching (AUTO/ MAN/OFF)
	MONATSZ	d	Monat der Sommerzeitumschaltung
	MONTHDST	e	Month of switching to daylight savings time
	WOTAGSZ	d	Wochentag der Sommerzeitumschaltung
	WKDAYDST	e	Weekday of switching to daylight savings time
	TAGNRSZ	d	Tagesnummer der Sommerzeitumschaltung
	DAYNODST	e	Day number of switching to daylight savings time
	STUNDESZ	d	Stunde der Sommerzeitumschaltung
	HOURDST	e	Hour of switching to daylight savings time
	MINSZ	d	Minute der Sommerzeitumschaltung
	MINDST	e	Minute of switching to daylight savings time
	MONATNZ	d	Monat der Normalzeitumschaltung
	MONTHNT	e	Month of switching to normal time
	WOTAGNZ	d	Wochentag der Normalzeitumschaltung
	WKDAYNT	e	Weekday of switching to normal time
	TAGNRNZ	d	Tagesnummer der Normalzeitumschaltung
	DAYNONT	e	Day number of switching to normal time
	STUNDENZ	d	Stunde der Normalzeitumschaltung

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	HOURNT	e	Hour of switching to normal time
	MINNZ	d	Minute der Normalzeitumschaltung
	MINNT	e	Minute of switching to normal time
	TAGSZ	d	Tag der Sommerzeitumschaltung
	DAYDST	e	Day of switching to daylight savings time
	TAGNZ	d	Tag der Normalzeitumschaltung
	DAYNT	e	Day of switching to normal time

13 Signaling Survivability

13.1 Leistungsmerkmalbeschreibung

IP Distributed Architecture ist eine Architektur mit einer Zentrale und vielen „unintelligenten“ Außenstellen. Ein Access Point/OpenScape 4000 SoftGate wird weitgehend von der Zentrale ferngesteuert. Fällt die Steuerungsverbindung aus, so ist der Access Point/OpenScape 4000 SoftGate für sich nicht überlebensfähig. Er muss Signalisierungsmeldungen von den Peripheriebaugruppen an die Zentrale weiterleiten. Er kann sie selber nicht verarbeiten. Deshalb bleibt dem Access Point/OpenScape 4000 SoftGate nach Verlust der Steuerungsverbindung zur Zentrale nicht anderes übrig, als sich selbst zurückzusetzen und darauf zu warten, dass die Zentrale ihn wieder in Betrieb nimmt.

Fällt also die Steuerungsverbindung zwischen der Zentrale und einem Access Point/OpenScape 4000 SoftGate aus, so kann im Access Point/OpenScape 4000 SoftGate nicht mehr telefoniert werden.

Wegen dieser sehr schweren Konsequenzen eines Ausfalls der Steuerungsverbindung zwischen OpenScape 4000 Zentrale und Access Point/OpenScape 4000 SoftGate wurde eine Möglichkeit geschaffen, derartige Störungen zu „überleben“. Signaling Survivability schaltet im Störungsfall die Steuerungsverbindung vom IP-Netz auf einen alternativen Weg um. Die Umschaltung des Signalisierungspfades erfolgt unterbrechungsfrei.

Gegen einen Ausfall des Zentralsystems hilft Signaling Survivability aber nicht. Ist keine Zentrale mehr verfügbar, um die Access Points/OpenScape 4000 SoftGates zu steuern, hilft auch kein Signalisierungspfad über Amt oder alternatives LAN. In solchen Fällen ist das gesamte Kommunikationssystem einschließlich aller Access Points/OpenScape 4000 SoftGates außer Betrieb.

Mit Signaling Survivability mögliche Gespräche:

- Gespräche innerhalb des Access Points/OpenScape 4000 SoftGates
- voller Leistungsmerkmalumfang
- Amtsgespräche von Teilnehmern im Access Point/OpenScape 4000 SoftGate über lokale Amtsleitungen
- voller Leistungsmerkmalumfang (für Amtsgespräche)
- Gespräche mit Teilnehmern an anderen Access Points/OpenScape 4000 SoftGates, zu denen noch eine IP-Verbindung für die Payload aufgebaut werden kann
- voller Leistungsmerkmalumfang

  Gespräche mit Teilnehmern im Zentralsystem, sowie mit Teilnehmern in Access Points/OpenScape 4000 SoftGates, zu denen keine IP-Verbindung für die Payload aufgebaut werden kann, sind nur möglich, wenn für die betroffenen Komponenten das Leistungsmerkmal „Payload Survivability“

eingerichtet ist. Jedoch auch bei eingerichteter „Payload Survivability“ kann im wesentlichen nur „Basic Call“ Funktionalität sichergestellt werden.

Siehe dazu IP Distributed Architecture > Abschnitt 2.9, „Payload Survivability“.

Signaling Survivability wird als Leistungsmerkmal verkauft und individuell je Access Point/OpenScape 4000 SoftGate eingerichtet.

Für das Leistungsmerkmal Signaling Survivability stehen zwei Alternativen pro Access Point/OpenScape 4000 SoftGate zur Verfügung (siehe auch Abschnitt 1.2, „Was wird als Alternativweg für die Signalisierung verwendet?“):

– Signaling Survivability über das öffentliche Amt
– Signaling Survivability über alternatives LAN

Wichtig: Bitte beachten Sie in diesem Zusammenhang die Verwendung des Leistungsmerkmales „HSR über UDP“ (siehe Abschnitt 1.3, „HSR über UDP“).

13.1.1 Wie wird die Störung erkannt?

Die Steuerungsverbindung (-> Signalisierungsverbindung) zwischen CC und Access Point/OpenScape 4000 SoftGate ist eine TCP-Verbindung. Alternativ kann es sich auch um eine Verbindung mittels UDP-Paketen handeln (Leistungsmerkmal „HSR über UDP“, siehe Abschnitt 1.3, „HSR über UDP“). In diesen UDP-Paketen sind nach wie vor die ursprünglichen TCP-Pakete enthalten. Deshalb können hier beide Verbindungsarten wie eine TCP-Verbindung betrachtet werden.

TCP-Verbindungen (also auch die Steuerungsverbindung zwischen CC und Access Point/OpenScape 4000 SoftGate) werden generell permanent auf deren Funktionieren hin überwacht. Übertragene Pakete werden quittiert. Trifft die Acknowledge nicht innerhalb einer bestimmten Zeit ein, wird das Paket wiederholt. Kann ein Paket, trotz Wiederholung innerhalb einer erweiterten, festgelegten Zeitdauer nicht erfolgreich zugestellt werden (keine Acknowledge innerhalb der festgelegten Zeit), muss der Absender von einem Verbindungs-verlust ausgehen. Auch wenn gerade keine Pakete übertragen werden, prüft TCP, ob die Verbindung funktioniert. Dazu werden dann in bestimmten Abständen „Keep Alive“ Meldungen verschickt, die beantwortet werden müssen.

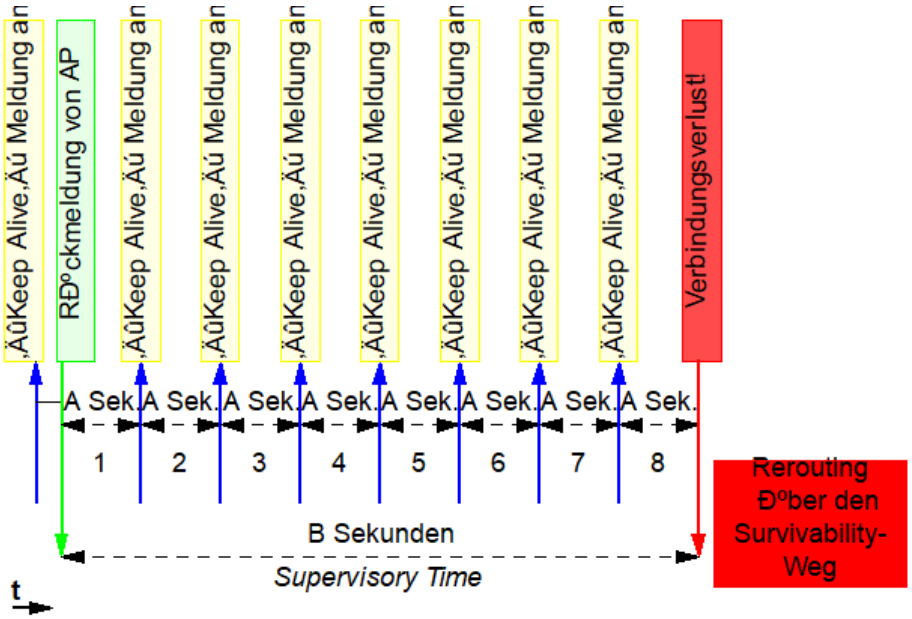
Wird auf einer Signalisierungsverbindung ein Fehler gemeldet, so ist seit dem ersten Indiz bereits eine relativ lange Zeit vergangen (z.B. mehr als 30 Sekunden). Unterstellt man, dass Signalisierungsmeldungen eines OpenScape 4000 Systems innerhalb einer bestimmten Zeit zugestellt werden müssen (z.B. 60 Sekunden), bleibt die Differenz zwischen diesen beiden Zeiten um einen alternativen Weg zu finden, aufzubauen und die Meldung erneut zu übertragen.

Die Zeit kann verkürzt werden, indem man die Zeit zwischen dem Fehlerindiz und der Meldung drastisch verkürzt.

Daher wird in OpenScape 4000 immer parallel zur Signalisierungsverbindung eine Überwachungsverbindung (Supervisory-Verbindung) zwischen Zentrale und Access Point/OpenScape 4000 SoftGate aufgebaut, sobald Signaling Survivability für den Access Point/OpenScape 4000 SoftGate eingerichtet ist.

Auf dieser Überwachungsverbindung werden in sehr kurzen Zeitabständen (z.B. jede Sekunde) ausschließlich „Keep Alive“ Meldungen ausgetauscht.

Bekommt der CC auf eine „Keep Alive“ Meldung hin innerhalb eines einstellbaren Zeitintervalls (Supervisory Time) keine Antwort, so schaltet er das Routing der Signalisierungsmeldungen zu diesem Access Point/OpenScape 4000 SoftGate vom IP-Router zum Survivability Router um.



B ist die Keep Alive-Time der Supervisory-TCP-Verbindung, Supervisory Time (SUPVTIME) genannt; z.B.: 4 s

A ist das Meldungswiederholintervall; (A=B/8) z.B.: 0,5 s

Zur Begrenzung der erzeugten Last wird bei A < 0,5 s maximal alle 0,5 s eine Meldung geschickt.

Bei SUPVTIME = 3 wird 6 mal alle 0,5 s eine Meldung geschickt, bevor der Timer abläuft

Supervisory-Meldungsfluss bei Signaling Survivability im CC

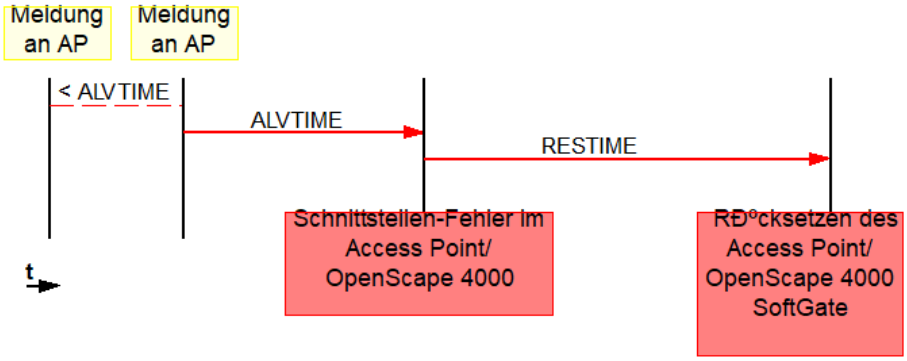
Auch im Access Point/OpenScape 4000 SoftGate läuft eine Eskalationsstrategie an.

Kommen unabhängig von der Überwachungsverbindung auch auf der Signalisierungsverbindung innerhalb des einstellbaren Zeitintervalls (**ALVTIME**) weder über das IP-Netz, noch über den alternativen Weg Meldungen am Access Point/OpenScape 4000 SoftGate an, so wird ein Schnittstellenfehler gemeldet.

Nach Meldung des Schnittstellenfehlers (**ALVTIME**) wird der Access Point/das OpenScape 4000 SoftGate aus der Liste der Vermittlungsplätze entfernt und innerhalb eines definierbaren Zeitintervalls (**RESTIME**) zurückgesetzt. Er wartet dann auf erneute Kontaktaufnahme durch die OpenScape 4000 Zentrale.

Bis zum Ablauf von **ALVTIME** werden alle Signaling-Meldungen, welche im CC und im Access Point/OpenScape 4000 SoftGate zur Übertragung anstehen, zwischengespeichert. Ist die „Alive“-Zeit (**ALVTIME**) abgelaufen, kann davon ausgegangen werden, dass die gespeicherten Meldungen veraltet sind und nicht mehr zugestellt werden dürfen. Damit ist dann aber der Meldungsfluss zwischen CC und Access Point/OpenScape 4000 SoftGate nicht mehr konsistent.

Die Zeitkonstanten können mit dem AMO SIPCO im Zweig **TIMING** verändert werden (siehe IP Distributed Architecture > Abschnitt 2.1, „OpenScape 4000 LAN Segment“ > System-Zeitverhalten (TIMING)).



Meldungsfluss bei Signaling Survivability im Access Point/OpenScape 4000 SoftGate

13.1.2 Was wird als Alternativweg für die Signalisierung verwendet?

Wenn die IP-Anbindung eines Access Points/OpenScape 4000 SoftGates ausfällt, wird ein Alternativweg in einem Netz benötigt, das von dem Ausfall nicht betroffen ist.

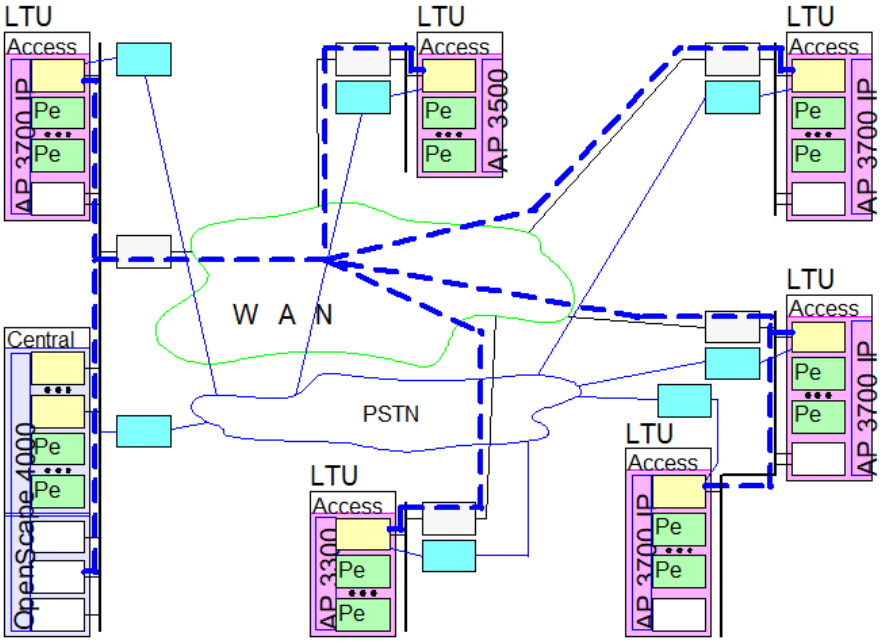
Die prinzipielle Anforderung an das Netz für den Alternativweg ist einfach:

- Es muss unabhängig vom IP-Netz sein, dessen Störung mit dem Alternativweg umgangen werden soll.
- Es muss ein Anschlussgerät für den Access Point/OpenScape 4000 SoftGate geben, das wie ein Modem agiert. Es muss aktiv anrufbar sein und dem Access Point/OpenScape 4000 SoftGate „Ring Indication“ geben.
- Die Zentrale muss durch einen entsprechenden Router oder eine STMI2/4 mit WAML-Funktion unterstützt werden.

Es gibt zwei verschiedene Wege für Signaling Survivability:

- Signaling Survivability über das öffentliche Amt
- Signaling Survivability über alternatives LAN

13.1.2.1 Signaling Survivability über das öffentliche Amt



IPDA mit Signaling Survivability

Mit Signaling Survivability über das öffentliche Amt wird ein *Umgehungsweg* für die Signalisierung über das ISDN-Netz (PSTN) aufgebaut, sobald eine Störung des IP-Weges erkannt wird. Die Meldungen werden dann über einen PSTN-Router an der Zentrale (z.B. Router mit IP > S2 oder STMI2/4-Baugruppe mit WAML-Funktion) und ein ISDN-Modem am Access Point/OpenScape 4000 SoftGate geführt. Nachdem dieser Umgehungsweg aufgebaut ist (ca. 30 ... 60 Sekunden) werden die Signalisierungsmeldungen hierüber geschickt. Es ist sichergestellt, dass von den eventuell aufgestauten Meldungen keine verloren geht.

In der Regel benötigt ein Access Point/OpenScape 4000 SoftGate mit Signaling Survivability für diesen Zweck einen Telefonanschluss. Der Anschluss sollte im öffentlichen Netz (PSTN) liegen, alternativ auch in einem privaten Netz - sofern die Verbindung nicht über das IP-Netz führt, dessen Störung mit dem Alternativweg umgangen werden soll.

Wichtig: Das Modem darf **nicht** über den Access Point/das OpenScape 4000 SoftGate ins öffentliche Netz gehen, es braucht einen eigenen Anschluss unabhängig vom Access Point/OpenScape 4000 SoftGate. Fällt die LAN Verbindung aus, kann der Access Point/das OpenScape 4000 SoftGate nicht mehr gesteuert werden. Führt der Alternativweg zum Modem über den Access Point/das OpenScape 4000 SoftGate, so kann er nicht geschaltet werden, bevor der Alternativweg aktiv ist. Der Alternativweg kann aber nicht aktiv werden, bevor er im Access Point/OpenScape 4000 SoftGate geschaltet wird.

Der Access Point/das OpenScape 4000 SoftGate hat auf der HG 3575 Baugruppe eine RS 232/ V.24 Schnittstelle zum Anschluss eines Modems, über das der Alternativweg der Signalisierung ins Telefonnetz geführt wird.

Gegenstelle zu diesem Modem ist ein spezieller Router am OpenScape 4000 LAN Segment, hier Survivability-Router genannt. Auch dieser Router benötigt einen Zugang zum Telefonnetz.

Fällt die LAN/WAN basierte Verbindung zum Access Point/OpenScape 4000 SoftGate aus, so wird eine Modem-Verbindung über Amt aufgebaut. Über diese Verbindung erfolgt die Steuerung des Access Points/OpenScape 4000 SoftGates so lange, bis die LAN/WAN-Verbindung wieder zur Verfügung steht.

Ist jeder Access Point/jedes OpenScape 4000 SoftGate mit einem eigenen Modem ausgestattet (und die Zentrale hat genügend Router-Verbindungen via Amt (PSTN) reserviert), deckt Signaling Survivability auch den Totalausfall der WAN-Infrastruktur ab. Kritisch ist hier nur noch die Anbindung zwischen dem aktiven CC und dem/den Survivability Router(n) im OpenScape 4000 LAN Segment sowie die Unabhängigkeit des (ausgefallenen) WAN von dem für Survivability genutzten PSTN.
Hinweise zum Übertragungsverfahren zwischen Router und Modem

Das Übertragungsverfahren zwischen Router und Modem muss zusammenpassen. Es sollte, wenn immer möglich, eine digitale Verbindung zwischen Router und Modem genutzt werden (ISDN-Modem), da analoge Modems sehr lange brauchen, um die Strecke auszumessen und sich auf ein Übertragungsverfahren zu einigen. Wenn während der Verbindungsaufbauzeit die Überwachungs-Timer von CC oder Access Point/OpenScape 4000 SoftGate ablaufen, besteht die Gefahr, dass Meldungen verloren gegangen sind. Der Access Point/das OpenScape 4000 SoftGate setzt sich zurück. Außerdem sind bei analogen Modems nur deutlich niedrigere Übertragungsraten zu erreichen, als über ISDN. Das kann zu Verzögerungen bei Signalisierungsmeldungen und in Stausituationen zum Ablauf von Überwachungstimern führen, worauf sich letztlich der Access Point/das OpenScape 4000 SoftGate zurücksetzt.

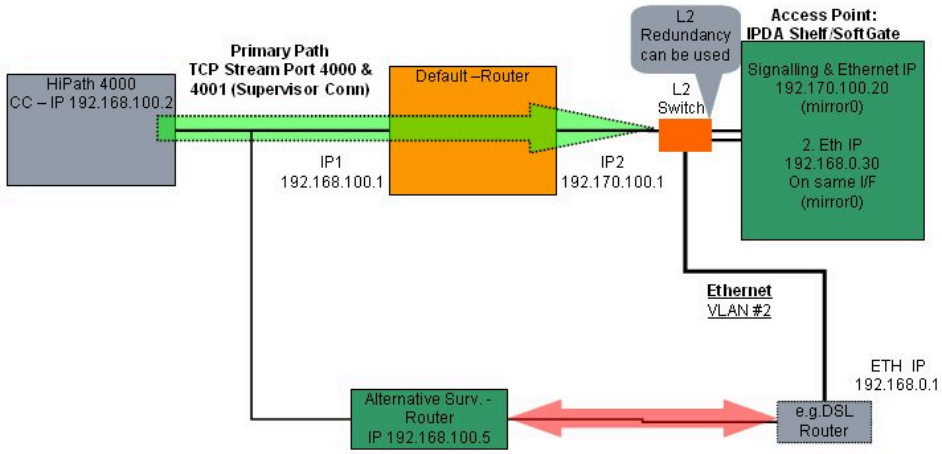
Generell werden etwa 64 kBit/s als maximal benötigte Übertragungskapazität im Signalisierungpfad als ausreichend betrachtet. Die Übertragungskapazität bei ISDN-Modems kommt diesem Wert hinreichend nahe. Bei analogen Modems ist maximal die Hälfte der Übertragungsbandbreite erzielbar. Damit kann es zu den beschriebenen Einschränkungen kommen. Es muss sichergestellt werden, dass mindestens 28,8 kBit/s tatsächlich als Übertragungsbandbreite zur Verfügung stehen. Erfolgen die Modem-Connects wegen schlechter Strecke mit niedrigerer Bitrate, ist der Pfad für Survivability ungeeignet.

13.1.2.2 Signaling Survivability über alternatives LAN

Mit Signaling Survivability über ein alternatives LAN wird ein Umgehungsweg für die Signalisierung über einen zweiten LAN-Weg aufgebaut, sobald eine Störung des IP-Weges erkannt wird. Hierfür wird ein Survivability Router an der Zentrale und eine zweite LAN-Infrastruktur am Access Point/OpenScape 4000 SoftGate benötigt. Es wird dann ein Umgehungsweg über den Survivability Router an der Zentrale und das zweite LAN am Access Point/OpenScape 4000 SoftGate aufgebaut. Nachdem dieser Umgehungsweg aufgebaut ist, werden die Signalisierungsmeldungen hierüber geschickt. Es ist sichergestellt, dass von den eventuell aufgestauten Meldungen keine verloren geht.

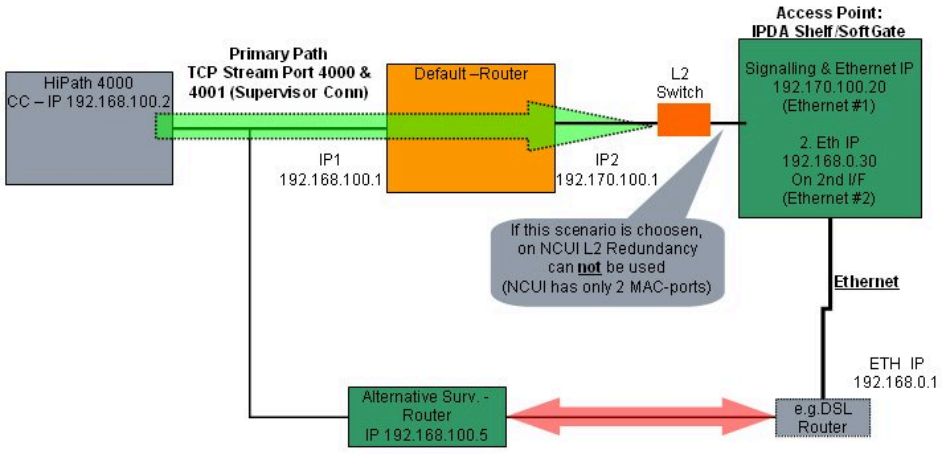
Es gibt zwei mögliche Szenarien für Signaling Survivability über alternatives LAN:

- L2 Redundanz am Access Point/OpenScape 4000 SoftGate als Input für den alternativen Router



Signaling Survivability über alternatives LAN und L2 Redundanz

- 2. Ethernet-Schnittstelle des Access Point/OpenScape 4000 SoftGate als Input für den alternativen Router



Signaling Survivability über alternatives LAN und zweiter Ethernet-Schnittstelle

Ist jeder Access Point/jedes OpenScape 4000 SoftGate mit einem eigenen Survivability Router ausgestattet, deckt Signaling Survivability auch den Totalausfall der WAN-Infrastruktur ab. Kritisch ist hier nur noch die Anbindung zwischen dem aktiven CC und dem/den Survivability Router(n) im OpenScape 4000 LAN Segment sowie die Unabhängigkeit des (ausgefallenen) WAN von dem für Survivability genutzten LAN.

13.1.3 HSR über UDP

Das Leistungsmerkmal „HSR (HiPath Signaling Router) über UDP“

- betrifft die Signalisierungs-Verbindung zwischen Hostsystem und Access Point/OpenScape 4000 SoftGate. Nicht betroffen ist die Signalisierungs-Verbindung zwischen APE und Access Point/OpenScape 4000 SoftGate.

Letztere ist immer nur eine reine TCP/IP-Verbindung unabhängig von der Konfiguration des Parameters **SIGMODE** im AMO UCSU.

- kann/darf bei „Signaling Survivability über das öffentliche Amt“ zusätzlich eingeschalten werden um Firewalls zu umgehen.
- muss bei Verwendung des Leistungsmerkmals „Signaling Survivability über alternatives LAN“ eingeschaltet werden.
- kann/muss pro Access Point/OpenScape 4000 SoftGate individuell ein-/ausgeschaltet werden (AMO UCSU, **SIGMODE=HSRUDP**).

Wichtig: Das Kunden-IP-Netzwerk (Firewall) darf die UDP-Ports 4000 und 4050 nicht unterbinden.

13.2 Serviceinformationen

- Das Leistungsmerkmal „Signaling Survivability“ ist für Access Points, OpenScape 4000 SoftGate und OpenScape Access freigegeben.
- Bis zu 10 Survivability Router können im System eingerichtet werden.
- Signaling Survivability über das öffentliche Amt (Modem) wird beim OpenScape 4000 SoftGate (vNCUI) für SoftGate 50 und SoftGate 500 unterstützt.
- **Nur gültig für Signaling Survivability über öffentliches Amt:** Je nach Anschlusskapazität kann ein Survivability-Router bis zu 30 Access Points/OpenScape 4000 SoftGates bedienen (Router mit S2-Anschluss). Da nicht vorhersagbar ist, wo im IP-Netz eine Störung auftritt, muss die Router-Kapazität für den schlimmsten Fall ausgelegt werden, d.h. den Ausfall der Verbindung vom OpenScape 4000 LAN Segment in das IP-Netz des Kunden. Dann werden schlagartig für alle Access Points/OpenScape 4000 SoftGates mit Signaling Survivability Alternativwege für die Signalisierung benötigt.
- **Nur gültig für Signaling Survivability über öffentliches Amt:** Führt die Modem-Verbindung über das öffentliche Netz, so fallen dort Verbindungsgebühren an. Die Verbindung zum einem Access Point/OpenScape 4000 SoftGate wird genutzt, solange der Access Point/das OpenScape 4000 SoftGate nicht über das IP-Netz erreichbar ist. In der Konfiguration des Survivability Routers wird eingestellt, nach welcher Zeit der „Nicht-Nutzung“ diese Verbindung wieder abgebaut wird. Diese „Hold-Time“ ist nicht Bestandteil der IPDA Konfiguration. Die Erreichbarkeit des Access Points/OpenScape 4000 SoftGates über die Modem-Verbindung wird zyklisch geprüft (RTO). Die Prüfung kann auch direkt über AMO TSU gestartet werden. Auch in diesen Fällen werden im PSTN Verbindungsgebühren anfallen.
- Die Verbindung vom aktiven Prozessor (CC-A oder CC-B) zum Survivability Router führt wie die Verbindung zum normalen LAN-Router über das OpenScape 4000 LAN Segment. Ist dieses LAN Segment gestört, weil z.B. ein zentraler L2-Switch defekt ist, so funktioniert auch Signaling Survivability nicht mehr. Dieser „Single Point of Failure“ kann etwas entschärft werden, wenn CC-A und CC-B an unterschiedlichen L2-Switches angeschlossen werden und z.B. je die Hälfte der Survivability-Router und der HG 3500 an den entsprechenden Switches angeschlossen werden. Damit ist bei Ausfall eines der beiden L2-Switches zumindest eine Hälfte des Systems weiter verfügbar.

- Der TCP-Stream (tcp.port=4000) muss absolut transparent durch das Kunden-IP-Netzwerk geroutet werden (d.h. keine Manipulation der SequenceNumber etc.), ansonsten funktioniert das Leistungsmerkmal Signaling Surviability nicht. Desweiteren müssen gegebenenfalls vorhandene Firewalls entsprechend konfiguriert werden, so dass eine SequenceNumber- und SYN-Prüfung für den tcp.port=4000 nicht stattfindet. Wenn das nicht garantiert werden kann, sollte man alternativ das Leistungsmerkmal „HSR über UDP“ einschalten.
- Signalling Survivability über das öffentliche Amt (Modem) mit OpenScape 4000 SoftGate (vNCUI) wurde getestet und wird mit OpenScape 4000 SoftGate 50 & OpenScape 4000 SoftGate 500 unterstützt. Startup- und Basis-Szenarien mit hoher Last wurden getestet (480 Teilnehmer mit > BHCA 6000) über Modem. Dennoch kann im Zusammenhang mit großen Gruppenleistungsmerkmalen und Signalisierung (z.B. AUN) es zu Signalisierungsverzögerungen kommen. Die Verzögerungen treten auf Grund von Bandbreitenbegrenzungen der PPP-Verbindungen (64kbit/s) auf, die zu TCP Retransmission führen. Wenn große Gruppen mit Signalisierung verwendet werden **oder** OpenScape 4000 SoftGate 1000 wird empfohlen „Signalling Survivability über alternatives LAN“ zuverwenden, weil hier weniger Probleme mit der Bandbreite bestehen (z.B. ADSL hat eine viel höhere Bandbreite für die Signalisierung). Andere Survivability-Optionen wie APE, Survivable OpenScape 4000 SoftGate und BPOOL Funktionen sind auch möglich, aber nicht ohne Unterbrechung der Telephonie.
- Bitte auch folgendes beachten:

  Um Signaling Survivability am OpenScape 4000 SoftGate zu gewährleisten, ist ein bestimmtes USB-Kabel notwendig (Sachnummer: C39195-Z7705-A3) Sie können den Kabeltyp in \var\log\messages unter Linux prüfen: Korrektes Kabel: New USB device found, idVendor=067b, idProduct=2303 Ein alternatives Kabel von ATEN mit der folgenden Vendor-ID und Produkt-ID verursacht Probleme: New USB device found, idVendor=0557, idProduct=2008.

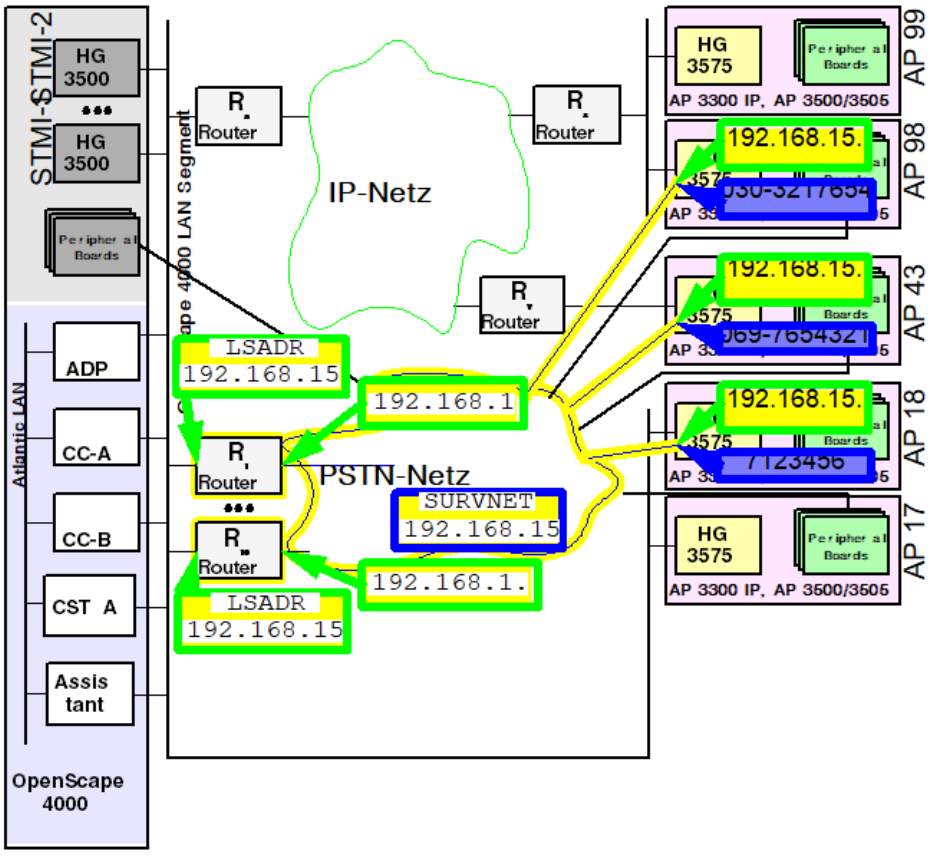
  Um Signaling Survivability mit einem externen ISDN-Router am OpenScape 4000 SoftGate zu gewährleisten, muss das ISDN-Modem mindestens die Firmware-Version V7.019 haben, um das AT**ACCM-Kommando verstehen zu können. Für mehr Informationen siehe MSC24547 in G-DMS.
- Signaling Survivability mit WAML-Replacement ist nur mit Common Gateway Baugruppe (HG 3500) freigegeben. Die WAML-Funktion darf also nur in einem Host-Shelf oder einem IPDA-Shelf (direct link) eingerichtet werden bzw. die Funktionalität auf einem OpenScape 4000 SoftGate / OpenScape Access wird nicht unterstützt.
- L2 Redundanz am Access Point als Input für den alternativen Router ist nur mit einem OpenScape 4000 SoftGate möglich.
- Bei Signaling Survivability über alternatives LAN (AMO APRT, Parameter **SURVLAN**) muss HSR über UDP konfiguriert sein.
- Einschränkungen und Informationen in Verbindung mit Deployment „Simplex mit integriertem SoftGate“ (OpenScape 4000 SoftGate auf dem selben Computer wie Host System):
- – Das integrierte OpenScape 4000 SoftGate unterstützt nicht HSR über UDP.
  – Das integrierte OpenScape 4000 SoftGate unterstützt nicht Signaling Survivability Funktion für die HSR-Verbindung.
  – Das integrierte OpenScape 4000 SoftGate darf eine HSR-Verbindung von einem AP-CC akzeptieren (Leistungsmerkmal APE).

- Einschränkungen und Informationen in Verbindung mit Deployment „Survivable SoftGate“ (OpenScape 4000 SoftGate und APE auf dem selben Computer):
- – APE unterstützt nicht Signaling Survivability Funktion für die HSR-Verbindung.
  – OpenScape 4000 SoftGate unterstützt HSR über UDP zum Host-System.
  – OpenScape 4000 SoftGate unterstützt Signaling Survivability Funktion für die HSR-Verbindung zum Host-System.
- Die Golden Load Loadware auf der NCUI-Baugruppe unterstützt nicht die UDP-Funktionalität, die a für Signaling Survivability über alternatives LAN benötigt wird. Deshalb muss beim Baugruppentausch das in Abschnitt 3.2.4, „Austausch einer defekten NCUI-Baugruppe durch eine neue NCUI-Baugruppe“ beschriebene Vorgehen beachtet werden.

13.3 Generierung (Beispiel)

13.3.1 Signaling Survivability über das öffentliche Amt

13.3.1.1 Konfiguration der OpenScape 4000



Signaling Survivability über Modem

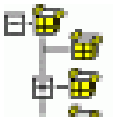
Die Zugänge der Survivability-Router und der Modems in das Telefonnetz PSTN bilden ein virtuelles IP-Netz, das Survivability Netz. Jeder Zugang zu diesem virtuellen Netz benötigt eine IP-Adresse in diesem Netz. Um den Administrationsaufwand für dieses virtuelle Netz so gering wie möglich zu halten, wurden einige Festlegungen getroffen:

- Das Survivability-Netz hat die Netzmaske 255.255.255.0.
- Es werden maximal 10 Survivability Router zwischen dem OpenScape 4000 LAN Segment und dem Survivability-Netz unterstützt, sie werden von 1 bis 10 durchnummeriert. Die vierte Stelle der IP-Adresse der Router im Survivability-Netz ist die laufende Nummer des Routers, also 1-10.
- Die Adresse eines Access Points im Survivability-Netz ist ebenfalls fest vorgegeben. Die vierte Stelle der IP-Adresse wird identisch der LTU-Nummer des Access Points gesetzt.

Es bleibt also im Wesentlichen ein Parameter im Survivability-Netz, der eingestellt werden muss - und das ist die Netzwerk-Adresse.

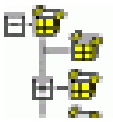
Sie wird mit dem AMO SIPCO eingestellt und muss bereits beim EINRICHTEN-SIPCO angegeben werden, wenn der Kunde Lizenzen für Signaling Survivability gekauft hat (siehe IP Distributed Architecture > Abschnitt 2.1, „OpenScape 4000 LAN Segment“).

Werden die Lizenzen für Signaling Survivability erst später dazugekauft, oder wurde bei der Erstinstallation die Null-Adresse 0.0.0.0 angegeben, so muss diese Adresse jetzt eingestellt werden.

	**Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken, auf der Registerkarte **Anlagendaten** Survivability-Netzwerk-Adresse eintragen oder ändern, dann auf **Sichern** klicken.
	`AENDERN-SIPCO:TYP=LSNET,SURVNET=192.168.15.0;`

Wichtig: Die letzte Stelle der SURVNET-Adresse muss immer gleich NULL sein. Sonst wäre es zusammen mit der fest vorgegebenen Netzmaske 255.255.255.0 keine Netzadresse.

Die Lizenzen für Signaling Survivability können folgendermaßen abgefragt werden:

	**Configuration Management > HiPath Inventory Management > HIM-Anlagendaten > Leistungsmerkmale > Marketing Einheiten** Auf **Suchen** klicken > Registerkarte **Vertriebsleistungsmerkmale** > Eintrag **Signaling Survivability**
	`ABFRAGEN-CODEW;` Eintrag „SIGNALING SURVIVABILITY“

Obwohl dieses Netz nur im Bedarfsfall genutzt wird und die Kommunikationspartner genau festgelegt sind, muss diese Adresse für dieses Netz mit dem Netzwerkadministrator des Kundennetzes abgestimmt werden.

Als nächstes muss die Zuordnung der Access Points zu den Survivability Routern überlegt werden. Jeder Survivability-Router kann beschrieben werden durch die folgenden Daten, die im Router selber auch konfiguriert werden müssen:

- Laufende Nummer des Routers [1..10]
- IP-Adresse des Routers im OpenScape 4000 LAN Segment
- IP-Adresse des Routers im Survivability-Netz
- Über diesen Router zu bedienende Access Points.Dafür jeweils:
- – LTU-Nummer und daraus abgeleitet deren IP-Adresse für Survivability
  – Telefonnummer des Modemanschlusses
- Signaling Survivability Typ = MODEM

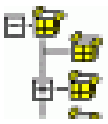
Der Router ist schließlich so zu konfigurieren, dass er beim ersten Empfang eines Pakets mit Zieladresse gleich Survivability Adresse eines Access Points eine Wählverbindung zum Modem dieses Access Points aufbaut und danach das Paket überträgt. Wird die Verbindung für längere Zeit (z.B. 30 Sekunden) nicht genutzt, ist der Access Point wieder über LAN erreichbar und die Verbindung zum Modem kann wieder abgebaut werden.

Als Survivability-Router kann auch eine STMI2/4-Baugruppe mit WAML-Funktion in der OpenScape 4000 Zentrale eingesetzt werden.

Wichtig: Soll ein Survivability Router über die OpenScape 4000 auf das ISDN-Netz zugreifen, dann muss für ausreichend Verbindungskapazität im Amtszugang der OpenScape 4000 gesorgt werden. Sollen z.B. 83 Access Points an einer Anlage mit Signaling Survivability ausgestattet werden, so müssen bei Ausfall des IP-Netzes im Zentralbereich um die OpenScape 4000 Anlage sofort 83 B-Kanäle ins Amt bereitstehen. Wird diese Kapazität nicht reserviert, so kann es passieren, dass nicht alle Access Points erreichbar sind. Access Points, die über Signaling Survivability nicht erreicht werden, führen einen Restart aus und gehen erst wieder in Betrieb, wenn sie vom CC über LAN oder Modem erreicht werden.

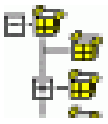
Die Konfiguration im OpenScape 4000 System geschieht folgendermaßen:

- Bekanntmachen der Survivability-Router im System

	**Configuration Management > Anlagendaten > IPDA -- > IPDA Signaling Survivability Router** Auf **Suchen** klicken, auf der Registerkarte „Router-Daten“ Router-Nummer und Adresse eintragen oder ändern, dann auf **Sichern** klicken.
	`EINRICHTEN-APRT:TYP=SURV,KONF=ROUTER,ROUTERNR=1, LSA-DR=192.168.1.101;` `EINRICHTEN-APRT:TYP=SURV,KONF=ROUTER,ROUTERNR=10, LSA-DR=192.168.1.110;`

Damit sind die beiden Router 1 und 10 aus dem Beispiel in Bild 48 „Signaling Survivability über Modem“ eingerichtet.

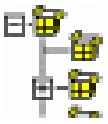
- Zuordnen der Access Points zu den Survivability-Routern

	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken, auf der Registerkarte **Allgemein** die gewünschte Router-Nummer bei Signaling Survivability einstellen und auf **Sichern** klicken.

	`EINRICHTEN-APRT:TYP=SURV,KONF=AP,LTU=98,ROUTERNR=1,SURVTYP=MODEM;`
	`EINRICHTEN-APRT:TYP=SURV,KONF=AP,LTU=43,ROUTERNR=1,SURVTYP=MODEM;`
	`EINRICHTEN-APRT:TYP=SURV,KONF=AP,LTU=18,ROUTERNR=1,SURVTYP=MODEM;`

Damit sind alle Access Points mit Signaling Survivability aus dem Beispiel in Bild 48 „Signaling Survivability über Modem“ einem Router zugewiesen. Bei der Zuweisung des Access Points an einen Router wird letztlich Signaling Survivability für den Access Point eingerichtet. Bei diesem Kommando wird geprüft, ob noch eine Lizenz für Signaling Survivability frei ist. Wenn ja, wird die Nutzung verbucht, wenn nein, wird das Einrichten abgewiesen.

Soll die Zuordnung eines AP zu einem Survivability-Router geändert werden, soll z.B. AP 43 statt von Router 1 künftig von Router 10 bedient werden, ist folgende Aktion notwendig:

	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken, auf der Registerkarte **Allgemein** die gewünschte Router-Nummer bei Signaling Survivability einstellen und auf **Sichern** klicken. **Configuration Management > Anlagendaten > IPDA > IPDA-Anlagendaten** Auf **Suchen** klicken und den Access Point auswählen. Im Pulldownmenü **Aktion** auf Ausführen **klicken und den Tätigkeitsmodus AP aktualisieren** einstellen. Mit **OK** bestätigen.



Ein AENDERN der Konfiguration für Signaling Survivability mit APRT ist nicht möglich. Zum Ändern wird einfach die entsprechende Zuordnung gelöscht und anschließend neu eingerichtet.

```
LOESCHEN-APRT:TYP=SURV,KONF=AP,LTU=43;
EINRICHTEN-
APRT:TYP=SURV,KONF=AP,LTU=43,ROUTERNR=10,SURVTYP=MODEM;
```

Damit diese Änderung wirksam wird, muss AP 43 neu geladen werden:

```
EXEC-USSU:ART=UPDATAP,LTU=43;
```

Wichtig: Verbindungen werden ohne weitere Nachfrage getrennt!!! Vor dem `EXEC-USSU:UPDATAP` muss ein Update der Konfiguration auf die Systemharddisk durchgeführt werden.

13.3.1.2 Konfiguration des Modems

Die Konfiguration des ISDN-Modems erfolgt über die RS232/V.24 Schnittstelle des Modems. Um die Einstellungen vornehmen zu können, muss das Modem an einen PC angeschlossen und auf dem PC ein Terminalemulationsprogramm (Hyperterminal) gestartet werden.

Wichtig: Für den Einsatz als IPDA Survivability-Modem mit ISDN-Schnittstelle wird das Modem **Pocket ISDN TA** von *INSYS Microelectronics, S30122-X7551-XAYA422* empfohlen.

Folgende Dinge müssen eingestellt werden, falls sie nicht bereits in der Werkseinstellung enthalten sind:

- Die Baudrate an der seriellen Schnittstelle des Modems muss auf 115200 Baud eingestellt werden, was meist über den Auto-Detect-Mode abgedeckt ist. **Modems, welche die Baudrate 115200 an der seriellen Schnittstelle nicht unterstützen, sind für den Einsatz mit IPDA ungeeignet.**
- Die automatische Rufannahme (Auto-Answer) muss **aus**geschaltet werden.
- Das lokale Echo muss **aus**geschaltet werden.
- Die Antwort des Modems auf Kommandos muss im Klartext (in der Langform) erfolgen, d.h. als Text „RING“, „CONNECT“, etc.
- Es dürfen weder Fehlerkorrektur noch Kompression im Modem aktiviert werden, das erledigt PPP selber.
- Der Software-Handshake (XON/XOFF) muss ausgeschaltet sein.
- *für ISDN-Modems:* das B-Kanal Protokoll: HDLC - PPP Protokoll („async to sync“ Konvertierung, PPP asynchron, single link PPP)
- *für Analog-Modems*: Leitungsbitrate auf beiden Modems fest vorgeben, um die Verhandlungszeit zu sparen. Auf die Meldung „RING“ des Modems an die HG 3575 schickt diese das Kommando „AT A“ an das Modem, welches innerhalb von 60 Sekunden „CONNECT“ melden muss.

Zuerst muss die Werkseinstellung wiederhergestellt werden (factory defaults)

```
AT&F
```

Danach folgt die Einstellung der oben genannten Parameter

Für Modem **Pocket ISDN TA**

- muss die automatische Rufannahme abgeschaltet werden:
- `ATS0=0`
- muss das lokale Echo abgeschaltet werden:
- `ATE` oder allgemein `ATE0`

Zuletzt muss die Konfiguration abgespeichert werden:

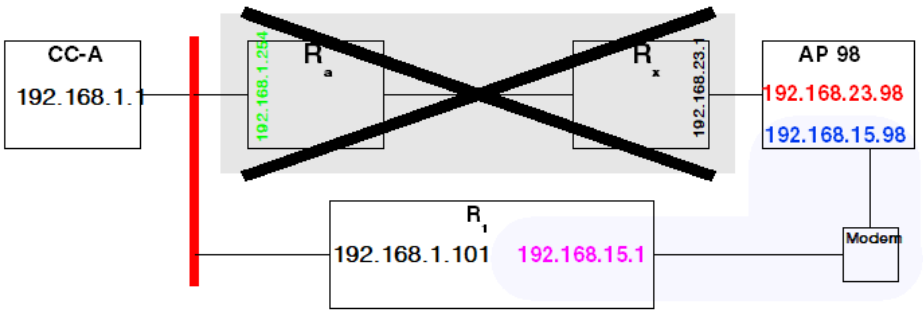
`AT&W`

13.3.1.3 Konfiguration des Routers

Überblick

- Signalisierungsfluss Survivability für „networked“ Access Points
- Signalisierungsfluss Survivability für „direct link“ Access Points
- Signaling Survivability mit WAML Replacement
- Externer ISDN-Router als Survivability Router

13.3.1.3.1 Signalisierungsfluss Survivability für „networked“ Access Points



Konfiguration Survivability Router

Bei der Konfiguration des Survivability Routers muss folgender Ablauf berücksichtigt werden.

Normalablauf (ohne Survivability):

1) CC-A generiert Paket an AP 98 mit Destination 192.168.23.98 und Source 192.168.1.1 und übergibt dies an Router Ra (192.168.1.254).

Dieser gibt das Paket eventuell über weitere Router an Rx, welcher das Paket an AP 98 zustellt.

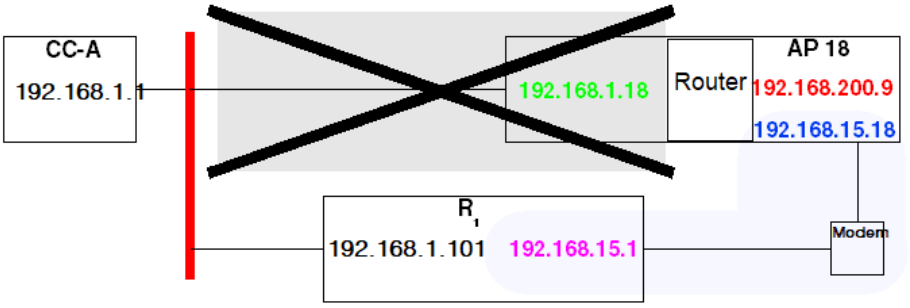
Survivability:

CC-A generiert Paket an AP 98 mit Destination 192.168.23.98 und Source 192.168.1.1 und übergibt dies an Router R1 unter 192.168.1.101.

Wichtig: Der komplette **IP-Frame** inklusive der Adressen bleibt identisch zum Normalbetrieb. Mit Survivability ändert sich (im OpenScape 4000 LAN Segment) nur der angesprochene Router, was sich in einer unterschiedlichen Zieladresse auf Ethernet-Ebene (MAC-DA) äußert. Die IP-Adresse des Routers R1 im OpenScape 4000 LAN Segment

wird nicht sichtbar angesprochen. Sie wird zur Bestimmung der MAC-Adresse des Router-Ports mit ARP benötigt.

13.3.1.3.2 Signalisierungsfluss Survivability für „direct link“ Access Points



Konfiguration Survivability Router

Bei der Konfiguration des Survivability Routers muss folgender Ablauf berücksichtigt werden.

Normalablauf (ohne Survivability):

1) CC-A generiert Paket an die Signalisierungsinstanz des AP 18 mit Destination 192.168.200.9 und Source 192.168.1.1 und übergibt dies an den internen Signalisierungs-Router des AP 18 (192.168.1.18).

Dieser stellt das Paket an die Signalsierungsinstanz des AP 18 (192.168.200.9) zu.

Survivability:

CC-A generiert Paket an AP 18 mit Destination 192.168.200.9 und Source 192.168.1.1 und übergibt dies an Router R1 unter 192.168.1.101.

> **Wichtig:** Der komplette **IP-Frame** inklusive der Adressen bleibt identisch zum Normalbetrieb. Mit Survivability ändert sich (im OpenScape 4000 LAN Segment) nur der angesprochene Router, was sich in einer unterschiedlichen Zieladresse auf Ethernet-Ebene (MAC-DA) äußert. Die IP-Adresse des Routers R1 im OpenScape 4000 LAN Segment wird nicht sichtbar angesprochen. Sie wird zur Bestimmung der MAC-Adresse des Router-Ports mit ARP benötigt.

a) R1 richtet das Paket an den Next-Hop-Router 192.168.15.18 und baut dazu die Modemstrecke für die PPP-Verbindung zwischen 192.168.15.1 und 192.168.15.18 auf, bzw. nutzt die bereits aufgebaute Verbindung.

Im AP 98 wird das Paket von der PPP-Instanz 192.168.15.98 an das Ziel 192.168.23.98 zugestellt.

Dafür ist es notwendig, dass im Survivability-Router R1 die Route für 192.168.23.98 über **192.168.15.98** eingerichtet wird und die Wählverbindung für das Ziel 192.168.15.98.

Im AP 98 wird das Paket von der PPP-Instanz 192.168.15.18 an das Ziel 192.168.200.9 zugestellt.

13.3.1.3.3 Signaling Survivability mit WAML Replacement

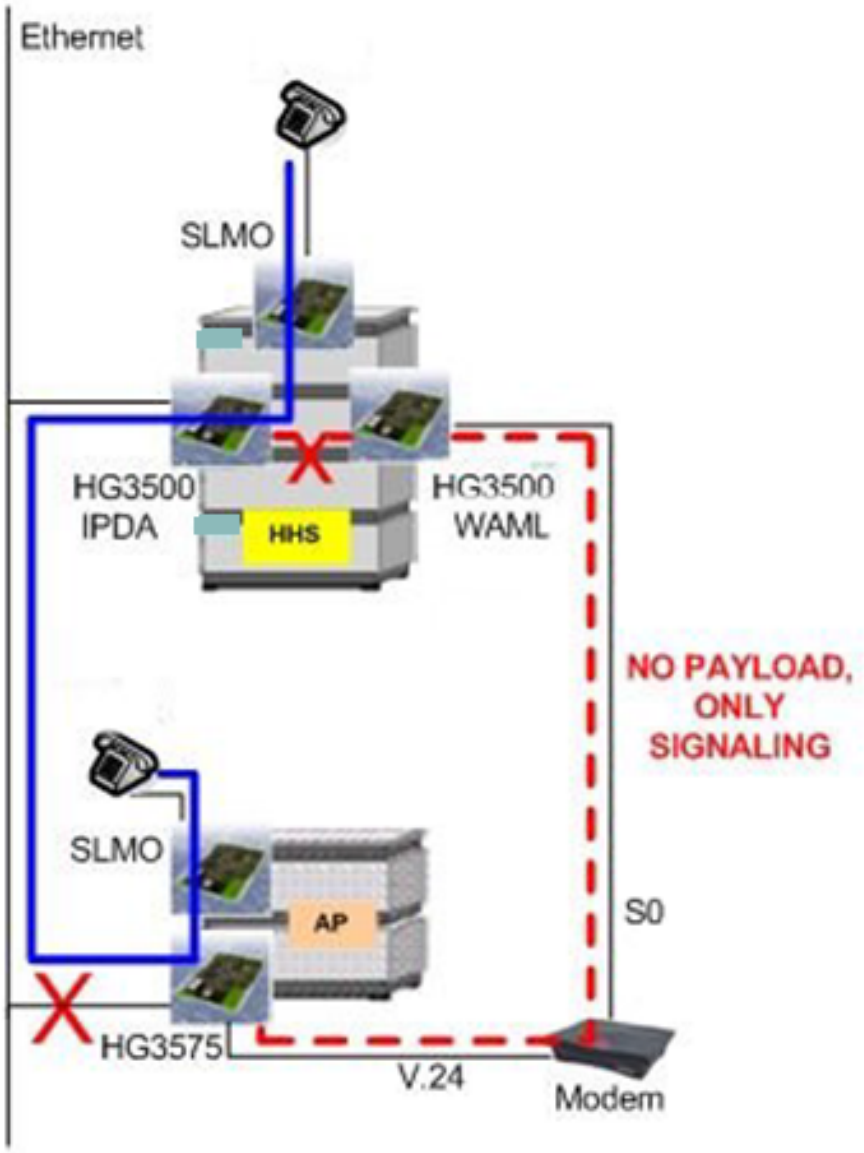
Für das Leistungsmerkmal „Signaling Survivability mit WAML Replacement“ muss eine Common Gateway Baugruppe (HG 3500) mit Hilfe des AMO

BFDAT mit **FUNCTION=WAML** eingerichtet werden. Man kann hierfür eine eigene Baugruppe verwenden oder eine Baugruppe, die mehrere Funktionen unterstützt.

Wichtig: Ist dieses Leistunsgmerkmal konfiguriert (Baugruppe STMI mit WAML-Funktion, dann funktioniert das Leistungsmerkmal redundante LAN-Schnittstellen nicht! Siehe auch Abschnitt 6.4, „Redundante LAN-Schnittstelle“.

Hardware:

- STMI (HG 3500) mit WAML Funktionalität wird als Router verwendet. Sie **muss** zwecks Kommunikation mit CCA/CCB (innerhalb desselben Netzwerkes) im Host System konfiguriert werden.
- S0-Anschluss muss konfiguriert werden.
- ISDN-Modem ist mit V.24 (Modem) an der NCUI (HG 3575) verbunden.



Signaling Survivability mit WAML Replacement

Die Konfiguration besteht aus 3 Teilen:

1. IPDA

```
EINRICHTEN-
SIPCO:NETADR=172.28.145.0,NETMASK=255.255.255.0,IPMODE=IPV4,DEFRT=172.
,CCAADR=172.28.145.150,CCBADR=0.0.0.0,SURVNET=192.168.15.0;
EINRICHTEN-UCSU:ART=AP,LTG=1,LTU=18,LTSACHNR=Q2305-
X40,SRCGRP=1,FRAME►
TYP=L80XF,VERBART=APDL,LSRTADR=172.28.145.155,APRTADR=172.28.145.254,S
2,STANDORT=âIPDA17WEASâ,PLCHECK=JA,ANZBKAN=30,KONVLAW=NEIN,TCLASS=0,AI
EINRICHTEN-APRT:TYP=APNET,LTU=18,APIPADR=172.28.0.57,NET►
MASK=255.255.255.255,TAIPADR=0.0.0.0;
```

/* HG3575 Konfigurationsdaten

ip_addr_eth is	*	172.28.145.155
netmask_eth is	*	255.255.255.0
default_gateway is	*1	172.28.145.254
ip_addr_signaling is	*	172.28.0.57
netmask_signaling is	*	255.255.255.255
ip_addr_survivability is	*2	192.168.15.18
netmask_survivability is	*2	255.255.255.0
gateway_survivability is	*2	192.168.15.1
netmask_hhs is	*	255.255.255.0
ip_addr_CC_A is	*	172.28.145.150
ip_addr_CC_B is	*3	0.0.0.0
ip_addr_CC_C is		0.0.0.0

2. Signaling Survivability mit WAML

/* **WAML**

```
EINRICHTEN-
BFDAT:FCTBLK=5,FUNCTION=WAML,BGBKAN=BKAN60&BKAN120;

AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=5,FUNCTION=WAML,ANZBKAN=1;

AENDERN-BFDAT:CONFIG=OK,FCTBLK=5,ANTW=JA;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=85,SACHNR=âQ2316-
X10â,FCTID=1,LW►
VAR=â0â,FCTBLK=5,BKANWAML=10;
EINRICHTEN-
CGWB:LTU=1,EBT=85,SMODE=NORMAL,IPADR=172.28.145.156,NET►
MASK=255.255.255.0;
```

/* **Richtung zum Router und Rufnummer des Routers**

```
EINR-BUEND:BUNUM=111,NAME=âWAMLâ,ANZ=30;
```

```
EINR-
COT:COTNU=222,COTPAR=MVLT&LOKN&VKNN&KTON&OLCR&OLRD,INFO=FUER_WAML
EINR-
COP:COPNU=222,COPPAR=SFOR,BERAMT=FBKW,BERFERN=FBKW,GER=LAN,INFO=C
ER_WAML;
EINR-COSSU:NEWCOS=222,ESBER=FBKW&QVKW;
EINR-WABE:RNR=446,KZP=QUER,PRUEF=NEIN;
EINR-TDCSU:ART=NEU,LAGE=1-1-85-0,COTNR=222,COS=222,COP►
NR=222,LCOSS=1,LCOSD=1,SATZNR=WAMLREPLACED,ZLNR=0,PROTVAR=ECMAV2,
MENT=8,KNNR=1-1-318,GER=HG3550LA,BUNR=111,BKANAL=1&&10;
EINR-
RICHT:ART=LRTGNEU,LRTG=223,LDIENST=ALLE,NAME=WAML,BUNUM=111,ZKNNR
EINRICHTEN-LODR:LWR=11,LWREL=ECHOFELD,FELD=1;

EINRICHTEN-LODR:LWR=11,LWREL=ENDE;

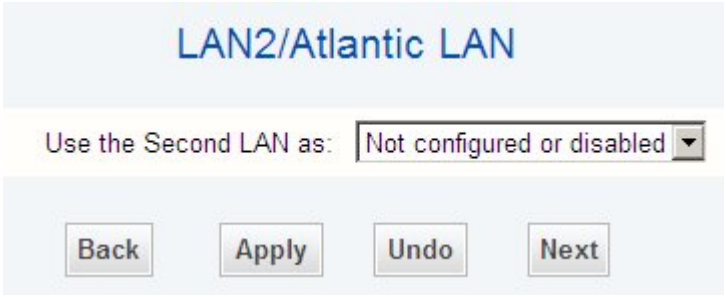
EINRICHTEN-LODR:LWR=11;
EINR-
LDAT:LRTG=223,LDIENST=ALLE,LWERT=1,BUNUM=111,LWR=11,LBER=1;
EINR-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=446,LRTG=223,LBER=1;
/* IP-Adresse des Routers (IP-Adresse des physikalischen
 Routers - WAML)
EINR-
APRT:TYP=SURV,KONF=ROUTER,ROUTERNR=1,LSADR=172.28.145.156;
/* Access Point dem Survivability-Router zuweisen
EINR-APRT:TYP=SURV,KONF=AP,LTU=18,ROUTERNR=1;
```

3. WAML (HG 3500/STMI) Konfiguration über WBM

WAML und LAN Redundancy

Unabhängig von der Konfiguration der 2. LAN-Schnittstelle (aktiv oder nicht) kann LAN Redundancy auf einer HG 3500 mit WAML-Funktionalität nicht konfiguriert werden.

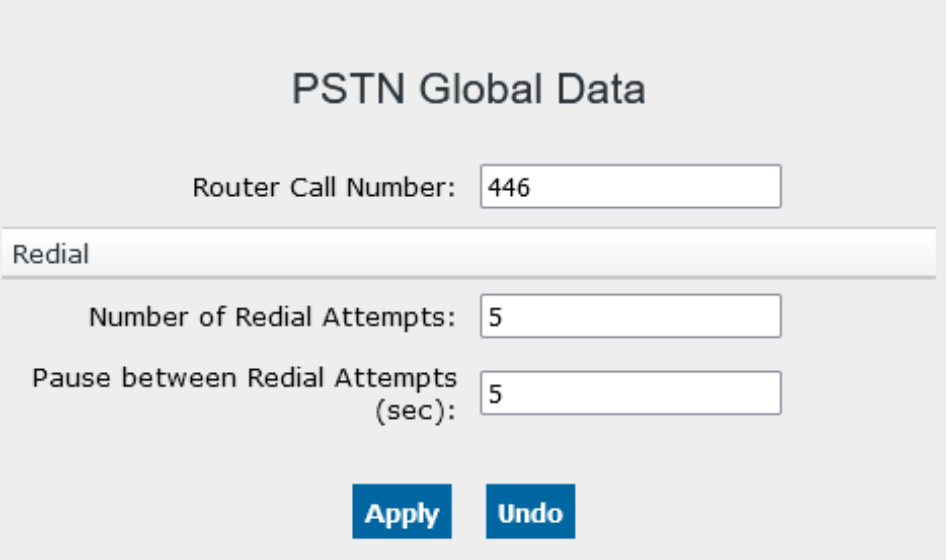
Wählen Sie deshalb bei der Erst-Installation für die zweite LAN-Schnittstelle Nicht konfiguriert oder deaktiviert.



WAMLReplacement - Zweite LAN-Schnittstelle

Router Rufnummer

Explorer > Routing > PSTN > (rechte Maustaste) Globale PSTN-Daten ändern wie im AMO LDPLN konfiguriert.



WAMLReplacement - Globale PSTN-Daten

Sie können das Ergebnis mit **Explorer > Routing > PSTN >** (rechte Maustaste) Globale PSTN-Daten anzeigen überprüfen.

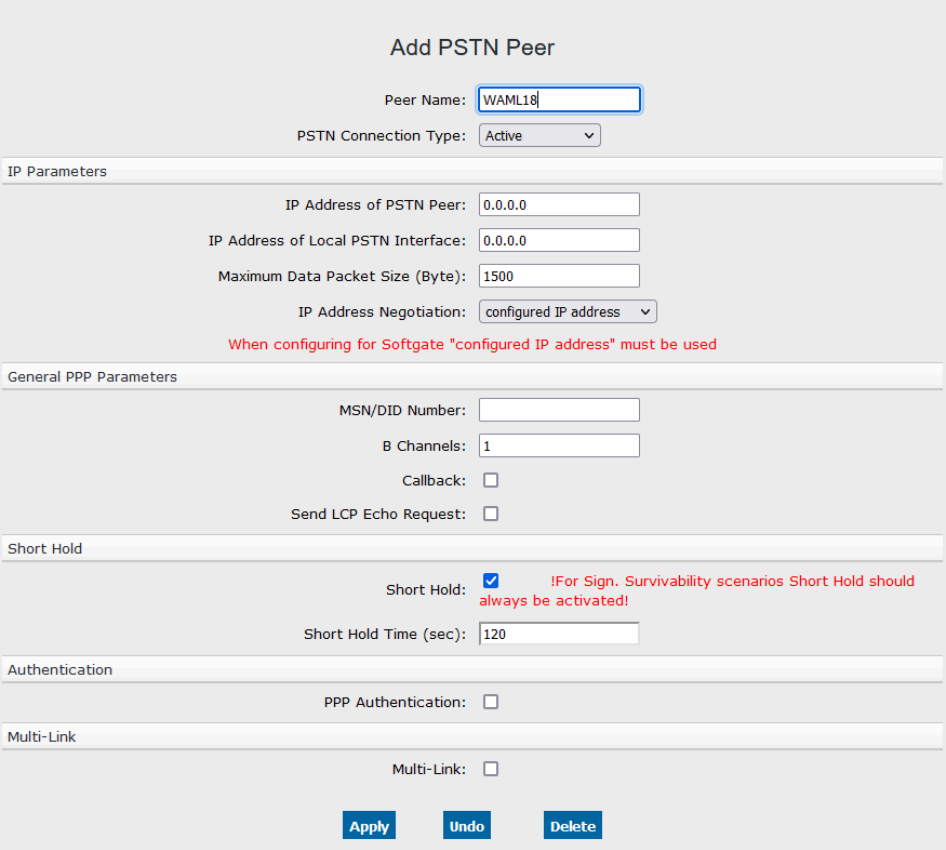
PSTN-Partner

Als PSTN-Partner wird das Survivability-Modem mit seiner IP-Address vom AMO SIPCO (Parammeter SURVNET + Access Point Nummer, hier 192.165.15.18) konfiguriert.

Die PSTN-Schnittstelle ist die PPP-Seite der WAML, z..B AMO SIPCO, Parameter SURVNET + Router-Nummer, hier 192.168.15.1.

Explorer > Routing > PSTN > PSTN Partner > (1) WAML18

Anmerkung: Aktivieren Sie den **Short-Hold-Modus** und setzen Sie die **Short-Hold-Zeit** auf 180 Sekunden.

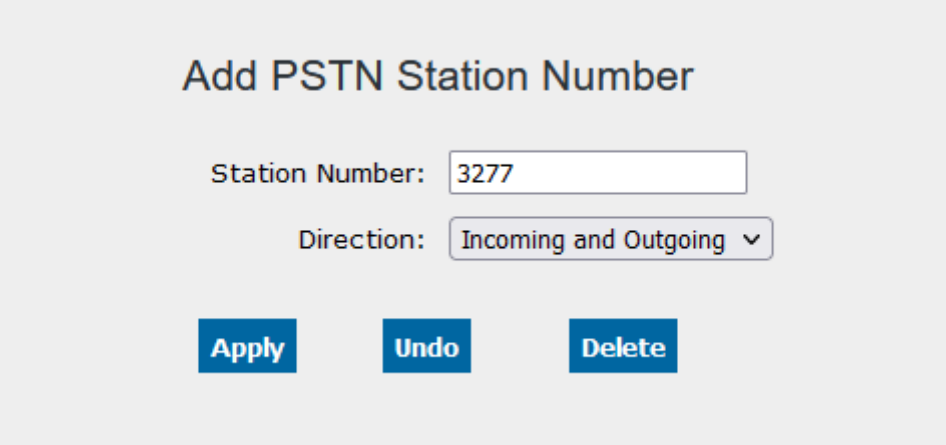


WAMLReplacement - PSTN-Partner

PSTN-Rufnummer

Mit dieser Nummer erreicht die WAML das Survivability Modem. Die Nummer wird auf dem S0-Satz mit der Nebenstelle 3277 konfiguriert. Die Rufrichtung muss auf Kommend und gehend eingerichtet werden.

Explorer > Routing > PSTN > PSTN-Partner > (1) WAML18 > PSTN-rufnummer hinzufügen



WAMLReplacement - PSTN-Rufnummer

Sie können das Ergebnis mit Explorer > Routing > PSTN > PSTN-Partner > WAML18 > Rufnummer anzeigen überprüfen.

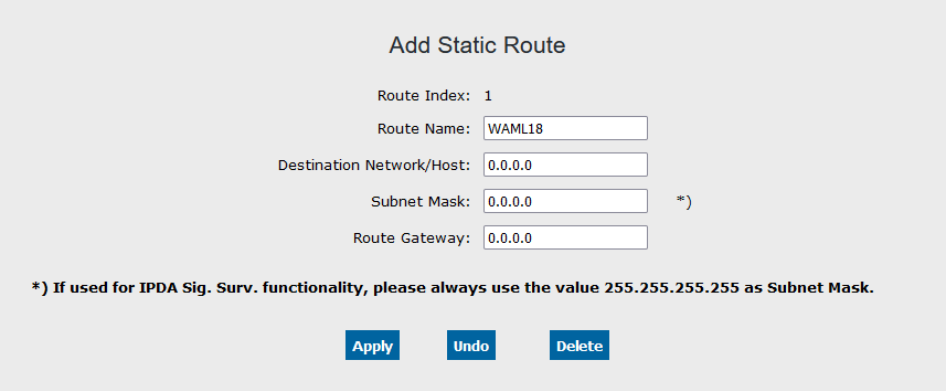
Statische Route

Für das Zielnetzwerk/Host wird die Signalisierungs-IP-Adresse der HG 3575 (NCUI) wie im Parameter APIPADDR im AMO APRT konfiguriert (172.28.0.57) eingetragen.

Für den Parameter Route-Gateway wird die ISDN IP-Adresse des Modems wie im AMO SIPCO, Parameter SURVNET+AP Nummer konfiguriert: 192.168.15.18

Die Ziel-Netzmaske muss für Tunneling auf 255.255.255.255 gesetzt werden. Daher ist der Netzmasken-Eintrag fest auf 255.255.255.255 kodiert und kann für STMI-Baugruppen mit WAML-Funktion nicht verändert werden.

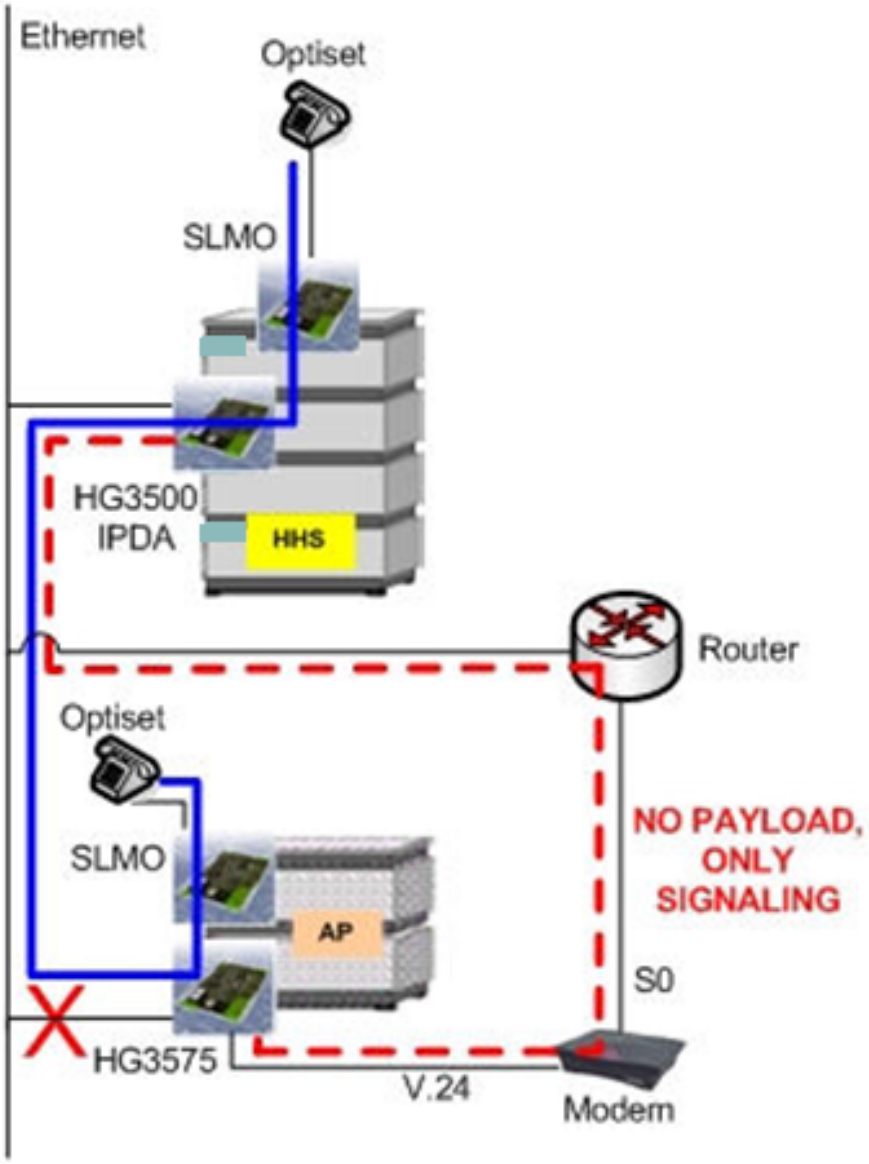
Explorer > Routing > IP-Routing > Statische Routen > WAML18



WAMLReplacement - Statische Route

Nun sichern Sie alle Änderungen (Disketten-Icon) und starten Sie die Baugruppe neu. Damit werden die Änderungen übernommen.

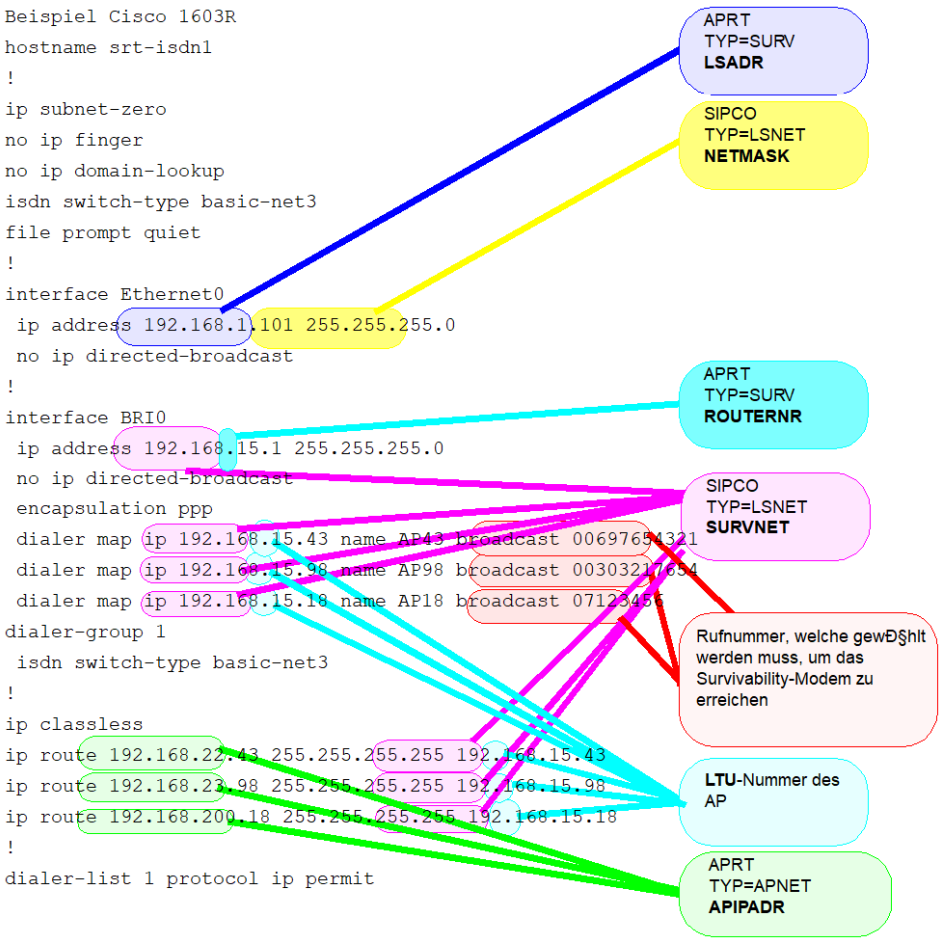
13.3.1.3.4 Externer ISDN-Router als Survivability Router



Signaling Survivability über einen Router (statt WAML Replacement)

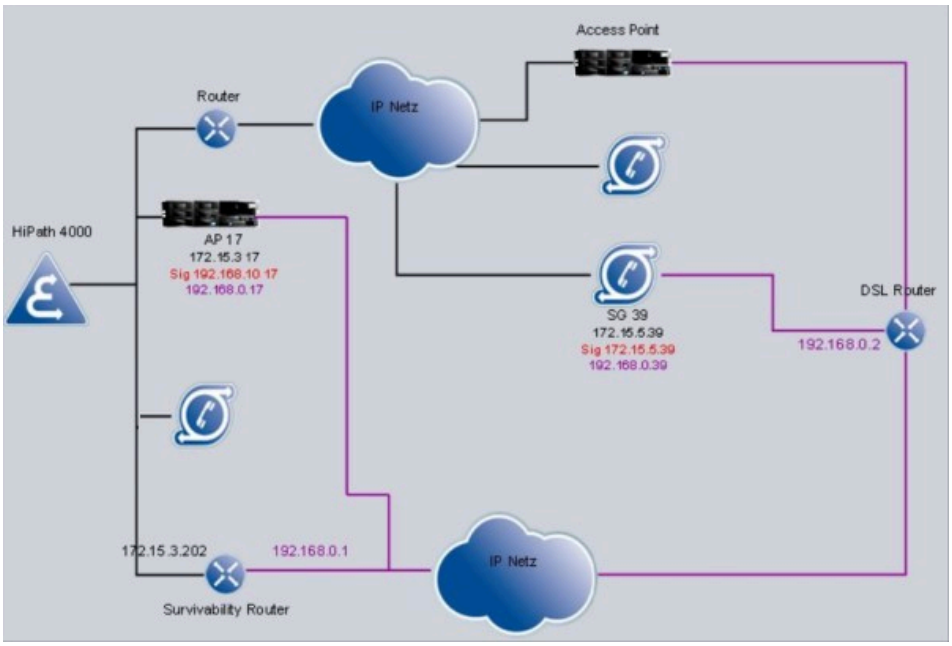
Als Beispiel werden die entsprechenden Einstellungen für einen externen Router *Cisco 1603R* dargestellt.

Wichtig: Die Auswahl des Routers ist als Beispiel zu verstehen und soll ausschließlich die Umsetzung der Parameter in eine Router-Konfiguration aufzeigen. Die getroffene Auswahl stellt weder eine spezielle Empfehlung dar, noch eine Aussage über die Lieferbarkeit. Es können natürlich auch Router anderer Produktlinien und Hersteller eingesetzt werden.



13.3.2 Signaling Survivability über alternatives LAN

13.3.2.1 Konfiguration der OpenScape 4000



Signaling Survivability über alternatives LAN

Die Konfiguration im OpenScape 4000 System geschieht folgendermaßen:

- Wenn Signaling Survivability über alternatives LAN genutzt werden soll, muss für den Access Point/das OpenScape 4000 SoftGate UDP als HSR-Signalisierung eingestellt werden.

Access Point (direct Link):

```
EINRICHTEN-
UCSU:ART=AP,LTG=1,LTU=17,LTSACHNR=â##Q2324-X10
“,SRCGRP=1,FRAMETYP=AP37009,VERBART=APDL,LSRTADR=172.15.3
ADR=172.15.3.1,STANDOID=722,STANDORT=â##722
 “,TEL=722,PL-
CHECK=JA,ANZBKAN=120,KONVLAW=JA,TCLASS=0,ALARMNR=0,IPMODE
V4=NEIN,DHCPV6=NEIN,SIUSPKZ=1,SIU=0,HZE=0,LANDKZ=0,SIGMOD
```

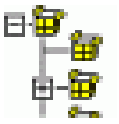
OpenScape 4000 SoftGate (networked Link):

```
EINRICHTEN-
UCSU:ART=AP,LTG=1,LTU=39,LTSACHNR=â##Q2329-X
“,SRCGRP=1,FRAMETYP=SOCOAP,VERBART=APNW,LSRTADR=172.15.3.
ADR=172.15.5.1,STANDOID=722,STANDORT=â##SG39
 “,TEL=722,PL-
CHECK=JA,ANZBKAN=250,KONVLAW=NEIN,TCLASS=0,ALARMNR=0,SOCO
0,IPMODE=IPV4,DHCPV4=NEIN,DHCPV6=NEIN,SIUSPKZ=1,SIU=0,HZE
KZ=0,SIGMODE=HSRUDP;
```

Wichtig: Bei Umschaltung von **HSRTCP** auf **HSRUDP** oder umgekehrt, muss immer ein `EXEC-USSU:ART=UPDATAP,LTU=<nummer>;` durchgeführt werden. Existierende Verbindungen werden ohne weitere Nachfrage getrennt!

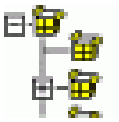
Anmerkung: Der SIPCO-Parameter SURVNET hat keine Auswirkungen auf das Leistungsmerkmal Signaling Survivability über alternatives LAN; im AMO APRT muss jedoch ein Eintrag erstellt werden, um einen Router hinzufügen zu können.

- Bekanntmachen der Survivability-Router im System

	**Configuration Management > Anlagendaten > IPDA -- > IPDA Signaling Survivability Router** Auf **Suchen** klicken, auf der Registerkarte „Router-Daten“ Router-Nummer und Adresse eintragen oder ändern, dann auf **Sichern** klicken.
	`EINRICHTEN-` `APRT:TYP=SURV,KONF=ROUTER,ROUTERNR=1,LSADR=172.15.3.202;`

Damit ist der Router 1 aus dem Beispiel in Bild 58 „Signaling Survivability über alternatives LAN“ eingerichtet.

- Zuordnen der Access Points zu den Survivability-Routern

	**Configuration Management > Anlagendaten> IPDA > IPDA Access Point** Auf **Suchen** klicken, auf der Registerkarte **Allgemein** die gewünschte Router-Nummer bei Signaling Survivability einstellen und auf **Sichern** klicken.

	`EINRICHTEN-`
	`APRT:TYPE=SURV,CONF=AP,LTU=17,ROUTERNR=1,SURVTYP=SUR▶`
	`VLAN,SURVIP=192.168.0.17,SURVNETM=255.255.255.0,SURV-`
	`RT=192.168.0.1,VLANTAG=NEIN,VLANID=0;`
	`EINRICHTEN-`
	`APRT:TYPE=SURV,CONF=AP,LTU=39,ROUTERNR=1,SURVTYP=SUR▶`
	`VLAN,SURVIP=192.168.0.39,SURVNETM=255.255.255.0,SURV-`
	`RT=192.168.0.1,VLANTAG=NEIN,VLANID=0;`

13.3.2.2 Konfiguration der LAN-Schnittstelle

Zusätzlich zu der Konfiguration mit den AMOs muss für die vHG 3575 im OpenScape 4000 SoftGate die LAN-Schnittstelle ausgewählt werden, die für Signaling Survivability genutzt werden soll.

WBM > Konfiguration > Signaling Survivability Schnittstelle

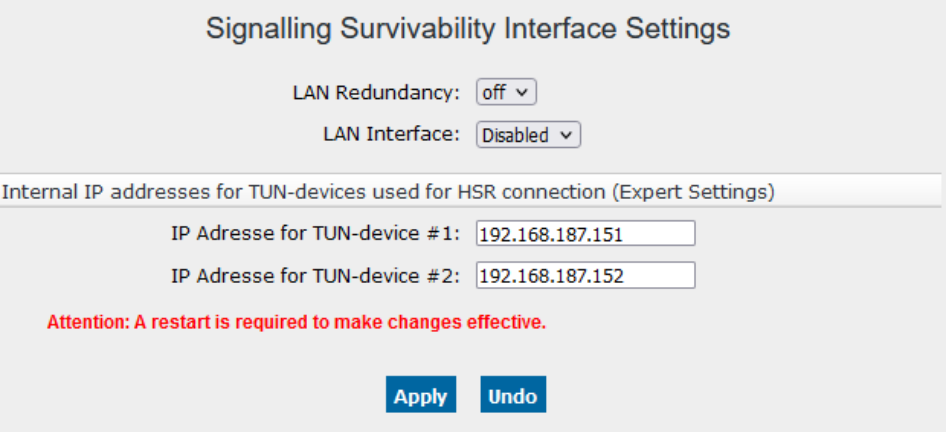


Abbildung 198: Signaling Surviivability LAN-Schnittstellen

13.3.2.3 Konfiguration des Routers

Beispiel für eine Routerkonfiguration

```
interface FastEthernet0/0
/*IP-Adresse und Netzmaske des Survivability LAN
  ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
/*IP-Adresse und Netzmaske des OpenScape 4000 LAN
 ip address 172.15.3.202 255.255.255.0
 duplex auto
 speed auto
!
ip route 0.0.0.0 0.0.0.0 172.15.3.1 /*IP-Adresse des
 Default Routers im OpenSca►
pe 4000 LAN
ip route 172.15.5.37 255.255.255.255 192.168.0.37
/*Routing für SoftGate 39
ip route 172.15.5.39 255.255.255.255 192.168.0.39
/*Routing für AP 17
ip route 192.168.10.17 255.255.255.255 192.168.0.17
```

13.3.2.4 Austausch einer defekten NCUI-Baugruppe durch eine neue NCUI-Baugruppe

Die Golden Load Loadware auf der NCUI-Baugruppe unterstützt nicht die UDP-Funktionalität, die für Signaling Survivability über alternatives LAN benötigt wird. Deshalb ist folgendes Vorgehen beim Baugruppentausch zu beachten.

Es gibt zwei Möglichkeiten:

Möglichkeit 1:

1) Vor der Inbetriebnahme der neuen NCUI die aktuelle Loadware auf die Baugruppe einspielen.

2) Den Baugruppentausch wie gewohnt durchführen (siehe auch „Gateways HG 3500 und HG 3575“ > Abschnitt 3.2.2, „Baugruppentausch“).

Möglichkeit 2:

1) Zuordnung des betroffenen Access Points zu Survivability-Router löschen.
2) `LOESCHEN-APRT:TYP=SURF,KONF=AP,LTU=<nummer>;`
3) Signalisierungsmode auf **HSRTCP** ändern.
4) `AENDERN-UCSU:ART=AP,LTU=<nummer>,SIGMODE=HSRTCP;`
5) Damit diese Änderung wirksam wird, muss der Access POint/das OpenScape 4000 SoftGate neu geladen werden.
6) `EXEC-USSU:ART=UPDATAP,LTU=<nummer>;`

Wichtig: Existierende Verbindungen werden ohne weitere Nachfrage getrennt!

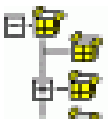
---

7) Neue NCUI-Baugruppe in Betrieb nehmen (siehe auch „Gateways HG 3500 und HG 3575“ > Abschnitt 3.2.2, „Baugruppentausch“).
8) **HSRUDP** als Signalisierungsmode wieder einrichten (siehe Abschnitt 3.1.1, „Konfiguration der OpenScape 4000“).
9) Zuordnung zum Survivability-Router wieder einrichten (siehe Abschnitt 3.1.1, „Konfiguration der OpenScape 4000“).

13.3.3 Ist Signaling Survivability gerade aktiv? (AB-UCSU)

Im Betrieb eines Systems mit Signaling Survivability kommt der Bedarf auf, ohne Auswertung irgendwelcher Fehlermeldungen spontan abzufragen, ob ein Access Point gerade normal über LAN, oder ob er in Signaling Survivability über Modem gesteuert wird.

Diese Abfrage leistet der AMO UCSU.

	Die Abfrage mit dem AMO UCSU kann nur über den Expertenmodus durchgeführt werden. **Expertenmodus > Expertenzugang > Open ...**<IP> mittels AMO (siehe AMO Kommando)
	`ABFRAGEN-UCSU:AP,1,;` Der AMO gibt eine Übersicht über alle eingerichteten Access Points aus, die nicht nur konfigurierte Parameter enthält, sondern auch aktuelle Betriebszustände.

```
+---------+------------------+---------+-------------
+----------+--------+
|ADRESSE   |SOLLAUSBAU         |ZUSTAND   |LTUC BAUGRUPPE|LTU
 TYP    |FRAMETYP|
|          +------------------+---------+-------------
+----------+--------+
|          |VERBART    STANDORTID STANDORT
          SRCGRP |
|          |TEL:                                FAX:
                 |
```

```
|         |LSRTADR          APRTADR          B-KAN ANZBKAN
 PLCHECK  SIGNAL. |
|         |IP MODE   DHCP V4  DHCP V6        AP REDUNDANCY
 TO APXY STATUS  |
|         |KONVLAW   KONTROLL-EINHEIT        TCLASS
 ALARMNR         |
|         |LANDKZ    SIGMODE
               |
|
 +-------------------------------------------------------------
+
|         |SIGNAL. ENCRYPTION AKTIV [ ]      PAYLOAD
 ENCRYPTION AKTIV [ ]  |
|         |SECURE-STATUS : SIEHE BESCHREIBUNG AM ENDE
               |
+---------+------------------+---------+--------------
+----------+---------+
|AP   1.17|EINGERICHTET       |READY    |Q2324-X10     |
AP37009   |AP37009 |
|         +------------------+---------+--------------
+----------+---------+
|         |APDL      722 722
              1 |
|         |TEL:  722                         FAX:
               |
|         |172.015.003.017  172.015.003.001   120   100
   JA   SURVLAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |  JA        HOST-CC                0
    0           |
|         |0           HSRUDP
               |
+---------+------------------+---------+--------------
+----------+---------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
               |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
               |
+---------+------------------+---------+--------------
+----------+---------+
|AP   1.18|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+--------------
+----------+---------+
|SOCOTYP  |APDL      722 722
              1 |
|SOCO1000 |TEL:  722                         FAX:
               |
|         |172.015.003.018  172.015.003.001   250   250
 NEIN     MODEM |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
```

```
|         |NEIN        HOST-CC                0
    0           |
|         |K           HSRTCP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : D   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.19|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+--------------
+----------+--------+
|SOCOTYP  |APDL      722 722
              1 |
|SOCO500  |TEL:  722                          FAX:
                |
|         |172.015.003.019  172.015.003.001   250   250
   JA       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |  JA        HOST-CC                0
    0           |
|         |0           HSRUDP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.26|EINGERICHTET       |READY    |Q2305-X35     |
AP37009   |AP37009 |
|         +------------------+---------+--------------
+----------+--------+
|         |APDL      722 722
              1 |
|         |TEL:  722                          FAX:
                |
|         |172.015.003.026  172.015.003.001    60    60
 NEIN       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |  JA        HOST-CC                0
    0           |
```

```
|         |0           HSRTCP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.27|EINGERICHTET       |READY    |Q2305-X35     |
AP37009   |AP37009 |
|         +------------------+---------+--------------
+----------+--------+
|         |APDL      722 722
              1 |
|         |TEL:  722                          FAX:
                |
|         |172.015.003.027  172.015.003.001    60    60
   JA       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP            |
|         |  JA        HOST-CC                0
    0           |
|         |0           HSRTCP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.36|EINGERICHTET       |READY    |Q2305-X35     |
INCH19    |INCH19  |
|         +------------------+---------+--------------
+----------+--------+
|         |APNW      722 722
              1 |
|         |TEL:  722                          FAX:
                |
|         |172.015.003.001  172.015.005.001    60    60
   JA     MODEM |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP            |
|         |NEIN        HOST-CC                0
    0           |
|         |0           HSRTCP
                |
```

```
+---------+------------------+---------+-------------
+----------+--------+
|         |SIUSPKZ : D   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+-------------
+----------+--------+
|AP   1.37|EINGERICHTET       |READY    |Q2305-X35     |
AP37009   |AP37009 |
|         +------------------+---------+-------------
+----------+--------+
|         |APNW      722 722
              1 |
|         |TEL:  722                          FAX:
                |
|         |172.015.003.001  172.015.005.001    60    60
 NEIN       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |NEIN        HOST-CC                0
    0           |
|         |0           HSRUDP
                |
+---------+------------------+---------+-------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+-------------
+----------+--------+
|AP   1.38|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+-------------
+----------+--------+
|SOCOTYP  |APNW      722 SG38
              1 |
|SOCO500  |TEL:  722                          FAX:
                |
|         |172.015.003.001  172.015.005.001   250   250
   JA     MODEM |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |NEIN        HOST-CC                0
    0           |
|         |0           HSRTCP
                |
+---------+------------------+---------+-------------
+----------+--------+
```

```
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.39|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+--------------
+----------+--------+
|SOCOTYP  |APNW      722 SG39
              1 |
|SOCO50   |TEL:  722                          FAX:
                |
|         |172.015.003.001  172.015.005.001   250   250
   JA       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP            |
|         |NEIN        HOST-CC                0
    0           |
|         |0           HSRUDP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+--------------
+----------+--------+
|AP   1.41|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+--------------
+----------+--------+
|SOCOTYP  |APDL      722 722
              1 |
|SOCO500  |TEL:  722                          FAX:
                |
|         |172.015.003.041  172.015.003.001   250   250
   JA       LAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP            |
|         |  JA        HOST-CC                0
    0           |
|         |0           HSRUDP
                |
+---------+------------------+---------+--------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
```

```
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+-------------
+----------+--------+
|AP   1.50|EINGERICHTET       |READY    |Q2329-X       |
AP37009   |SOCOAP  |
|         +------------------+---------+-------------
+----------+--------+
|SOCOTYP  |APNW      722 SG50
             1 |
|SOCO500  |TEL:  722                          FAX:
                |
|         |172.015.003.001  172.015.005.001   250   250
   JA   SURVLAN |
|         |    IPV4  NEIN     NEIN           AP REDUNDANCY
 TO AP           |
|         |NEIN        HOST-CC                0
    0           |
|         |0           HSRUDP
                |
+---------+------------------+---------+-------------
+----------+--------+
|         |SIUSPKZ : 1   SIU : 00   HZE : 00
                |
|
 +-------------------------------------------------------------
+
|         |CP / SIU :  KEIN UNTERSCHIED VON ZAND
                |
+---------+------------------+---------+-------------
+----------+--------+
```

13.4 Relevante AMOs

Tabelle 75: Parameter des AMO APRT im EINRICHTEN-Zweig unter TYP=SURV, KONF=ROUTER

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	ROUTERNR	d	Nummer des Routers für Signaling Survivability. IPDA unterstützt bis zu 10 Survivability Router, welche von 1..10 durchnummeriert und über diesen Index verwaltet werden.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ROUTERNR	e	Number of the Router for Signaling Survivability. IPDA supports up to 10 survivability routers, numbered 1..10 which are administered using this index.
	LSADR	d	IP-Adresse eines Routers für Signaling Survivability im OpenScape 4000 LAN Segment. Diese IP-Adresse muss zum OpenScape 4000 LAN Segment gehören (siehe IP Distributed Architecture > Parameter **NETADR** im AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“)
	LSADR	e	IP Address of a Router for Signaling Survivability in the OpenScape 4000 LAN Segment. This IP address must belong to the OpenScape 4000 LAN Segment (see IP Distributed Architecture > parameter **NETADR** in AMO SIPCO, Tabelle 13 „Parameter AMO SIPCO im EINRICHTEN-Zweig,bzw. für AENDERN unter TYP=LSNET“)

Tabelle 76: Parameter des AMO APRT im EINRICHTEN-Zweig unter TYP=SURV, KONF=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
APRT	ROUTERNR	d	Nummer des Routers für Signaling Survivability. Bestimmt einen der bis zu 10 Survivability Router, über den dieser Access Point erreicht werden soll.
	ROUTERNR	e	Number of the Router for Signaling Survivability. Selects one of the up to 10 survivability routers, via which this Access Point shall be reached.

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	SURVTYP	d	MODEM = Signaling Survivability über Modem SURVLAN = Signaling Survivability über alternatives LAN
	SURVTYPE	e	MODEM = Signaling survivability via modem SURVLAN = Signaling survivability via alternate LAN

Tabelle 77: Parameter des AMO UCSU im EINRICHTEN-/AENDERN-Zweig unter ART=AP

AMO	Parameter	Sprache/ Language	Beschreibung/Description
UCSU	SIGMODE	d	HSRTCP: HSR über TCP-Verbindung HSRUDP: HSR über UDP-Verbindung
	SIGMODE	e	HSRTCP: HSR via TCP connection HSRUDP: HSR via UDP connection

14 SIP-Konnektivität

14.1 Übersicht

Die folgenden SIP-Schnittstellen stehen OpenScape 4000 zur Verfügung:

- SIP-Teilnehmer
- UFIP-Geräte
- SIP-Trunking

14.1.1 Schnittstellen

14.1.1.1 SIP-Teilnehmer

Das Leistungsmerkmal „SIP-Teilnehmer für OpenScape 4000“ umfasst den Betrieb von SIP-Endpunkten, die mithilfe eines Gateways (virtuelles HG 3500 oder HG 3500) auf einem OpenScape 4000-System unterhalten werden können.

14.1.1.2 UFIP-Geräte

UFIP (Universal Feature access IP) ist eine neue SIP-Geräteschnittstelle mit erweiterter CSTA-Unterstützung.

Die UFIP-Schnittstelle stellt Circuit-Konnektivität bereit.

UFIP ist die bevorzugte SIP-Geräteschnittstelle.

14.1.1.3 SIP-Trunking

OpenScape 4000 unterstützt:

1) SIP-Q Trunking (z. B. für die Verbindung zu OpenScape Voice)
2) • Native SIP-Trunking (z. B. für die Verbindung zum SIP-Service-Provider)

14.1.2 Unterstützte RFCs (Anfrage für Kommentare) für SIP-Schnittstellen

Tabelle 78: Unterstützte RFCs (Anfrage für Kommentare) für SIP-Schnittstellen

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 2198	RTP Payload for Redundant Audio Data	Ja	Ja	Ja

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 2246	The TLS Protocol Version 1.0	Ja	Ja	Ja
RFC 2327	SDP: Session Description Protocol (veraltet durch RFC4566)	Ja	Ja	Ja
RFC 2396	Uniform Resource Identifiers (URI): Generische Syntax	Ja	Ja	Ja
RFC 2617	HTTP-Authentifizierung: Basis- und Digest-Zugangsauthentifizierung	Ja	Ja	Ja
RFC 2782	DNS RR for specifying the location of services (DNS SRV)	Nein	Ja	Ja
RFC 2833	RTP-Nutzlast für DTMF-Ziffern, Telefonie-Töne und Telefonsignale	Ja	Ja	Ja
RFC 2976	Die SIP INFO-Methode	Nein	Nein	Ja
RFC 3204	MIME media types for ISUP and QSIG Objects	Ja	Ja	Ja
RFC 3261	SIP: Session Initiation Protocol	Ja	Ja	Ja
RFC 3262	provisional Response Acknowledgement (PRACK) Early Media	Ja	Ja	Ja
RFC 3263	SIP Locating Servers	Nein	Ja	Ja
RFC 3264	An Offer/Answer Model with SDP	Ja	Ja	Ja
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification	Ja	Nein	Nein
RFC 3310	HTTP Digest Authentication	Ja	Ja	Ja
RFC 3311	Session Initiation Protocol (SIP) UPDATE Method	Ja	Ja	Ja

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)	Ja	Ja	Nein
RFC 3324	Short Term Requirements for Network Asserted Identity	Ja	Ja	Ja (aber kein Anwendungsfall)
RFC 3325	Private Erweiterungen zum Session Initiation Protocol (SIP) für die behauptete Identität in vertrauenswürdigen Netzen	Ja	Ja	Nein
RFC 3326	The Reason Header Field for the Session Initiation Protocol (SIP)	Nein	Nein	Ja
RFC 3484	Default Address Selection for Internet Protocol version 6 (IPv6)	Ja	Ja	Ja
RFC 3515	Das Session Initiation Protocol (SIP) Refer Method[5]	Ja	Ja	Nein
RFC 3550	RTP: Transportprotokoll für Echtzeitanwendungen	Ja	Ja	Ja
RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control	Ja	Ja	Ja
RFC 3581	An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	Nein	Ja	Nein
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	Ja	Ja	Ja

[5] Refer wird nur für SIP-Abonnenten und native SIP-Trunks (konfigurierbar in WBM > SIP-Trunk-Profilen) unterstützt - (ICHT EMPFOHLEN FÜR SIP-Dienstanbieter aufgrund von Buchhaltung, Abrechnung, Berechtigungen usw.)

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 3725	Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)	Ja	Nein	Ja
RFC 3830	MIKEY: Multimedia Internet KEYing	Nein	Ja	Ja
RFC 3842 (teilweise)[6]	Message Waiting Indication Event Package	Ja	Ja	Nein
RFC 3891	The Session Initiation Protocol (SIP) Replaces Header	Ja	Ja	Nein
RFC 3892	Der Referred-By-Mechanismus von Session Initiation Protocol (SIP) [7]	Ja	Ja	Nein
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)	Ja	Ja	Ja
RFC 4119	Ein präsenzbasiertes GEOPRIV-Standort-Objektformat	Nein	Ja	Ja
RFC 4291	IP Version 6 Addressing Architecture	Ja	Ja	Ja
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams	Ja	Ja	Ja

6 "teilweise" bedeutet, dass nur das statische Abonnement auf Voicemail Server unterstützt wird (in ausgehender Richtung). OpenScape 4000 unterstützt kein dynamisches Abonnement in ausgehender Richtung, d. h. es wird keine SUBSCRIBE-Nachricht gesendet. Die statische Subscription ist typisch für PBX (wie OpenScape 4000) und dynamische Subscription ist typisch für SIP Clients. In kommender Richtung (z. B. von einem SIP Client zu OpenScape 4000) unterstützen wir sowowhl statische als auch dynamische Suebscription.

7 Refer wird nur für SIP-Abonnenten und native SIP-Trunks unterstützt (konfigurierbar in WBM- > SIP-Trunk-Profilen) - (NICHT EMPFOHLEN FÜR SIP-Dienstanbieter aufgrund von Buchhaltung, Abrechnung, Berechtigungen usw.)

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 4733	RTP-Nutzlast für DTMF-Ziffern, Telefonie-Töne und Telefonsignale	Ja	Ja	Ja
RFC 5009	Private Header (P-Header) Erweiterung zum SIP zur Autorisierung von frühen Medien	Nein	Ja	Nein
RFC 5139	Überarbeitetes Bürgerliches Standortformat für Presence Information Data Format Location Object (PIDF-LO)	Nein	Ja	Ja
RFC 5246	Transport Layer Security (TLS) Protocol Version 1.2	Ja	Ja	Ja
RFC 5491	Nutzungserklärung, Überlegungen und Empfehlungen für GEOPRIV Presence Information Data Format Location Object (PIDF-LO)	Nein	Ja	Ja
RFC 5746	Transport Layer Security (TLS) Renegotiation Indication Extension	Ja	Ja	Ja
RFC 5806	Umleitungsanzeige in SIP	Ja	Ja	Nein
RFC 5923	Connection Reuse in the Session Initiation Protocol (SIP)	Ja	Ja	Ja
RFC 6140	Registrierung für mehrere Telefonnummern im Session Initiation Protocol (SIP)[8]	Nein	Ja	Ja

[8] nur möglich, wenn ein SIP-Trunk-Profil verwendet wird.

RFC-Nummer	Titel	Schnittstellen:		
		Abonnent	Native Trunk	SIP-Q
RFC 6716	Definition of the Opus Audio Codec	Ja	Ja	Ja
RFC 7433	Ein Mechanismus für den Transport von Benutzer-zu-Benutzer-Anrufsteuerungsinformationen in SIP	Nein	Ja	Ja
RFC 7852	Zusätzliche Daten im Zusammenhang mit einem Notruf	Nein	Ja	Ja
RFC 7044	Eine Erweiterung zum Session Initiation Protocol (SIP) für die Anfrage-Verlaufsinformationen	Nein	Ja	Ja
RFC 8446	Transport Layer Security (TLS) Protocol Version 1.3	Nein	Ja	Ja

14.1.3 Verwendete Baugruppen

Die Common-Gateway-Baugruppe HG 3500 und die virtuelle HG 3500 im OpenScape 4000 SoftGate unterstützen SIP-Connectivity. Für Details siehe „Gateways HG 3500 und HG 3575“, Kapitel 3, „Unterstützte Gateways“ und die Dokumentation zu „OpenScape 4000 SoftGate“.

14.1.4 Konfigurieren des Gateway-Ports

- UDP
- UDP ist an SIP-Teilnehmer- und Native SIP-Trunk-Schnittstellen als Transportprotokoll zulässig. Es werden symmetrische UDP-Ports verwendet. Der UDP Listening-Port wird mit dem AMO-Parameter SIPTCPP konfiguriert.
- TCP/TLS
- Als Quell-Ports werden vorübergehende Ports verwendet. RFC 5923: Die Session Initiation Protocol (SIP)-Funktion Connection Reuse wird für die Wiederverwendung von TCP- und TLS-Verbindungen unterstützt.

  Der TCP Listening-Port wird mit dem AMO-Parameter SIPTCPP und der TLS Listening-Port mit dem AMO-Parameter SIPTLSP konfiguriert.

14.2 SIP-Teilnehmer

In OpenScape 4000 V8 ist UFIP die bevorzugte Methode zum Konfigurieren von SIP-Teilnehmern. Sollten bei einer früheren S0PP-Konfiguration Funktionsabweichungen auftreten, ist dies über das Kundenticket zu melden.

Bis zu 240 „Native SIP“-Teilnehmer können am gemeinsamen Gateway HG 3500 und der virtuellen HG 3500 konfiguriert werden. Die Gesamtzahl von 240 IP-Teilnehmern pro gemeinsamem Gateway (CGW) bezieht sich auf HFA- und SIP-Teilnehmer (z. B. 200 HFA- und 40 SIP-Teilnehmer).

SIP-Teilnehmer können sich auch über das Internet verbinden (siehe Secure Remote Subscriber on page 397).

14.2.1 SIP-Endpunkte

Folgende SIP-Endpunkte werden unterstützt:

- OpenStage SIP-Familie*
- OpenScape CP SIP-Familie
- LifeSize Phone (Audiokonferenz)
- OpenStage WL3/WL4
- OpenScape Personal Edition SIP
- Mediatrix Analog Access Points 41xx
- Mediatrix 44xx (OpenScape 4000 SoftGate)*
- LifeSize Express, Team und Room **nur** am OpenScape 4000 SoftGate (siehe „OpenScape 4000 SoftGate“ > Videoverbindungen auf Seite 354)
- OpenScape UC Web Embedded Client

Dieses Leistungsmerkmal umfasst in beide Ruf-Richtungen

- G.7xx, Audioanrufe
- G.711, transparente FAX-/MODEM-Anrufe

_____ * Eine projektspezifische Freigabe wird benötigt.

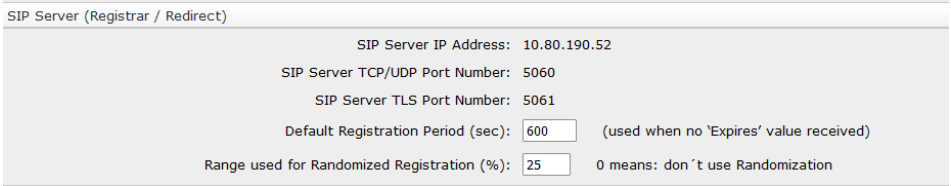
14.2.2 Service-Informationen

- RFC 2833 (DTMF via RTP) und RFC 2198 (Unterstützung für Redundant Audio Data) werden unterstützt.
- Die folgende Tabelle zeigt die Kombinationen der Parameter **SECZONE**, **USERID** und **PASSWD** in AMO SBCSU, um eine sichere Registrierung zu ermöglichen.

Parameter			
SECZONE	USERID	PASSWD	möglich
gesetzt	gesetzt	gesetzt	ja
nicht gesetzt	gesetzt	gesetzt	ja
gesetzt	nicht gesetzt	gesetzt	ja

Parameter			
SECZONE	USERID	PASSWD	möglich
nicht gesetzt	nicht gesetzt	gesetzt	ja
gesetzt	nicht gesetzt	nicht gesetzt	nein
nicht gesetzt	gesetzt	nicht gesetzt	nein
gesetzt	gesetzt	nicht gesetzt	nein
nicht gesetzt	nicht gesetzt	nicht gesetzt	ja

- Als zusätzliche Sicherheitsmaßnahme schränkt die Konfiguration des SUBIPADD-Parameters die Client-Registrierung auf die definierte IP-Adresse ein und verhindert die Registrierung mehrerer Clients (mehrere IPs) unter demselben Teilnehmer.
- Jeder Registerwert, der von einem Partner angeboten wird, wird mit einem Standard-Randomisierungswert von 25 % bewertet (um Lastspitzen zu vermeiden). Wenn kein Wert angegeben wird, wird ein Standardwert von 600 Sekunden (10 Minuten) verwendet. Sowohl der Randomisierungs-Timer (0% deaktiviert die Randomisierung) als auch die Standardzeit (wenn keine empfangen wird) sind konfigurierbar. Für den **Standardregistrierungszeitraum** ist der Bereich 120-3600 zulässig. Die neuen Konfigurationsparameter ersetzen die alten und sind unter **WBM > Konfiguration > Voice Gateway > SIP-Parameter** zu finden.



1) Mit diesem Bereich wird ein Zufallstimer zwischen diesem Bereich für weitere Neuregistrierungen nach der ersten Meldung SIP REGISTER verwendet.

Die übliche minimal zulässige Zeit für die SIP-Registrierung ist fest auf 120 Sekunden programmiert. Bei mehr als 60 konfigurierten Teilnehmern beträgt die minimale Zeit 120 + die Anzahl der SIP-Teilnehmer über 60. Bei 65 Teilnehmern beträgt die minimale Zeit also beispielsweise 125 Sekunden, bei 70 Teilnehmern 130 Sekunden usw.

NOTICE: Es wird empfohlen, einen Wert von 20 SIP-Registrierungsnachrichten pro Sekunde nicht zu überschreiten.

14.2.3 Leistungsmerkmale

Table 79: UFIP SIP-Merkmale-Übersicht

Leistungsmerkmal	UFIP SIP
CLIP/CLIR	☑
COLP/COLR	☑
Namensanzeige	☑
Anrufweiterleitung (keine Antwort, besetzt, bedingungslos)?	☑
Halten / Abrufen / Umschalten	☑
Direktes Anruf-Parken	☑
Anrufübergabe nach Melden	☑
Halb besuchte Anrufweiterleitung	☑
Lokale 3-Parteien-Konferenz (falls vom SIP-Terminal unterstützt)	☑
Message Waiting Indication (MWI) (weitere Informationen finden Sie in Abschnitt 2.5.7, "Message Waiting Indication (MWI)")	☑
Anrufschutz	☑
CSTA/ACL-Überwachung des SIP-Teilnehmers	☑
Sammelanschluss mit SIP-Abonnent als Slave	☑
T.38 Fax-Verbindungen mit Mediatrix 41xx	☑
DTMF-Signalisierung (Inband und RFC2833 konform)	☑
SIP Session Timer RFC4028-konform (weitere Informationen finden Sie in Abschnitt 2.4, "Restrictions")	☑
Digest-Authentifizierung	☑
Nummernkennung	☑
Zweitanruf (annehmen, zurückweisen oder weiterleiten)	☑
Zweitanruf (den zweiten Anruf weiterleiten, halten)	☑

Leistungsmerkmal	UFIP SIP
SIP-Teilnehmer als Mitglied/Master einer ONS-Gruppe (siehe OpenScape 4000-Dokumentation, **Abschnitt 3 - Beispiele für die Nutzung von Leistungsmerkmalen > Paralleles Klingeln - One Number Service (ONS)**)	☑
SIP-Teilnehmer als DR-Taste eines Tischtelefons	☑
SIP-Peer-Filtering	☑
Unterstützte RFCs (siehe Abschnitt 1.2, "Unterstützte RFCs (Request for Comments) für SIP-Schnittstellen").	☑
Programmierung der zentralen Anrufumleitung (CFU, CFNR, CFB)	☑
Aktivierung der Remote-Anrufumleitung	☑
Rufnummernunterdrückung	☑
Blinde Weiterleitung	☑
Wiederanruf nach Übergabe	☑
Aufschalten und Freigeben/Aufschalten bei Notruf (nur Aufruf. UFIP-Geräte können nicht eingedrungen/erzwungen freigegeben werden)	☑
Anrufübernahmegruppe	☑
Rückruf bei "Besetzt" mit WL3/WL4-Telefonen. Zur Konfiguration lesen Sie bitte Kapitel 8, "OpenStage WL3/WL4 Konfiguration".	☑
Anzeigeunterdrückung mittels Zugangscode (DISUON/DISUOFF)	☑
Privatgespräch mittels Zugangscode und PIN	☑
Bis zu fünf Teilnehmer haben sich mit der gleichen Nummer angemeldet	☑
Unterstützung der Registrierung mit E.164-Nummer (mit und ohne vorangestelltes +) und nur mit Durchwahl	☑
ACL/CSTA-Services: Anrufen/Defekt/SST usw.	☑
ACL/CSTA: Monitor Set	☑
ACL/CSTA: Monitor Abbrechen	☑
ACL/CSTA: Gerätetyp prüfen	☑
ACL/CSTA: Get Switching Function Devices	☑

Leistungsmerkmal	UFIP SIP
ACL/CSTA: Snapshot-Aufruf	☑
ACL/CSTA: Anrufannahme	☑
ACL/CSTA: Snapshot Monitor	☑
ACL/CSTA: Anruf umleiten	☑
ACL/CSTA: Anruf fortsetzen	☑
ACL/CSTA: Predictive Call tätigen	☑
ACL/CSTA: Anruf ablehnen	☑
Busy Override, Emergency Intrusion und Emergency Disconnect	☑
Logische Geräteinformationen abrufen	☑
Switch-Funktionsgeräte	☑
Überwachungsfilter ändern	☑
Alternativer Anruf - Rückfrageverbindung muss über den Rückfragedienst initiiert worden sein	☑
Telefonkonferenz - Rückfrageverbindung muss über den Rückfragedienst initiiert worden sein	☑
Anruf initiieren – Der Client muss die in OSCAR SIP Client-Spezifikation definierte Prozedur 9.18.1.1. unterstützen. https://sp2013.myatos.net/org/usp/_layouts/DocIdRedir.aspx?ID=5SMA7FHWUQFR-1472063257-248304 TIPP: Bei Unify Phone muss **Konfiguration > Eingehende Anrufe > CTI > Auto-Antwort zulassen** aktiviert sein, um die Funktion zu ermöglichen.	☑
Anruf wiederverbinden - Rückfrageverbindung muss über den Rückfragedienst initiiert worden sein	☑
Anruf übergeben - Rückfrageverbindung muss über den Rückfragedienst initiiert worden sein	☑
Nicht stören abrufen - System nicht stören abrufen	☑
Weiterleitung abrufen - Status der Systemanrufweiterleitung abrufen	☑
Nicht stören setzen - System nicht stören setzen	☑

Leistungsmerkmal	UFIP SIP
Anrufumleitung definieren – Systemanrufumleitung definieren	☑
Anrufannahmedienst - Der Client muss die in der OSCAR SIP Client-Spezifikation definierte Prozedur 9.18.1.1 unterstützen. https://sp2013.myatos.net/org/usp/_layouts/DocIdRedir.aspx?ID=5SMA7FHWUQFR-1472063257-248304 TIPP: Bei Unify Phone muss **Konfiguration > Eingehende Anrufe > CTI > Auto-Antwort zulassen** aktiviert sein, um die Funktion zu ermöglichen.	☑
SIP-Teilnehmer unterstützen Remote-Teilnehmer mit OS-SBC Einschränkung: OS-SBC unterstützt keine Cluster-Server-Zuordnung für Remote-Abonnenten, wie beispielsweise für ATC in Remote-Endpunkten. Dies führt zu einer Begrenzung auf 240 registrierte SIP-Teilnehmer pro Gateway. Es wird nur der Clustered Mode mit Routing-Präfix unterstützt, der die Einschränkung erweitern könnte.	☑

IMPORTANT: Alle weiteren Leistungsmerkmale, die von den SIP-Endgeräten angeboten werden, aber die Unterstützung der Baugruppe bräuchten, funktionieren nicht.

SIP-Telefone verhalten sich anders als HFA- oder digitale Telefone (z. B. OpenStage HFA/T). Aufgrund des unterschiedlichen Verhaltens von SIP-Telefonen zeigt die ACL-Überwachung in einigen Aufrufszenarien andere Überwachungsströme im Vergleich zur ACL-Überwachung digitaler Nebenstellen.

HiPath CAP V3.0 R9 (oder höher) wird für die entsprechenden CSTA Services benötigt. Diese sind

- CSTA Monitor Start/Stop
- CSTA Snapshot Device/Call
- CSTA Get Device Type
- CSTA Get Switching Function Devices

Die BLF WIN-Applikation R15.4.0 (Belegtlampenfeld) unterstützt diese neue CSTA-/ACL-Überwachungsfunktion und kann den Gerätestatus im Belegtlampenfeld der Teilnehmerkonsolen anzeigen.

Passive Leistungsmerkmale

Die folgenden Leistungsmerkmale können SIP-Teilnehmer zwar nicht aktivieren, sie können aber passiv eingebunden werden:

- (S0PP & UFIP) Rückruf besetzt/nicht melden (Auf ein SIP-Endgerät kann ein Rückruf im Frei- bzw. Besetztfall eingetragen werden, das SIP-Endgerät selbst kann keinen Rückruf eintragen).
- *CCBS wird für WL3/WL4-Geräte als aktives Merkmal unterstützt.
- (S0PP) Der SIP-Teilnehmer kann den Code für die Anrufübernahme nicht wählen, aber ein passives Mitglied der Anrufübernahmegruppe sein. Das

bedeutet, dass andere Teilnehmer der Anrufübernahmegruppe Anrufe mit der Rufnummer des SIP-Teilnehmers als Zielnummer übernehmen können.

UFIP WABE DARs

Die folgenden WABE-DARs sind über ein UFIP-Gerät verfügbar:

- DUSABE
- ANKLAS
- AUN
- ACDLOGON
- ACDLOGOF
- ACDNVB
- ACDARB
- EIGENKZ
- TRENNEN
- NOTAUF
- FLTRACE
- QUER
- QUVPL
- KUWAZ1
- KUWAZ2
- MELDEN
- ALTROUTE
- RFAMTUA
- RFHAUSUA
- AMT
- SAMMEL
- SAESPR
- SAASPR
- NOEC
- TLN
- TLNTR
- VPL
- VPI
- APIN
- PINAUS
- ANZUEIN
- ANZUAUS
- PSMSUN
- PSMSUD
- PSMMEL
- AULEEXIN
- AULEKA
- AULEB
- AULASPR
- AULESPR
- AULFESPR
- AULFASPR
- NAVAR

Unterstützung von uaCSTA

OpenScape 4000 unterstützt uaCSTA nur für CSTA-Anfragen, nicht aber für CSTA-Ereignisse. Eine Liste der unterstützten Anfragen finden Sie in Anhang D von CSTA-Konnektivitätsadapter - Anwendungsentwicklerhandbuch (ADG).

Unterstützung von partiellem Rerouting (SIP 302 Moved Temporary)

OpenScape 4000 unterstützt partielles Rerouting, ausgelöst durch SIP 302 Moved Temporary (Contact Header).

Um das Leistungsmerkmal zu aktivieren, muss der COT-Parameter
AULN und RWSN (Deutsch)

FWDN und FNAN (Englisch)

müssen eingestellt werden.

14.2.4 Einschränkungen

14.2.4.1 Einschränkungen der System-Leistungsmerkmale

Die folgenden Systemmerkmale können von SIP-Endgeräten nicht verwendet werden:

- Chef / Sekretär - SIP-Endgeräte können nicht als Chese-Mitglied eingerichtet werden.
- Keyset-Funktionalität - SIP-Endgeräte können nicht als Keysets eingerichtet werden.
- ACD (automatischer Rückruf (CCBS / CCNR))
- Zeugenzuschaltung - Ein SIP-Endgerät kann nur der passive Teilnehmer bei Zeugenzuschaltung sein.
- Fangen - Ein SIP-Endgerät kann zwar gefangen werden, kann aber nicht selbst eine Verbindung fangen.
- UFIP-Geräte greifen auf Systemfunktionen zu, indem sie die gesamte Ziffernzeichenkette auf einmal senden. Derzeit ist diese Zeichenkette auf 22 Stellen begrenzt. Um zum Beispiel die "Fernweiterleitung" zu aktivieren, muss der UFIP-Benutzer wählen: <AFWDREM_WABE_CD><src_STNO_#><PIN_src_STNO#><dest_STNO_#> - Die gesamte Zeichenfolge darf nicht länger als 22 Ziffern sein.
- Um eine PIN von einem UFIP-Gerät zu aktivieren, muss PINNKEY in der entsprechenden PERSI/COPIN auf **JA** gesetzt werden.
- Bei Aktivierung eines Merkmals von einem SIP-Gerät (konfiguriert als UFIP-Abonnent) gibt es keine Bestätigung auf dem Gerätedisplay, dass das Merkmal aktiviert wurde.
- Kein DMC in UFIP-UFIP, in den Aufzeichnungsfällen.

14.2.4.2 Einschränkungen der Terminal-Leistungsmerkmale

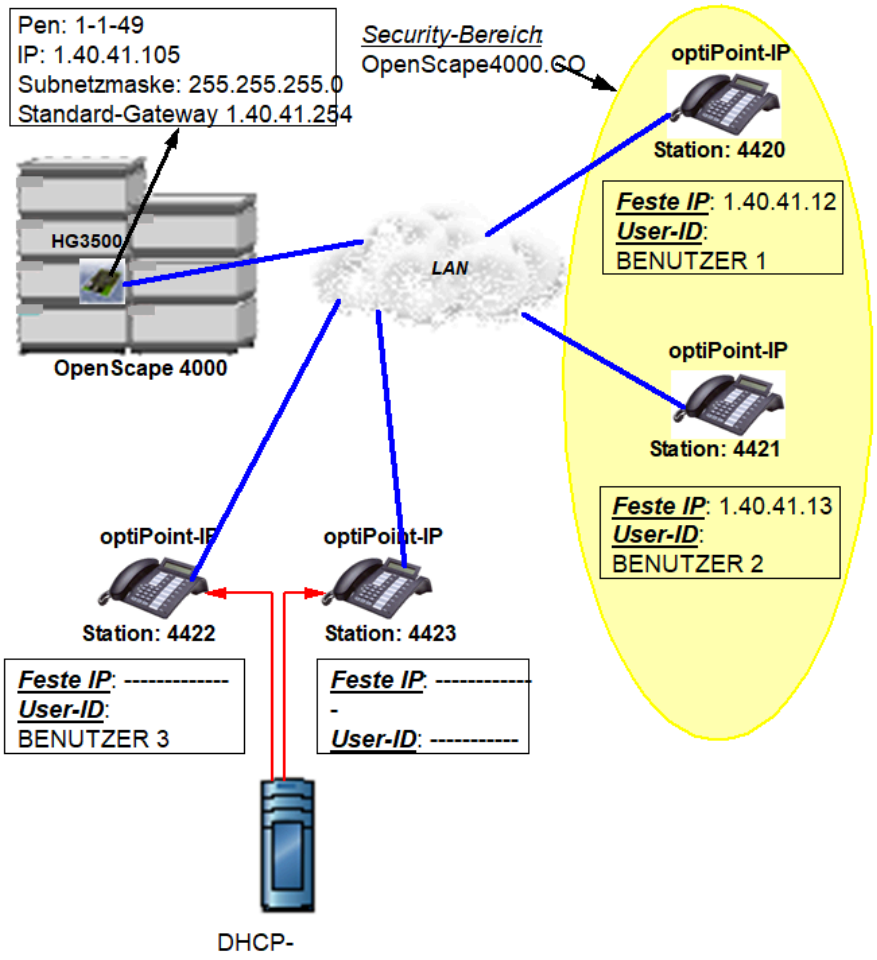
Folgende Einträge müssen bei den SIP-Endgeräten (entweder im DLS oder direkt am Endgerät) gesperrt werden, weil diese Leistungsmerkmale von der OpenScape 4000 **nicht** unterstützt werden:

- Umgeleitete Anrufe protokollieren
- Anzeige Rufnummer
- Wartemusik
- Nachricht wartet
- Automatische Wiederaufnahme
- Parken
- Übernahme geparktes Gespräch
- Rückruf nach Besetzt (nur mit WL3/WL4-Telefonen unterstützt)
- Rückruf nach nicht Melden

14.2.4.3 Allgemeine Einschränkungen

Die parallele Registrierung ist generell nur für die Nutzung mit Circuit und OpenScape Mobile Clients freigegeben. Der Endpunkt, der Funktionen wie die Rufumleitung aufruft, wird nicht unterstützt, wenn die Mehrfachregistrierung für einen anderen SIP-Client-Typ aktiv ist.

14.2.5 Konfiguration



14.2.5.1 STMI2/4- und STMIX-Baugruppenkonfiguration



Configuration Management > Systemdaten > Baugruppe > CGW-Funktionsblock

Klicken Sie auf **Neu**, geben Sie die entsprechenden Daten ein und klicken Sie auf **Speichern**.

Configuration Management > Systemdaten > Baugruppe > Baugruppe

Klicken Sie auf **Neu**, geben Sie die entsprechenden Daten ein (Header-Informationen, Registerkarte **Allgemeine Baugruppendaten**, Registerkarte **STMI2-IGW-Baugruppendaten**, **CGW-Funktionen**) und klicken Sie auf **Speichern**.



```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=SIP,BGBKAN=BKAN60;

AENDERNBFDAT:
 CONFIG=WEITER,FCTBLK=1,FUNCTION=SIP,ANZSATZ=10,
 ANZB▶
KAN=10;

AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA;
EINRICHTENBCSU:
 TYP=IPGW,LTG=1,LTU=1,EBT=49,SACHNR=âQ2316-X ",FC▶
TID=1,FCTBLK=1;
EINRICHTENCGWB:
 LTU=1,EBT=49,SMODE=NORMAL,IPADR=1.40.41.105,NET▶
MASK=255.255.255.0,DEFRT=1.40.41.254;
```

Die Parameter **GWAUTREQ** und **SIPREG** müssen auf NEIN gestellt sein, falls die Baugruppe für SIP-Teilnehmer verwendet wird.

```
AENDERN-
CGWB:MTYP=CGW,LTG=1,LTU=1,SLOT=49,TYP=SIPTRERH,GWAUTREQ=NEIN;
AENDERN-
CGWB:MTYP=CGW,LTG=1,LTU=1,SLOT=49,TYP=SIPTRSSA,SIPREG=NEIN;
```

14.2.5.2 Konfigurieren eines SIP-Teilnehmers

Wichtig: Die Konfiguration der HG 3500 (CGW)-Baugruppe ist eine Voraussetzung für die Unterstützung von SIP-Teilnehmern (siehe Abschnitt 2.5.1, „STMI2/4- und STMIX-Baugruppenkonfiguration“).

Wichtig: Werden die Parameter **SECBER**, **KENNUNG** und **PASSWD** für eine gesicherte Registrierung im AMO SBCSU verwendet, ist der Parameter **AUTHERF** auf **JA** zu setzen und die Sicherheitsdaten müssen auch im SIP-Endgerät eingestellt werden!

Wichtig: Der Parameter **MBCHL** in AMO SDAT sollte für alle SIP-Teilnehmer gesetzt werden. Ist dieser Parameter nicht gesetzt, sind Leistungsmerkmale, die einen zweiten B-Kanal benötigen, nicht möglich (z. B Konferenz, Zweitanruf).

Wichtig: Bei allen Arten von SIP-Telefonen werden Einstellungen wie Lautstärke oder Rufton nicht durch das System gesteuert. Daher werden die für solche Geräte über AMO ACTDA/AMO KCSU eingestellten Werte nicht verwendet.

Konfiguration der UFIP-Schnittstelle

UFIP-Teilnehmer können auf IP-Gateways (STMI oder vHG) mit SIP-Funktionalität (BFDAT) konfiguriert werden. Die Circuit-Funktionalität wird nur über vHG (SoftGate) bereitgestellt.

Im Allgemeinen können „normale“ SIP-Endpunkte und Circuit-Clients parallel auf demselben Gateway konfiguriert werden.

AMO:
`ADD-SBCSU:STNO=<UFIP_STN>,OPT=OPTI,CONN=IP2,PEN=<X-Y-Z-T>,DVCFIG=UFIP;`

Für die Digest-Authentifizierung müssen die Parameter IPPASW, USER ID und SECZONE konfiguriert werden.

Der Kunde unterstützt die Registrierung nur mit der E.164-Nummer (mit und ohne führendes +) und der Nebenstellennummer.

Die Registrierung kann über das vHG WBM geprüft werden: Configuration > Sprachgateway > Clients > UFIP SIP.

Tatsächliche SIP-Geräte erfordern weder eine spezielle Loadware noch besondere Konfigurationsänderungen.

14.2.5.3 Entfernen eines SIP-Teilnehmers

	**Configuration Management > Anschluss > Anschluss** Klicken Sie auf **Suchen**. Wählen Sie den zu löschenden Teilnehmer aus. Klicken Sie auf **Löschen**.
	`DELETE-SBCSU:STNO=4420,SVC=ALL;`

14.2.5.4 Ändern eines SIP-Teilnehmers

Die Daten des SIP-Endpunkts werden unter dem Zweig „OPT=FPP“ geändert.

	**Configuration Management > Anschluss > Anschluss** Klicken Sie auf **Suchen**. Wählen Sie den zu ändernden Teilnehmer aus. Ändern Sie die Daten. Klicken Sie auf **Speichern**.
	`CHA-SBCSU:STNO=4220,OPT=OPTI,SUBIPADD=1.40.41.15;`

14.2.5.5 DMC aktivieren/deaktivieren

DMC wird für Teilnehmer 4420 und aktiviert, für Teilnehmer 4422 und 4423 deaktiviert.

	**Configuration Management > Anschluss > Teilnehmeranschluss** Klicken Sie auf **Suchen**. Wählen Sie den Teilnehmer aus, dessen DMC-Einstellungen Sie ändern möchten. Aktivieren/Deaktivieren Sie das Kontrollkästchen **DMC erlaubt** auf der Registerkarte **Basic 3** .
	`CHANGE-SDAT:STNO=4420, TYPE=ATTRIBUT, AATTR=DMCALLWD;`

NOTICE: Eine Änderung dieses Attributs wird erst nach Deaktivierung und erneuter Aktivierung des entsprechenden Kreises über RES-DSSU wirksam.

14.2.5.6 SIP Session Timer

Der „SIP Session Timer“ bietet einen „keepalive“ Mechanismus für SIP Sessions. Ist dieses Leistungsmerkmal aktiviert, werden über eine bestehenden SIP-Verbindung periodisch reINVITE oder UPDATE Meldungen geschickt. Antwortet der Partner verlängert sich die Session um einen zuvor zwischen den Partnern ausgehandelten Zeitraum. Antwortet er nicht, wird ausgelöst. So wird verifiziert, ob die Verbindung noch besteht.

Die Randwerte für die Dauer einer Verlängerung können im WBM des Gateways festgelegt werden:

1) **WBM -> Configuration -> Sprachgateway -> SIP Parameters**

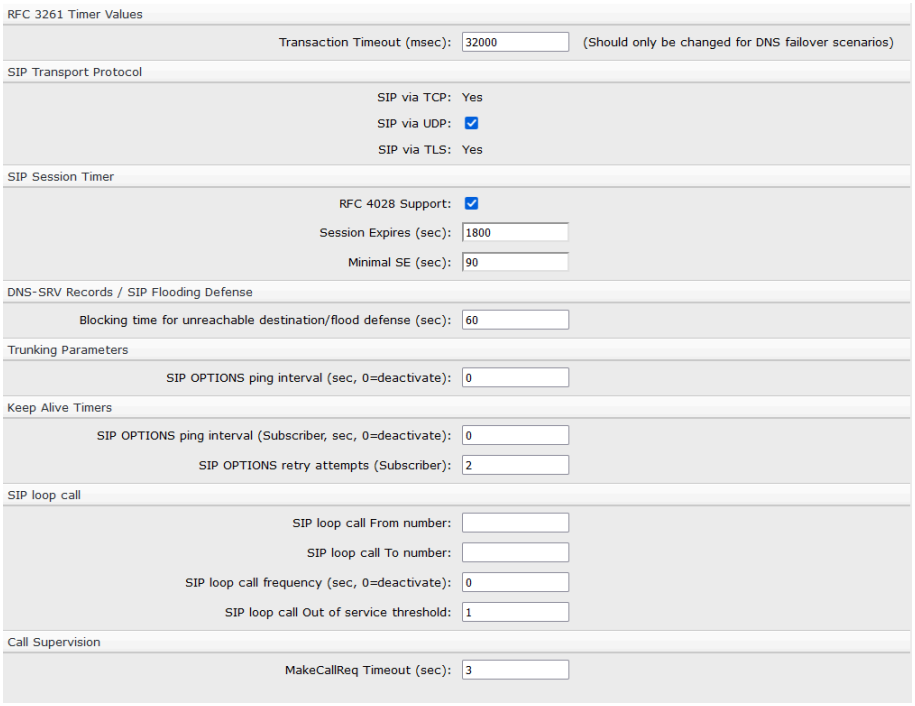


Abbildung 199: SIP Session Timer

- Mit der Checkbox **RFC4028 verwenden** wird der SIP Session Timer aktiviert.
- **Session-Expires**: Legt die maximale Zeitdauer fest um die eine Session verlängert wird.
- **Minimal-SE**: Legt die minimale Zeitdauer fest um die eine Session verlängert wird.

Die tatsächliche Zeitdauer der Verlängerung hängt auch von den Einstellungen des Partners ab, liegt aber innerhalb des konfigurierten Intervals. Eine Session wird erneuert, sobald sie zur Hälfte abgelaufen ist.

Wichtig: Bitte beachten Sie, dass sehr kleine Abstände zu einem erhöhten Meldungsverkehr führen!

14.2.5.7 Teilnehmer Parameter

Ab V10R1 unterstützt die OpenScape 4000 Teilnehmerparameter für UFIP-Clients basierend auf Nachrichten mit SIP OPTIONS

Falls eine Station nicht innerhalb einer bestimmten Zeit auf die Nachrichten antwortet, wir die Station abgemeldet

WBM Implementierung

Teilnehmerparameter werden im WBM des HG-Boards unter Konfiguration – Voice Gateway – SIP Options, angezeigt

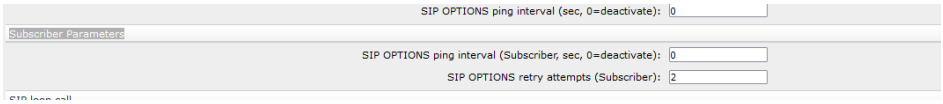


Abbildung 200: Teilnehmer Parameter

SIP OPTIONS ping interval:

- Der Timer wird gestartet, indem ein Wert ungleich 0, sondern im Bereich von 30 – 3600 Sekunden eingestellt wird.
- Der Wert stellt das Zeitintervall dar, nach dem eine OPTIONS-Nachricht an eine Station gesendet wird.

SIP OPTIONS Wiederholungsversuch:

- Sie stellt die Anzahl der gesendeten Nachrichten dar, auf die keine Antwort (200 OK) eingeht, bevor die Station abgemeldet wird.
- Die Werte sollten im Bereich von 1 – 5 liegen.

14.2.5.8 Briefkastensignalisierung (MWI)

Das Leistungsmerkmal Briefkastensignalisierung (Message Waiting Indication MWI) wird aktiviert/deaktiviert indem man bei jedem SIP-Teilnehmer im AMO SBCSU den Parameter **PMIDX** und in der COS des Teilnehmers die Autorisierung **BRK** setzt.

Das Leistungsmerkmal ist sowohl für OpenScape 4000 SoftGate als auch für das Common Gateway HG 3500 realisiert.

MWI Aktivierung:

- Erzeugen Sie mit AMO RICHT für **ART=PM** einen neue IDX für den Phone Mail Zugang:
- `EINR-RICHT:ART=PM,IDX=1,SAN=0894711,NAME=XPRESSION;`

ART=PM	Art der Adressierung der Richtung ist Phone Mail (PM)
IDX	Index für die Service-Access-Nummer
SAN	Service Access Nummer
NAME	Name der Richtung

- Im AMO SBCSU muss **PMIDX=1** für SIP-Teilnehmer gesetzt werden.
- In der COS des Teilnehmer mit Hilfe des AMO COSSU **ESBER=BRK** (Briefkasten (Ausleseberechtigung)) setzen.

MWI Deaktivierung:

- Im AMO SBCSU muss **PMIDX=0** für die entsprechenden SIP-Teilnehmer gesetzt werden.
- In der COS des Teilnehmer mit Hilfe des AMO COSSU **ASBER=BRK** (Ausleseberechtigung für Briefkasten wird zurückgenommen) setzen.

14.2.5.9 SIP-Teilnehmer als DR-Taste eines Tischtelefons

Leistungsmerkmalbeschreibung

Es ist möglich, mit Hilfe des AMO ZIEL einen SIP-Teilnehmer als DR-Taste (DR-Ziel) auf einem Tischtelefon zu konfigurieren.

Szenarien

Der Besetztzustand des SIP-Teilnehmers wird durch eine LED an der DR-Taste der überwachenden Nebenstellen angezeigt.

- LED aus: Der SIP-Teilnehmer ist frei und kann Anrufe erhalten.
- LED an: Der SIP-Teilnehmer ist besetzt.

Wenn SIP-Teilnehmer Mitglied einer ONS-Gruppe ist:

- Wenn der SIP-Teilnehmer als Master der ONS-Gruppe fungiert, zeigt die DR-LED den Status der ONS-Gruppe an.
- Wenn der SIP-Teilnehmer als Slave fungiert und die Slave-Rufnummer überwacht wird, zeigt die DR-LED den Status des Slave an.

Der SIP-Teilnehmer wird angerufen, wenn er frei ist (LED aus) und die DR-Taste an einer überwachenden Nebenstelle gedrückt wird.

Anmerkungen

- Da der Rufzustand des SIP-Teilnehmers als Besetztzustand behandelt wird, blinkt die DR-LED nicht, und eine Anrufübernahme ist nicht möglich.
- Aufseiten des SIP-Teilnehmers aktivierte lokale Leistungsmerkmale können nicht durch das System überwacht werden. Eine aufseiten des SIP-Teilnehmers lokal aktivierte Anrufumleitung wird ausgeführt, wenn die mit dem SIP-Teilnehmer als Ziel konfigurierte DR-Taste gedrückt wird.

Generierung (Beispiel)

Digit: 3412, SIP: 3434

```
ADD-ZIEL:TYPE=DSS,SRCNO=3412,KYNO=12,DESTNOD=3434;
DIS-ZIEL:DSS,3412;
H500:  AMO ZIEL STARTED
DSS

 SOURCE      | DEVICE |  KEY   | DEST.        | SLKTYPE  |
 SLKTEXT

-------------+--------+--------+--------------+----------
+-------------

3412         |   BD   | 12     | 3434         | SLKSTNO  |

AMO-ZIEL -111       DESTINATIONS FOR VARIOUS STATION
 FEATURES
DISPLAY COMPLETED;
```

14.2.5.10 SIP-Peer-Filtering

Das Leistungsmerkmal **SIP-Peer-Filtering** ist für HG 3500 und vHG 3500 SIP freigegeben.

Um SIP-Leitungen gegen Hackerangriffe (Scanning) zu schützen, werden nur SIP Requests von „bekannten“ Gegenstellen (Partner) beantwortet, alle anderen Requests werden abgewiesen. „Bekannte“ Peers sind IP-Adressen oder FQDNs von einem aktivierten SIP Trunk Profil und/oder registrierten SIP Clients.

Die Funktion kann eingestellt werden für

- in Gateways / HGs konfigurierte B- Kanäle für SIP-Clients **und** SIP-Trunks
- Es werden dann nur eingehende REGISTER Meldungen von „bekannten“ Gegenstellen beantwortet. Alle anderen Requests „unbekannter“ Gegenstellen werden ignoriert.
- Gateways / HGs, die nur als trunking Gateway konfiguriert sind.
- Es werden dann nur „bekannte“ Requests beantwortet. Alle Requests von „unbekannten“ Gegenstellen werden ignoriert.

  Ein typischer Anwendungsfall für dieses Leistungsmerkmal ist wenn ein SIP-Trunk-Gateway mit einem SIP Provider über WAN/Internet ohne zusätzliche Security Tools, wie eine Firewall verbunden ist.

  Das Leistungsmerkmal kann über die Chechkbox **SIP-Peer-Filtering aktivieren** im **SIP-Trunk-Profilparameter** Menu aktiviert werden. Nach der Aktivierung/Deaktivierung des Leistungsmerkmales muss das Gateway neu gestartet werden.

  WBM > Sprachgateway > SIP-Trunk-Profilparameter

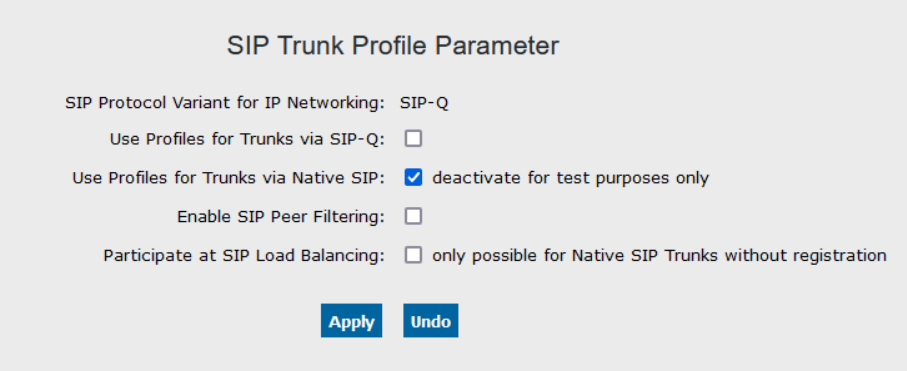


Abbildung 201: SIP-Peer-Filtering

14.2.5.11 Anrufweiterleitung

3 Arten der Anrufumleitung sind möglich:

- CFU - ständige Anrufumleitung (Call Forwarding Unconditional)
- `EINRICHTEN-ACTDA:TYP=TLN,RNR=<rufnummer>,LMACT=AUL,AULVAR=<AUL variante>,UART=CFU,SI=VCE;`
- CFNR - Anrufumleitung bei nicht melden (Call Forwarding No Reply)
- `EINRICHTEN-ACTDA:TYP=TLN,RNR=<rufnummer>,LMACT=AUL,AULVAR=<AUL variante>,UART=CFNR,SI=VOICE;`
- CFB - Anrufumleitung bei besetzt (Call Forwarding Busy)
- `EINRICHTEN-ACTDA:TYP=TLN,RNR=<rufnummer>,LMACT=AUL,AULVAR=<AUL`

```
variante>,UART=CFB,SI=VOICE;
```

Anmerkung: Für ältere SIP-Geräte mit S0PP muss SI=SPCH verwendet werden.

14.2.5.12 Anzeige der SIP-Teilnehmer

Registrierte und nicht registrierte SIP-Teilnehmer können mit dem **HG35xx Web Based Management** im OpenScape 4000 Assistant abgefragt werden.

Im OpenScape 4000 Assistant:

1) Expertenmodus -> Gateway Dashboard ->HG35xx Web Based Management

Im HG35xx Web Based Management:

Configuration-> Sprachgateway

Configuration -> Sprachgateway - Clients - UFIP SIP

Registrierte Clients sind fett dargestellt.

14.2.5.13 Besetzter Override, Notfall-Einbruch und Notabschaltung für SIP (UFIP)-Abonnenten

Busy Override, Emergency Intrusion und Emergency Disconnect sind für SIP (UFIP) Teilnehmer in der Version V8R1 mit spezifischen Einschränkungen der SIP-Schnittstelle implementiert:

Busy Override, Emergency Intrusion und Emergency Disconnect gegen SIP-Teilnehmer:

1) Die Anzeige auf SIP-Ebene wird nicht aktualisiert

2)
- Auf CP-Ebene gilt der SIP-Teilnehmer als besetzt, wenn mindestens eine Transaktion besetzt ist, wenn Übersteuerung, Noteinbruch oder Notabschaltung aufgerufen werden (Aktivierung der Funktion „Zweitanruf“ auf Geräteebene muss berücksichtigt werden).

Busy Override, Emergency Intrusion und Emergency Disconnect aufgerufen von einem SIP-Teilnehmer:

- Nur WL3/WL4 (UFIP)-Geräte unterstützen derzeit die Funktion
- Das System unterstützt die Funktion für jede Art von SIP (UFIP)-Gerät, aber auf Geräteebene muss die Schnittstelle implementiert werden, um bestimmte Menüoptionen für Busy Override, Emergency Intrusion und Emergency Disconnect zu unterstützen.
- Die Funktionen können über jede SIP (UFIP) aufgerufen werden, indem bestimmte WABE-Codes (KNOVR, EOVR, RELEASE), gefolgt von der Teilnehmernummer gewählt werden.

Aktivierung der Funktion über AMO-Befehle:

```
CHANGE-FEASU:TYPE=A,CM=OVR&EMOVR&EMRLS;
CHANGE-ZAND:TYPE=ALLDATA,OVRMST=YES;
```

SDAT-Attribute für eindringend Station:

```
CHANGE-SDAT:STNO=13203,TYPE=ATTRIBUT,AATTR=EOVR&KNOVR;
ADD-WABE:*56,,,KNOVR,N,,,,,,,;
```

```
ADD-WABE:*57,,,EOVR,N,,,,,,,;
ADD-WABE:*58,,,RELEASE,N,,,,,,,;
```

Weitere Informationen finden Sie in der Dokumentation zur Featurebeschreibung.

Bei einem WL3/WL4 (UFIP)-Gerät müssen die Feature-Aktivierung und die Aktivierungscodes auch im Telefon-WBM konfiguriert werden.

14.2.5.14 UFIP in Pickup Group

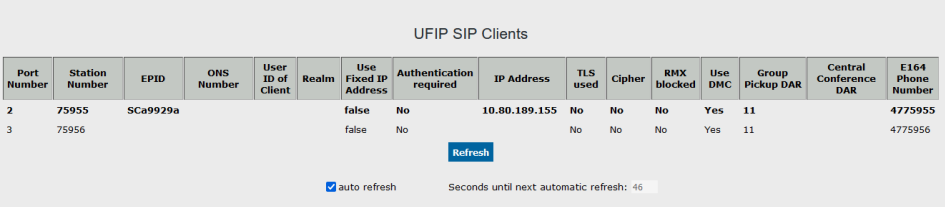
Starting with V8, the chronologically first and only the first WABE PU code configured in the system will be marked and used also for UFIP devices.

```
DISPLAY-WABE:TYPE=GEN,DAR=PU;
H500:  AMO WABE  STARTED
  ---------------------------------------------------------------------------
  | DIGIT INTERPRETATION                  VALID FOR ALL DIAL PLANS           |
  ---------------------------------------------------------------------------
  |                  |    CALL PROGRESS STATE     |NODE/DIGIT| RESERVED/CONVERT |
  |       CODE       |          1 11111 11112 22| ANALYSIS | DNI/ADD-INFO/UFIP|
  |                  |0 12345 67890 12345 67890 12|  RESULT  | *=OWN NODE       |
  ---------------------------------------------------------------------------
  | *19              |. ....* ..... ..... ..... ..| PU       |                  |
  | *70              |. ....* ..... ..... ..... ..| PU       |    UFIP          |
  | *90              |. ....* ..... ..... ..... ..| PU       |                  |
  ---------------------------------------------------------------------------

AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES
DISPLAY COMPLETED;
  <
```

Once the UFIP PU code is configured, it can be changed only via CHANGE-WABE command. Deleting it is not allowed.

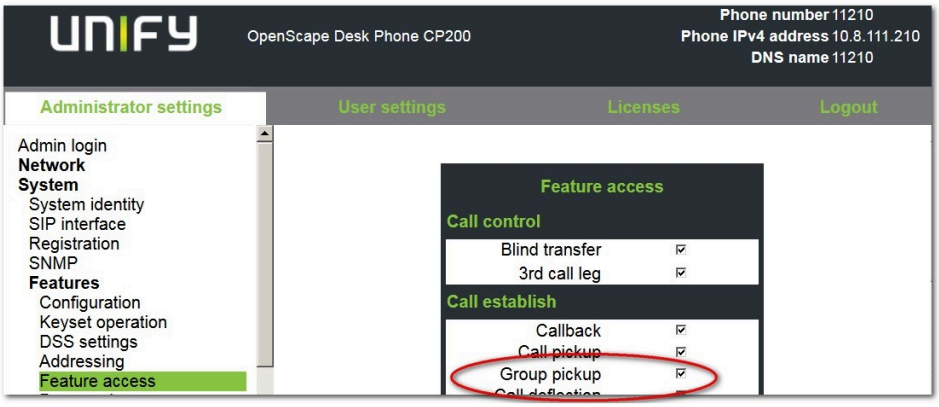
UFIP gateways must be restarted to load the new UFIP PU code, which can be checked in WBM: Configuration -> Voice Gateway -> Clients -> UFIP SIP: “Group Pickup DAR” column



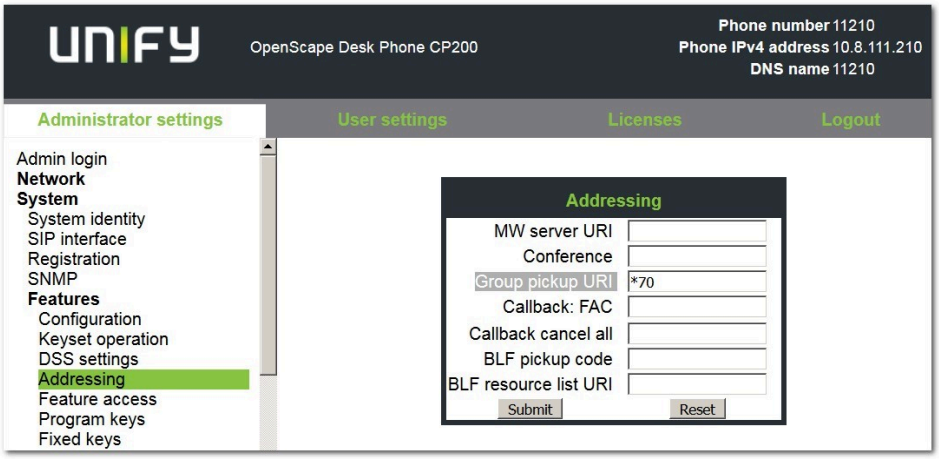
Restrictions: only one PU code at a time can be used for UFIP clients. Since REGENERATE-WABE will return the codes in numerical order, after new generation of the system (including upgrades via Auto-GENDB) manual adaption maybe needed to change the order of configured codes.

Following the system AUN configuration, for each UFIP device:

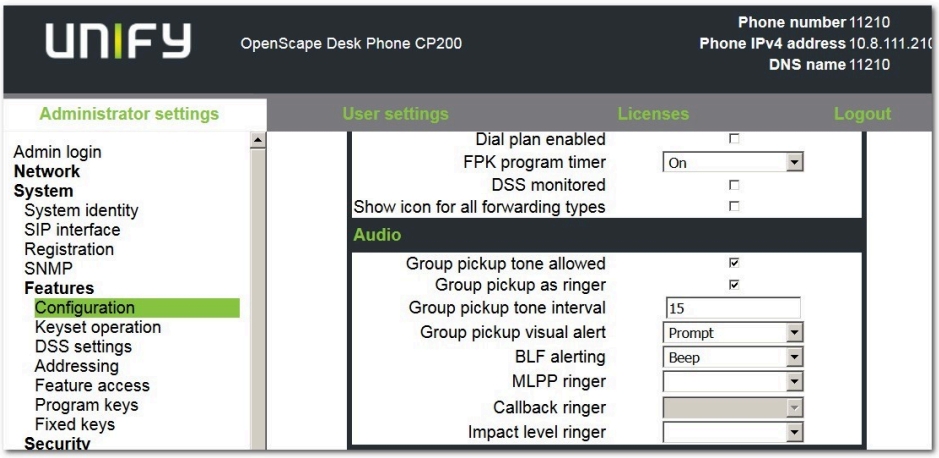
- “Group pickup” feature must be enabled:

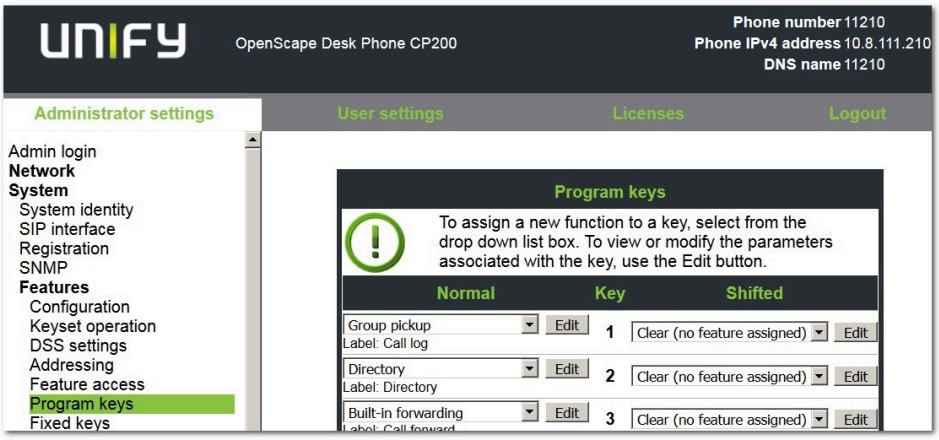


- WABE UFIP PU code must be configured:



- Optional device pickup call behavior customization and key configuration:





For details, please check phone documentation.

14.2.5.15 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
ACTDA	UART	d	CFB: Anrufumleitung bei besetzt CFNR: Anrufumleitung bei nicht melden CFU: ständige Anrufumleitung
	DTYPE	e	CFB: call forwarding busy CFNR: call forwarding no reply CFU: Call forwarding unconditional
BCSU	ALARMNR	d	Alarm Nummer
	ALARMNO	e	Alarm number
	ART=HWYBDL	d	Highway-Bündel
	TYPE=HWYBDL	e	Highway bundle
	BKANSIP	d	Anzahl der B-Kanaele fuer die SIP-Subscriber Funktion
	BCHLSIP	e	Number of b channels for sip subscriber function
	FCTID	d	Function Id (wird immer auf 1 gesetzt)
	FCTID	e	Function id (is always set to 1)
	FCTBLK	d	Funktionsblock-Index (einen beliebigen freien Funktionsblock zwischen 1-20 wählen)
	FCTBLK	e	Function block index

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LWVAR	d	Index auf Loadware Block der T1 Baugruppe
		e	Loadware variant
	SACHNR	d	Baugruppensachnummer (2. und 3. Block) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	PARTNO	e	Part numver (2nd and 3rd bloc) Q2316-X, Q2316-X10, Q2324-X500, Q2324-X510
	TYP=IPGW	d	IP Gateway (Common Gateway Baugruppe)
	MTYPE=IPGW	e	IP Gateway (Common gateway board)
BFDAT	ANZSATZ	d	Anzahl der funktionsbezogenen Saetze. Mögliche Werte: 1-240
	LINECNT	e	Defines the number of lines related to the selected function.
	BGBKAN	d	Block fuer Baugruppe mit 60 und/oder 120 B-Kanaelen
	BRDBCHL	e	dedicates the block for boards with 60 and/or 120 b-channels
	CONFIG=WEITER	d	Weitere Block-Konfiguration ermöglichen
	CONFIG=CONT	e	Continue block configuration
	CONFIG=OK	d	Block-Konfiguration abschließen
	CONFIG=OK	e	Finish block configuration
	FCTBLK	d	Dieser Index beschreibt den Funktionsblock welcher auf dem Common Gateway konfiguriert werden soll. Anhand des Funktionsblocks wird die Konfiguration der benötigten pyhsikalischen Lines (Sätze der Baugruppe) festgelegt.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	FCTBLK	e	This index describes the function block which should be configured on the common gateway board. With that index the amount of needed physical lines (board circuits) is calculated.
	FUNCTION	d	Dieser Parameter legt das Konfigurationsprofile des Common Gateways fest. Dabei muss die eventuell benötigte HG 3570 Funktion als erste angeführt werden. Falls ein bestimmter Line-Bereich für die Funktionen HG 3530 oder HG 3550 vorreserviert werden soll, muss die entsprechende Funktion am Ende stehen und mit dem Wert HG35xxR abgeschlossen sein. Die Funktion kann nur als Einzel-Funktion konfiguriert werden. FUNCTION=SIP: SIP Subscriber Funktion
	FUNCTION	e	This parameter defines the configuration profile of the common gateway board. If HG3570 functionality is used, it must be configured at first position. If a prereservation of a certain line range of functions HG3530 or HG3550 is desired, this function must be at the end of the profile just suffixed by the according HG35xxR value. The function can only be configured as single function. FUNCTION=SIP:SIP subscriber function
CGWB	DEFRT		IP-Adresse des Default Routers innerhalb des LAN-Segmentes. Der Default Router übernimmt die Weiterleitung der Pakete, die eine Zieladresse außerhalb des eigenen LAN-Segmentes haben. 0.0.0.0 bedeutet, daß kein Default Router konfiguriert ist.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	DEFRT	e	IP address of the default router within the LAN segment. The default router takes care of routing forward all packets with a destination address with a network part different from the own LAN segment. 0.0.0.0 means that no default router is configured.
	IPADR	d	IP Adresse der Common Gateway Baugruppe (Source Adresse)
	IPADR	e	IP address of common gateway board (source address)
	MTYP=INITCGWB	d	Zurücksetzen der Konfigurationsdaten der Common Gateway Baugruppe auf die Standardwerte
	MTYPE=INITCGWB	e	Reset configuration data of common gateway board to default values
	NETMASK	d	IP-Netzmaske des LAN-Segmentes. Die IP-Netzmaske bestimmt die Grenze zwischen Netz- und Host-Teil in der IP-Adresse. Alle IP-Adressen am LAN-Segment müssen bezüglich des Netzanteils der IP-Adresse gleich und bezüglich des Host-Teils unterschiedlich sein (auch der Default Router muss dieser Bedingung entsprechen).
	NETMASK	e	IP net mask of LAN segment The IP net mask determines the network and the host partition of an IP address. All IP addresses of a LAN segment must contain the identical network address part but different host address parts (also the Default Router must fulfill this requirement).

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	SMODE=NORMAL	d	Mode oder Normal Mode Eine Baugruppe im Normal Mode hat gültige Baugruppendaten und normalerweise auch OPTIIPs konfiguriert. Eine Baugruppe im Ready Mode hat keine gültigen Baugruppendaten, auf diese Baugruppe können OPTIIPs umgeschaltet werden, falls eine andere Baugruppe aus demselben Baugruppen-Pool (AMO BPOOL) defekt wurde. Eine Baugruppe im Defekt Mode hat ebenfalls keine gültigen Baugruppendaten, diese Baugruppe hat aufgrund eines Defekts seine OPTIIPs und seine Baugruppendaten abgegeben.
	SMODE=NORMAL	e	Mode or Normal Mode A board in Normal Mode has valid board data and normally also OPTIIPs assigned to it. A board in Ready Mode has no valid board data, to this board OPTIIPs can be switched over if another board of the same board reconfiguration pool (AMO BPOOL) becomes defective. A board in Defect Mode has also no valid board data, this board has lost its OPTIIPs and its board data to another board because it's gone defective.
SBCSU	ART=FPP	d	Hauptrufnummer des S0-/S2-Punkt zu Punkt Anschlusses
	OPT=FPP	e	Functional point-to-point connection
	ANSCHL=SIP	d	Anschlussart=SIP
	CONN=SIP	e	Kind of connection=SIP
	GERKON=S0PP	d	S0-Punkt zu Punkt Anschluss
	DVCFIG=S0PP	e	S0-point-to-point
	PROT=SBDSS1	d	Protokollvariante DSS1
	PROT=SBDSS1	e	Protocol variant DSS1
	OPT=10	d	Optiontabellenindex 10
	OPTIDX=10	e	Option table index 10

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	IPADR	d	IP-Adresse
	IPADDR	e	IP address
	PASSWD	d	Passwort
	PASSWD	e	Password
	KENNUNG	d	Benutzerkennung
	USERID	e	User ID
	SECBER	d	Security-Bereich (Art Domäne)
	SECZONE	e	Security zone (kind of a Domain)
	FESTEIP	d	Feste IP-Adresse
	FIXEDIP	e	Fixed IP address
	AUTHERF	d	Authentifizierung erforderlich
	AUTHREQ	e	Authentification required
	SMGTLN	d	SMG Teilnehmer; Für Survivability-Lösung mit der H8k;
	SMGSUB	e	SMG subscriber For survivability solution with H8k;
SDAT	EMERK	d	Teinehmermerkmal einfügen
	AATTR	e	Add attribute
	AMERK	d	Teinehmermerkmal ausfügen
	DATTR	e	Delete attribute

14.3 SIP-Trunking

14.3.1 SIP-Q-Trunking

SIP-Q: CorNet-NQ-Tunneling über SIP. SIP-Q ist das bevorzugte Protokoll für die Zusammenarbeit mit anderen Unify-Systemen.

14.3.1.1 Leistungsmerkmale

Wichtig: Nur mit SIP-Q können alle CorNet-NQ-Leistungsmerkmale bei einer Vernetzung unterstützt werden.

Seit HiPath 4000 V4 ist SIPQ die bevorzugte Methode für die Vernetzung von HiPath 4000- und OpenScape 4000-Systemen. SIPQ v2 wird ab HiPath 4000 V4 unterstützt.

14.3.1.1.1 Konnektivität mit OpenScape Voice

Für die Konnektivität mit OpenScape Voice wird nur das Protokoll SIP-Q V2 freigegeben, SIP-Q V2 unterstützt TLS und SRTP.

Außerdem wird SIP-Q für die Konnektivität mit OpenExchange verwendet, um einen sehr leistungsfähigen und skalierbaren IP LCR bereitzustellen.

Für SIP-Q Anbindung mit OpenScape Voice muss Blockwahl für die Teilnehmer und OpenScape 4000 LCR konfiguriert werden. Es werden zwei Blockwahl-Verfahren unterstützt:

- wie bei SIP-Teilnehmern in einer OpenScape Voice Lösung.
- wie der vorhandene OpenScape 4000-Blockwahlmodus (bekannt von Systemen bis OpenScape 4000 V4).

Wichtig: Blockwahl für OpenStage 60 und 80 HFA wird mit OpenStage HFA **V2** unterstützt.

Leistungsmerkmale bei SIP-Q V2 zwischen HiPath 4000/OpenScape 4000 und OpenScape Voice

- Anrufidentifizierung
  - CLIP/CLIR
  - COLP/COLR
  - CNIP/CNIR
  - CNOP/CNOR
- Anrufübergabe
- Halten / Wiederaufnehmen / Makeln
- Anrufumleitung
  - CFU (Anrufumleitung unbedingt)
  - CFB (Anrufumleitung bei besetzt)
  - CFNR (Anrufumleitung bei nicht melden)
- Rückruf bei besetzt / nicht melden
- Briefkastensignalisierung (MWI)
- Wegeoptimierung
- Übertragung von „CorNet-NQ“-Meldungen
- IPv6 (siehe „OpenScape 4000 SoftGate“ > IPv6 auf Seite 380)
- Signalisierungs (TLS)- und Sprachverschlüsselung (SRTP) (siehe „Signalisierungs- und Sprachverschlüsselung (SPE)“)
- Gebührenerfassung
- T.38 Fax Verbindungen (z.B. für SIP-Q-Trunking im Common Gateway HG 3500 in Richtung OpenScape Voice V4/V5)

14.3.1.1.2 Codecs nach Zielgateway für SIP-Q Trunking

Leistungsmerkmalbeschreibung

OpenScape 4000 kann so konfiguriert werden, dass der Codec in Abhängigkeit vom Zielgateway ausgewählt wird. Dies bedeutet, dass die Sprach-Codec-Einstellungen von der IP-Adresse des Zielgateways abhängen. Alle

anderen Konfigurationsoptionen (z.B. Faxeinstellungen) spielen für dieses Leistungsmerkmal keine Rolle.

Für das Festlegen der Anrufrichtung stehen die folgenden Optionen zur Verfügung:

- Konfigurieren einzelner IP-Adressen
- Konfigurieren eines IP-Adressbereichs
- Konfigurieren einer Subnetzmaske

Serviceinformationen

- Dieses Leistungsmerkmal wird für Common Gateway HG 3500 und vHG 35000 OpenScape 4000 SoftGate unterstützt.
- Dieses Leistungsmerkmal wird nur für OpenScape 4000-interne SIP-Q-Vernetzung mit festen IP-Adressen unterstützt.
- Wenn FQDNs (voll qualifizierten Domain-Namen) verwendet werden (z.B. zu OpenScape Voice), kann dieses Leistungsmerkmal nicht verwendet werden.
- Die spezifischen Spach-Codec-Einstellungen sollten für ankommende und abgehende Anrufe (aus Sicht des Gateways) bestimmt werden. Die zielspezifischen Codecs können dynamisch ohne Neustart geändert werden (sowohl für SIP-Q in Common Gateway als auch für OpenScape 4000 SoftGate).

14.3.1.1.3 SIP-Peer-Filtering

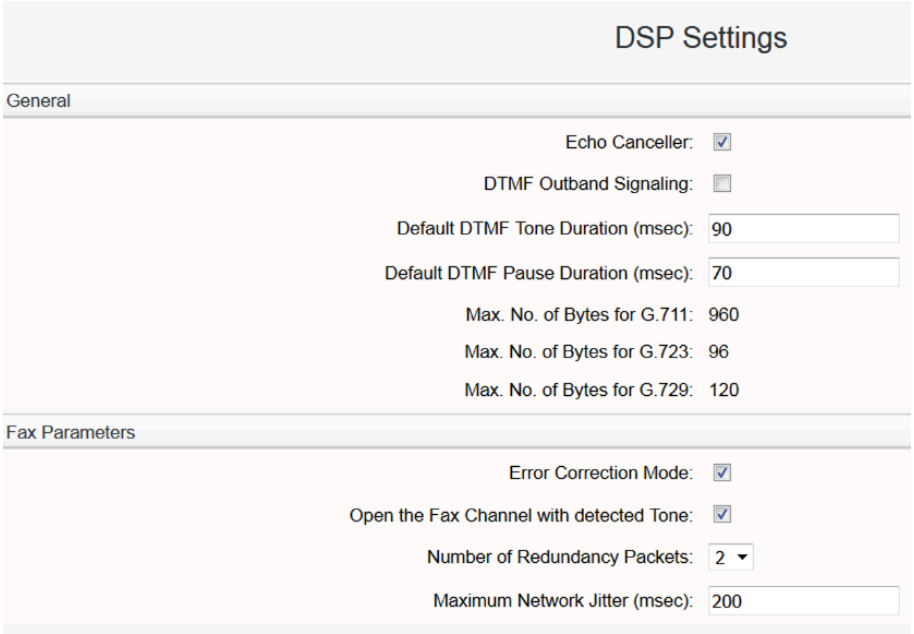
SIP Peer Filtering ist für HG 3500 und vHG 3500 SIP freigegeben.

Für mehr Informationen siehe Abschnitt 2.5.9, „SIP-Peer-Filtering“.

14.3.1.2 Einschränkungen

- Outband Signalisierung wird nicht unterstützt.
- Funktion muss über das WBM ausgeschaltet werden:

  WBM > Configuration > Voice Gateway > Payload > HW Modules > DSP-Einstellungen



- Trunking zwischen HiPath 3000 und OpenScape 4000
- SIP-Registrierung der HG 1500-Baugruppe am Large Enterprise Gatekeeper (LEGK) wird nicht unterstützt.
- SIP-Q V2 zwischen HiPath 4000/OpenScape 4000 und OpenScape Voice
- Gebührenerfassung wird nicht unterstützt.

14.3.1.3 Konfiguration

siehe Kapitel 6, „Konfiguration SIP-Q-Trunking / Native SIP Trunking“.

14.3.2 Native SIP Trunking

Native SIP-Trunks können für die Anbindung von SIP-Service-Providern (siehe Abschnitt 3.2.3.1, „SIP-Service-Provider“) oder externen SIP-Produkten (z. B. OpenScape Xpressions, Abschnitt 3.2.3.3, „Anwendungen“) verwendet werden.

Native SIP-Verbindungen von Drittanbietern können unter Verwendung der standardmäßig gelieferten Profile des Gateways ohne projektspezifische Freigabe (Project Specific Release, PSR) mit OpenScape 4000 Gateway verbunden werden.

Die Liste der unterstützten RFCs finden Sie im Kapitel SIP-Konnektivität in diesem Dokument. Sollte das OpenScape 4000 Gateway mit keinem der veröffentlichten RFCs konform sein, kann jedes gefundene Problem über ein Service-Ticket gelöst werden.

Das Erstellen oder Ändern der festen Parameter vorhandener Profile wird nicht unterstützt. Das empfohlene Profil für SIP-Anwendungen von Drittanbietern ist „NatTrkEnterprise“, das die Unterstützung von SIP Refer beinhaltet. Es gibt spezielle Profile für die externen Produkte MS Teams und Cisco UCM.

Das Verfahren zur Beantragung neuer Baugruppenprofile, das für SIP Service Provider (SSP) obligatorisch ist, finden Sie hier: https://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers_on_Enterprise_Platforms#OpenScape_4000

14.3.2.1 Leistungsmerkmale

Wichtig: Die Verfügbarkeit der folgenden Funktionalitäten hängt vom SIP-Partner ab und ist im Einzelfall zu testen!

- Basic Call entsprechend RFC3261 SIP (unterstützte RFCs siehe Abschnitt 1.2, „Unterstützte RFCs (Request For Comments) für SIP-Schnittstellen“)
- CLIP/CLIR
- COLP/COLR
- Senden und Empfangen expliziter internationaler E.164-Rufnummern mit vorangestelltem „+“ (z. B. +498972237729) oder impliziter Telefonnummern mit Präfix (z. B. 00498972237729)
- Namensanzeige (z. B. für OpenScape Xpressions V6-Verbindung)
- Halten / Wiederaufnehmen / Makeln

- Anrufübergabe (Anrufübergabe nach Melden / Übergabe vor Melden / Anrufübergabe ohne Melden)
- Anrufweiterleitung („Forward-Switching“-Methode)
- Diversion header
- Early media (183 Call Progress with SDP)

Wichtig: Anrufumleitung nach der „Call-Reroutring“-Methode wird nicht unterstützt. Stattdessen wird Diversion Header unterstützt (Senden von Anrufumleitungsinformationen; erforderlich für Anrufumleitung-Szenarien zum SIP-Service-Provider).

- Konferenz (3er-Konferenz)
- Briefkasten Signalisierung MWI
- Dieses Leistungsmerkmal kann für SIP-Verbindungen zu Service-Providern verwendet werden, die gehostete Unified Messaging-Dienste anbieten.
- DNS SRV - Lokalisierung und Adressierung von SIP-Servern/Proxies mittels vollqualifizierter Domänennamen
- SIP Proxy-Failover und -Recovery
- Registrierung bei SIP Service Provider (Registrierung **bei** OpenScape 4000 **durch** andere Anbieter wird nicht unterstützt).
- Session Border Controller-Konnektivität
- SIP Session Timer RFC4028 (mehr Informationen finden Sie im Abschnitt 2.4, „Einschränkungen“)
- Digest Authentication
- L2- und L3-QoS für Signalisierung und Payload
- T.38-Fax-Verbindungen (in Richtung SIP-Service-Provider, z.B. T-Systems)
- DTMF-Signalisierung (Inband und RFC2833 konform)
- Sprach-Codecs G.729 und G.711
- Sprechpausenunterdrückung (Silence Suppression)
- Inband / Outband Proxy-Konfiguration
- SIP-Trunking-Profile (ermöglichen einfache Integration und Administration von SIP-Service-Providern)
- UDP/TCP-Transport
- IPv6 (siehe „OpenScape 4000 SoftGate“ > IPv6 auf Seite 380)
- Signalisierungs (TLS)- und Sprachverschlüsselung (SRTP) (siehe „Signalisierungs- und Sprachverschlüsselung (SPE)“)

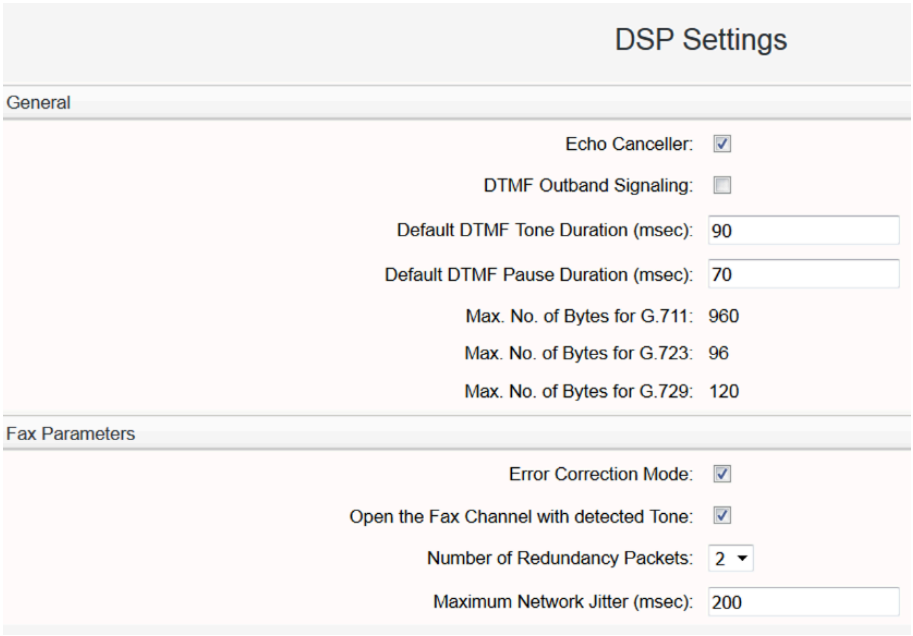
OpenScape 4000- und OpenScape Voice-Systeme werden normal per SIP-Q vernetzt (siehe Abschnitt 3.1, „SIP-Q-Trunking“).

14.3.2.2 Einschränkungen

- Common Gateway HG 3500: SRTP wird nicht für native SIP-Trunking unterstützt.
- Outband Signalisierung wird nicht unterstützt.

- Funktion muss über das WBM ausgeschaltet werden:

  WBM > Configuration > Voice Gateway > Payload > HW Modules



- Trunking zwischen HiPath 3000 und OpenScape 4000
- SIP-Registrierung der HG 3500-Baugruppe am Large Enterprise Gatekeeper (LEGK) wird nicht unterstützt.

14.3.2.3 Anwendungsfälle

14.3.2.3.1 SIP Service Provider

Native SIP-Trunking wird hauptsächlich für Verbindungen zu SIP-Service-Providern verwendet.

Wichtig: Für ein Anschaltung an einen noch nicht freigegebenen SIP-Service-Provider muss ein Change Request erstellt werden!

Die in OpenScape 4000 freigegebenen SIP-Provider und SIP-Trunking-Partner sind in den OpenScape 4000-Versionshinweisen aufgeführt. Die Liste wird mit jedem Minor oder Fix Release aktualisiert.

Mehr Informationen finden Sie im Kapitel 5, „SIP-Carrier / SIP Service Provider konfigurieren“.

14.3.2.3.2 Remote Agent Server-Konnektivität

Der Remote Agent-Server ermöglicht die Konnektivität von Agenten über Mobiltelefone, Festnetztelefone oder beliebige MFV-Telefone. Diese Konnektivität wird über eine native SIP-Trunk-Schnittstelle bereitgestellt.

Weitere Informationen finden sie in der Dokumentation zur Remote Agent Server-Lösung.

14.3.2.3.3 Applikationen

Native SIP-Trunking wird aber auch für die Konnektivität zu anderen firmeneigenen Applikationen genutzt, z.B. zu OpenScape Xpressions.

14.3.2.4 Konfiguration

14.3.2.4.1 Allgemeine Konfiguration

Siehe Kapitel 6, „Konfiguration SIP-Q-Trunking / Native SIP Trunking“ oder Kapitel 5, „SIP-Carrier / SIP Service Provider konfigurieren“.

14.3.2.4.2 Konfiguration der Codecs

OpenScape Xpressions unterstützt die folgenden Codecs:

- G711-A,
- G711-µ
- G729AB.

Die Konfiguration der Codecs erfolgt über AENDERN-CGWB bzw. über WBM:

1) `AENDERN-CGWB:MTYP=CGW,LTU=<LTU>,EBT=<SLOT>,TYP=ASC,PRIO=PRIO1,CODEC=<CODEC>,RTP=<RTP>;`

14.3.3 SIP-Trunk Profile

SIP-Trunk-Profile werden für native SIP-Trunking-Verbindungen benötigt und können im WBM konfiguriert werden.

Es ist auch möglich, SIP-Q Trunking-Verbindungen (z. B. zu OpenScape Voice) über das WBM mit SIP-Trunk-Profilen zu konfigurieren.

Informationen zu verfügbaren SIP-Trunk-Profilen finden Sie in Abschnitt 3.3.2, „Standardprofile“.

14.3.3.1 Allgemeine Informationen

- Sicher
- Wenn Proxy und/oder Registrar, Inbound-Proxy und/oder Outbound-Proxy über das WBM konfiguriert sind, wird jeder eingehende Anruf überprüft, ob die Partneradresse konfiguriert ist. Wenn nicht, wird der Anruf abgewiesen (mit 403 Forbidden).

  Hinweis: Wenn keine Profile für Native SIP Trunk verwendet werden, findet keine Prüfung der Partner-IP statt, weshalb das Gateway anfällig für gefälschte SIP-Anrufe ist. In diesem Fall muss das Gateway auf andere Weise geschützt werden, z. B. durch Trennung des VLAN vom Client-Netzwerk.
- Das richtige Profil für den richtigen Partner
- Trunk-Profile sind bereits auf die spezifischen Bedürfnisse eines SIP-Trunk-Partners zugeschnitten, z. B. wenn in einem ausgehenden FROM-Header-Account oder einer Rufnummer gesendet werden soll.

  Generische Profile sind verfügbar, wenn ein Partner nicht zertifiziert ist.
- DNS SRV Unterstützung

- DNS SRV gibt über DNS bekannt, welche IP-basierten Services (z. B. SIP) in einer Domäne (z. B. SIP-Provider-Domäne) bereitgestellt werden. Mit DNS/SRV können mehrere Partner-IP-Adressen konfiguriert werden.

  Das DNS SRV-Timeout wird von zwei Faktoren beeinflusst:

  Transaktions-Timeout konfiguriert in:

  – RFC 3261 Timer-Werte
  – WBM-Voice Gateway-SIP-Parameter-RFC 3261 Timer-Werte-Transaktions-Timeout

  Timeout beim Sperren

  – DNS-SRV-Einträge / SIP-Flooding-Abwehr
  – WBM-Voice Gateway-SIP-Parameter-Sperrzeit für unerreichbares Ziel/ Flooding-Abwehr

  Wenn z. B. DNS SRV zwei Partner-IP-Adressen, IP1 und IP2, enthält und bei einem Invite an IP1 keine Antwort erfolgt, sendet das GW die Anfrage nur bei UDP bis zum Timeout weiter. Zuerst nach 500 ms, dann verdoppelt sich das Intervall nach jeder erneuten Übertragung. Nach Ablauf der Transaktionszeit wird IP2 für die laufende und die nächsten Transaktionen für die Dauer des "Sperr-Timeouts" kontaktiert und IP1 wird gesperrt.

  Hinweise:
- Es kann nur ein Profil aktiviert werden.
- Die Trunk-Profile „Profile für Trunks via Native SIP verwenden“ dürfen nur zu Testzwecken deaktiviert werden.
- Outbund-Proxy muss konfiguriert werden, wenn ein Session Border Controler (SBC) für LAN/WAN Nat-Traversal verwendet wird.

14.3.3.2 Standardprofile

Neben speziellen Profilen für SIP-Trunk-Partner gibt es SIP-Trunk-Standardprofile für Native SIP und SIP-Q:

zum Beispiel:

- native SIP-Trunking
- – Profile für SIP-Service-Provider
  – OpenScapeUC
  – NATTrkEnterprise (empfohlenes Profil für SIP-Anwendungen von Drittanbietern mit REFER)
  – NatTrkWithoutRegistration

  Verwenden Sie dieses Profil für einen externen nativen SIP-Trunk-Partner ohne Registrierung.

  – NatTrkWithRegistration

  Verwenden Sie dieses Profil für einen externen nativen SIP-Trunk-Partner mit Registrierung.
- SIP-Q-Trunking

- – SIPQTrkWithoutRegistration

  Verwenden Sie dieses Profil für einen internen SIP-Q-Trunk-Partner ohne Registrierung.

  – SIPQTrkWithRegistration (SIPQ Trunking mit Registrierung)

  Verwenden Sie dieses Profil für einen internen SIP-Q-Trunk-Partner mit Registrierung

  Die Profile für SIP-spezifische Provider wurden getestet und (siehe auch Versionshinweis) freigegeben. Die Liste der Profile kann um Minor Releases / Hotfixes erweitert werden.

14.3.3.3 Aktivieren der SIP-Trunk Profile

Bevor ein Profil aktiviert werden kann, muss es konfiguriert werden.

14.3.3.3.1 Native SIP-Trunk Profile

1) Die SIP-Protokollvariante für IP-Vernetzung muss in AMO CGWB (Parameter **TRPRSIP**) auf Native SIP eingestellt werden.
2) Die Verwendung von SIP-Trunk-Profilen für Native SIP-Trunking muss im WBM aktiviert sein (Standardeinstellung).
3) Aufruf:

   WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter > (rechte Maustaste) Kontrollkästchen **„Use Profiles for Trunks via Native SIP“ aktivieren**



Abbildung 202: Native SIP-Trunk-Profile aktivieren

Wenn die Verwendung von Profilen im Menü aktiviert ist, wird im WBM unter „Voice Gateway“ (Sprachgateway) der Eintrag **SIP Trunk Profiles** angezeigt (siehe Abschnitt 3.3.4, „Menü „SIP-Trunk-Profile““).

14.3.3.3.2 SIP-Q-Trunk Profile

1) Die SIP-Protokollvariante für IP-Vernetzung muss in AMO CGWB (Parameter **TRPRSIPQ**) auf SIP-Q eingestellt werden.
2) Standardmäßig sind die SIP-Trunk-Profile für SIP-Q im WBM deaktiviert. Die Verwendung von SIP-Q Trunk-Profilen muss im WBM aktiviert werden:
3) **WBM > Configuration > Voice Gateway > SIP Trunk Profile Parameter >** (rechte Maustaste) Kontrollkästchen **„Use Profiles for Trunks via SIP-Q“ aktivieren**

   Wenn die Verwendung von Profilen im Menü aktiviert ist, wird im WBM unter „Voice Gateway“ (Sprachgateway) der Eintrag **SIP Trunk Profiles** angezeigt (siehe Abschnitt 3.3.4, „Menü „SIP-Trunk-Profile““).

14.3.3.4 Menü „SIP-Trunk-Profile“

Wichtig: Die Verwendung von Profilen muss aktiviert werden, um das Menü **SIP Trunk Profile Parameter** zu sehen (siehe Abschnitt 3.3.3, „Aktivieren der SIP-Trunk Profile“).

Es stehen verschiedene SIP-Trunk-Profile zur Verfügung (siehe Abschnitt 3.3.2, „Standardprofile“).

1) WBM > Configuration > Sprachgateway > SIP-Trunk-Profile

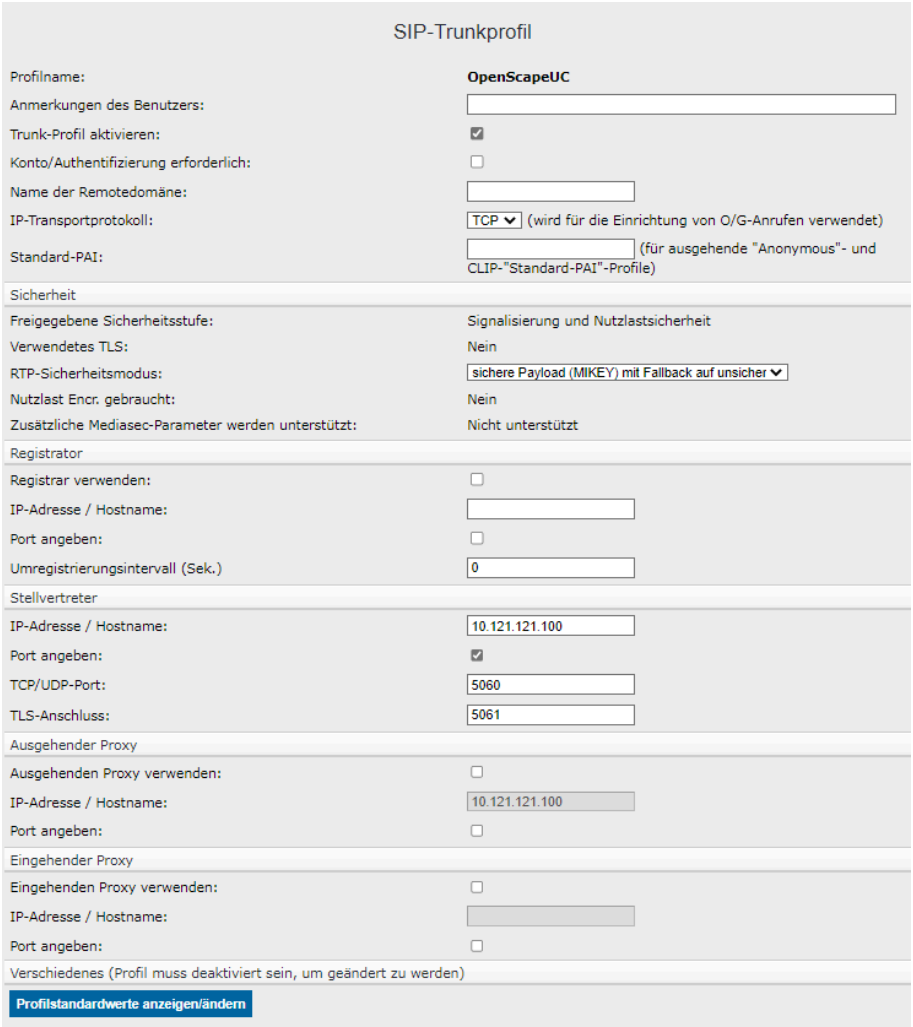


Abbildung 203: Beispiel für ein Standardprofil:

14.3.3.4.1 Ändern

Die folgenden SIP-Trunk-Parameter können konfiguriert werden.

- **Konto/Authentifizierung erforderlich** (siehe Abschnitt 3.3.4.2, "Authentifizierung")
- **Name der Remote-Domäne**
- **SIP Transport-Protokoll**
- **Registrar, IP-Adresse/Hostname** und/oder **Port**
- Proxy
- Inbound-Proxy

- Outbound-Proxy
- **Sicherheit** (siehe Abschnitt 3.3.4.3, "Sicherheit")

Wenn im SIP-Trunk-Profil für Registrar, Proxy, Inbound Proxy oder Outbound Proxy anstelle von IP-Adressen DNS-Namen konfiguriert sind, wird für deren Auflösung DNS SRV verwendet.

Die Parameter des Expertenmodus für SIP-Trunk-Profile können über die Schaltfläche "Profil-Standardwerte anzeigen/ändern" angezeigt und geändert werden (nur für ein nicht aktiviertes Profil).

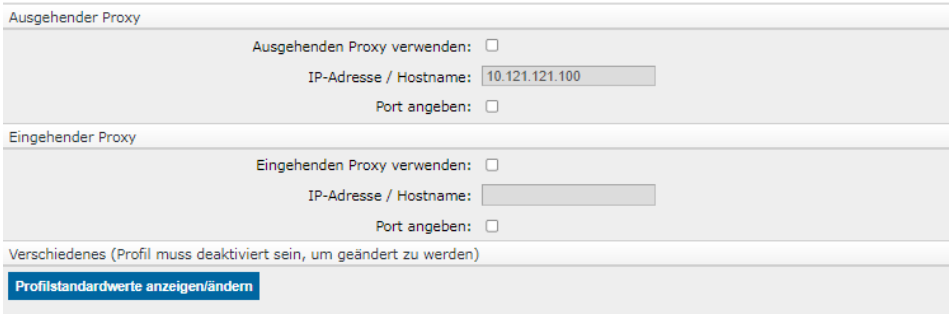


Figure 204: Anzeigen/Ändern von Profilvorgaben für SIP-Trunk-Profile

Es wird ein geändertes Profil angezeigt, wie in der folgenden Abbildung dargestellt:

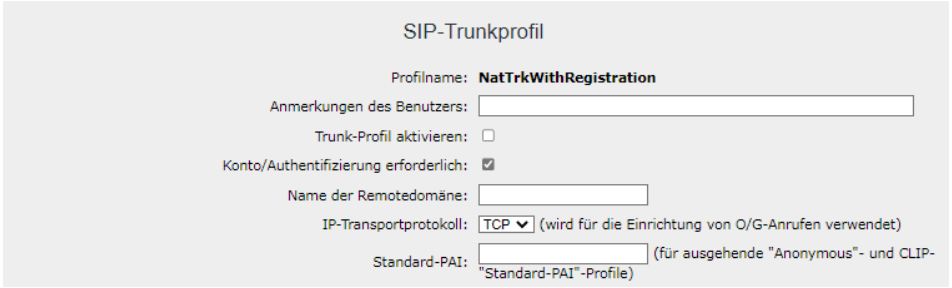


Figure 205: Anzeige eines geänderten Profils

Die Schaltfläche "Profil-Standardwerte zurücksetzen" setzt nur die Parameter des "Expertenmodus" auf die Standardwerte zurück:

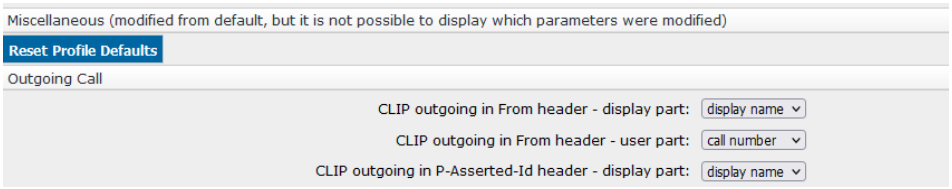


Figure 206: Profil-Standardwerte zurücksetzen

Nach dem Ändern der Parameter muss die Schaltfläche "Übernehmen" gedrückt werden.

Es wird empfohlen, die Standardprofilparameter zu verwenden und sie nur nach Rücksprache mit GVS zu ändern. Die Unterstützung für geänderte Profile ist eingeschränkt, da die Profile nicht mehr dem zertifizierten Standard entsprechen. Wir behalten uns das Recht vor, Softwareerweiterungen für geänderte Profile abzulehnen.

Probleme mit aktuellen Software-Builds, die eine Profiländerung erfordern, um korrekt mit einem zertifizierten SIP-Partner zusammenzuarbeiten, sollten gemeldet werden, um alle Zertifikatsdiskrepanzen zu untersuchen und zu beheben.

14.3.3.4.2 Authentifizierung

Wenn der Trunk-Partner „Authentifizierung“ erfordert, muss dies im Profil konfiguriert werden. Die Authentifizierungsdaten (Login und Passwort) werden vom Trunking-Partner bereitgestellt.

Wichtig: Die Authentifizierung muss vor dem Aktivieren des SIP-Trunk-Profils konfiguriert werden.

Vorgehensweise:

1) Im SIP-Trunk-Profil Menü, Checkbox **Account/Authentifizierung nötig** aktivieren.
2) Rechte Maustaste **Account/Authentifizierung hinzufügen** aus dem Menü auswählen und die Daten eintragen (die Daten werden vom Trunking-Partner zur Verfügung gestellt).

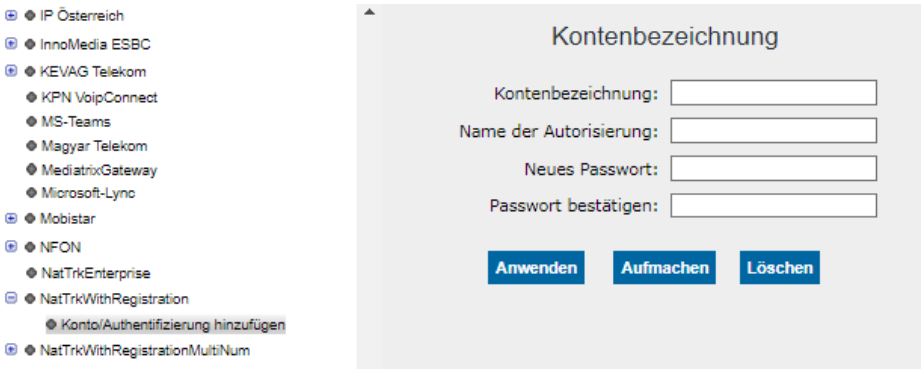


Abbildung 207: Account/Authentifizierung hinzufügen (Beispiel)

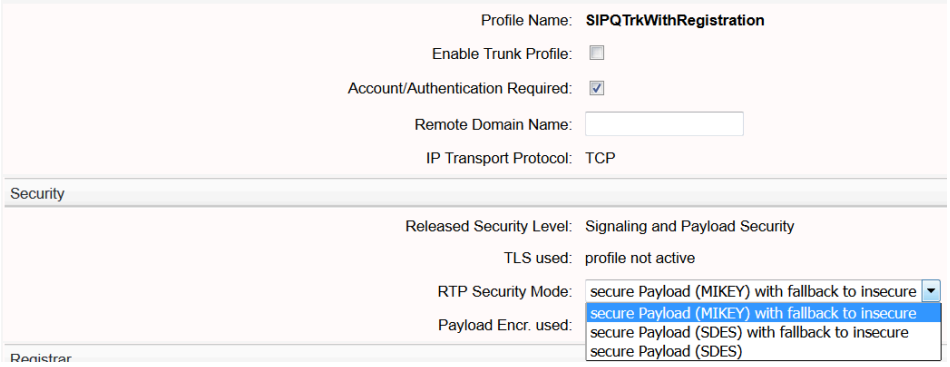
1) Profil aktivieren (siehe Abschnitt 3.3.4.4, „Aktivieren“).

14.3.3.4.3 Security

Die Security-Paramter sind unterschiedlich für native SIP-Trunk-Profile und SIP-Q-Trunk-Profile.

RTP-Security-Mode bei SIP-Q-Trunk-Profilen

Für SIP-Q Trunk-Profile kann der RTP-Sicherheitsmodus konfiguriert werden. Da die Common Gateway-Baugruppe keine Unterstützung für SDES bietet, wird dieses Menü nicht angezeigt. Wenn alle Bedingungen für SRTP erfüllt sind, wird die Payload gemäß der Konfiguration verschlüsselt.



Security-Konfiguration bei SIP-Q-Trunk-Profilen

Sicherheitsmodus für Native SIP-Trunking

Für den Native SIP-Trunk wird der Sicherheitsmodus angezeigt. Der Sicherheitsmodus wird durch AMO TDCSU und durch die freigegebene Sicherheitsstufe des ausgewählten SIP-Trunk-Partners definiert.

Die Common Gateway-Baugruppe bietet keine Unterstützung für Payload-Sicherheit auf dem Native SIP-Trunk. Wenn alle Bedingungen erfüllt sind, werden Sicherheit, Signalisierung und/oder Payload verschlüsselt. Die Payload wird mit dem getesteten und freigegebenen SDES-Modus verschlüsselt.



Security-Konfiguration bei SIP-Q-Trunk-Profilen

14.3.3.4.4 Aktivieren

Bevor ein Profil aktiviert werden kann, muss es konfiguriert werden.

Vorgehensweise:

1) Markieren Sie ein SIP-Trunk-Profil.
2) Aus dem Menü (rechte Maustaste) **Aktivieren** auswählen.

Wichtig: Wenn im eingerichteten Profil „Account/ Authentifizierung nötig“ aktiviert ist, muss ein Account mit Authentifizierungsdaten **vor** der Profile-Aktivierung hinzugefügt werden (siehe Abschnitt 3.3.4.2, „Authentifizierung“).

14.3.3.4.5 Deaktivieren

Vorgehensweise:

1) Markieren Sie ein SIP-Trunk-Profil.
2) Aus dem Menü (rechte Maustaste) **Deaktivieren** auswählen.

Ist die Deaktivierung erfolgreich, so wird die Grünfärbung zurückgenommen.

14.3.3.4.6 Löschen

Bevor ein SIP-Trunk-Profil gelöscht werden kann, müssen zunächst alle Konten gelöscht werden.

Vorgehensweise:

1) SIP-Trunk-Profil markieren.

2) Aus dem Menü (rechte Maustaste) Löschen auswählen.

Das ausgewählte Profil wird gelöscht.

14.3.3.5 Parameter für den Expertenmodus

Über die Schaltfläche "Profilvorgaben anzeigen/ändern" können die Parameter des Expertenmodus für SIP-Trunk-Profile angezeigt und geändert werden (nur bei einem nicht aktivierten Profil).

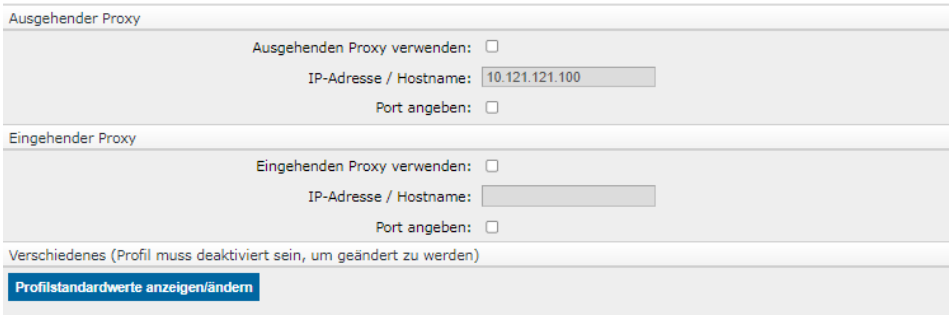


Figure 208: Profilvorgaben für SIP-Trunk-Profile anzeigen/ändern

Ein geändertes Profil wird wie in der Abbildung unten dargestellt angezeigt:

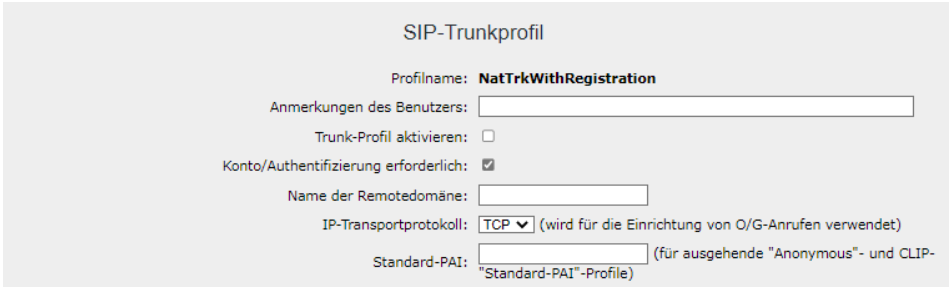


Figure 209: Anzeige eines geänderten Profils

Die Schaltfläche "Profil-Standardwerte zurücksetzen" setzt nur die "Expertenmodus-Parameter" auf die Standardwerte zurück:

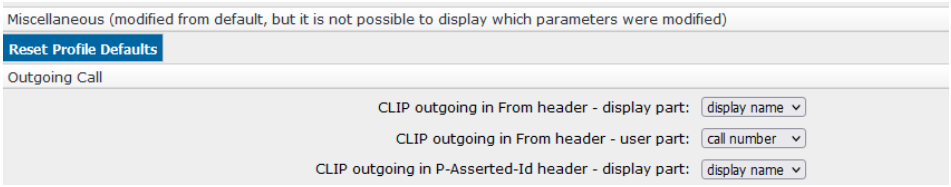


Figure 210: Reset Profile Defaults

Nach dem Ändern der Parameter muss die Schaltfläche "Übernehmen" gedrückt werden.

NOTICE: Es wird empfohlen, die Standardprofilparameter zu verwenden und sie nur nach Rücksprache mit GVS zu ändern. Die Unterstützung für modifizierte Profile ist eingeschränkt, da die Profile nicht mehr dem zertifizierten

Standard entsprechen. Wir behalten uns das Recht vor, Softwareerweiterungen für modifizierte Profile abzulehnen.

Probleme mit aktuellen Software-Builds, die eine Profiländerung erfordern, um korrekt mit einem zertifizierten SIP-Partner zusammenzuarbeiten, sollten gemeldet werden, um alle Zertifikatsdiskrepanzen zu untersuchen und zu beheben.

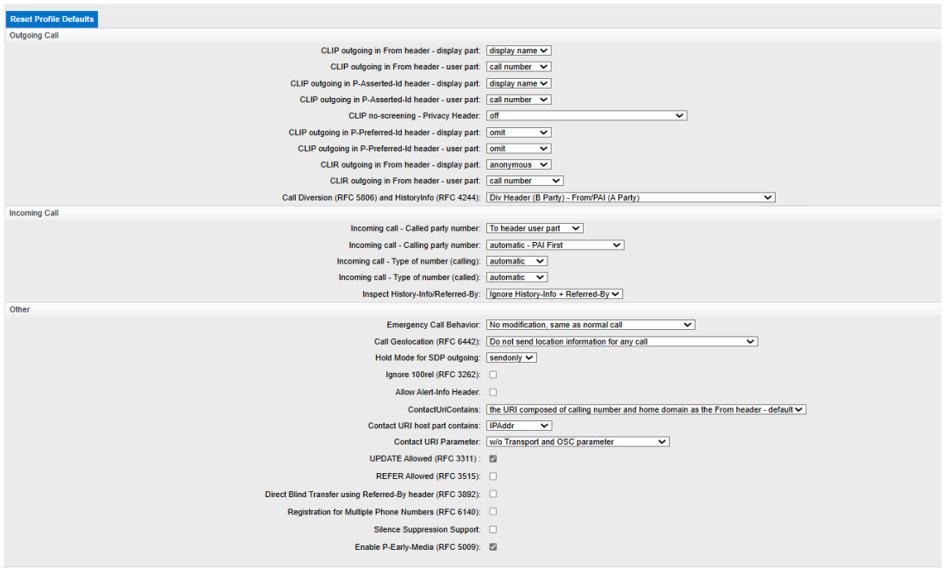


Figure 211: Parameter für den Expertenmodus

Ausgehender Anruf

Änderung des SIP-Headers entsprechend der WBM-Beschreibung.

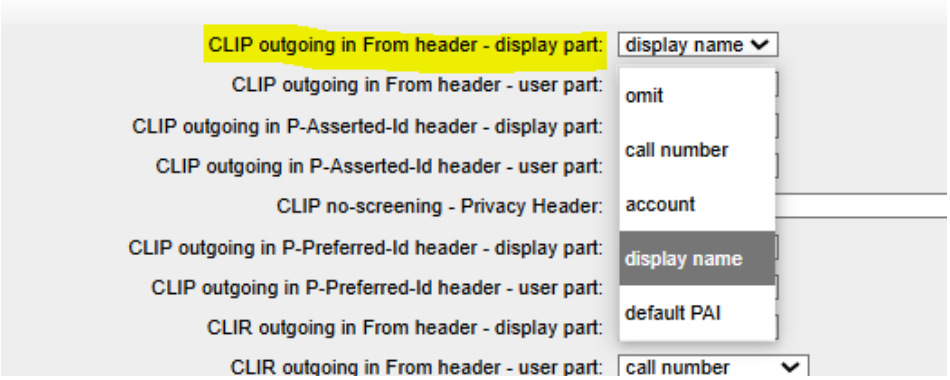


Figure 212: Ausgehender CLIP in Von Header - Anzeigeteil

Zusätzliche Informationen:

- A**uslassen:** Die SIP-Header-Informationen werden nicht gesetzt.
- Standard-PAI: **Parameter aus dem Hauptmenü für die Konfiguration des Trunk-Profils**.

Wenn Konto ausgewählt ist, wird der konfigurierte Kontoname (AOR) verwendet.

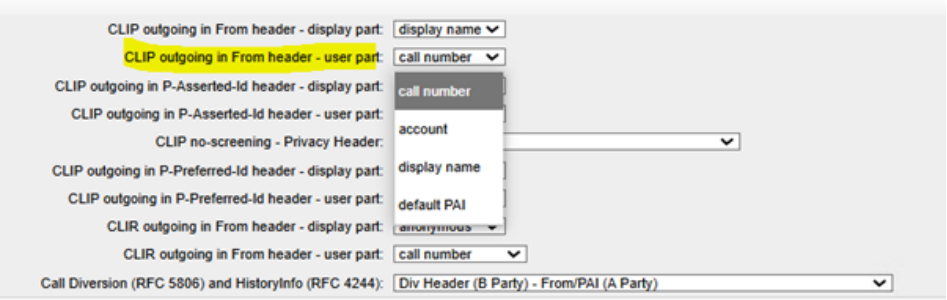


Figure 213: CLIP ausgehend im From-Header - {{user}}-Teil

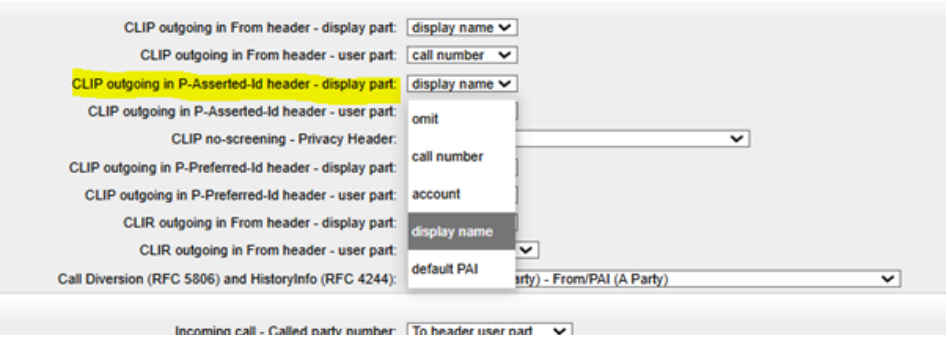


Figure 214: CLIP outgoing im P-Asserted-Id-Header - Anzeigeteil

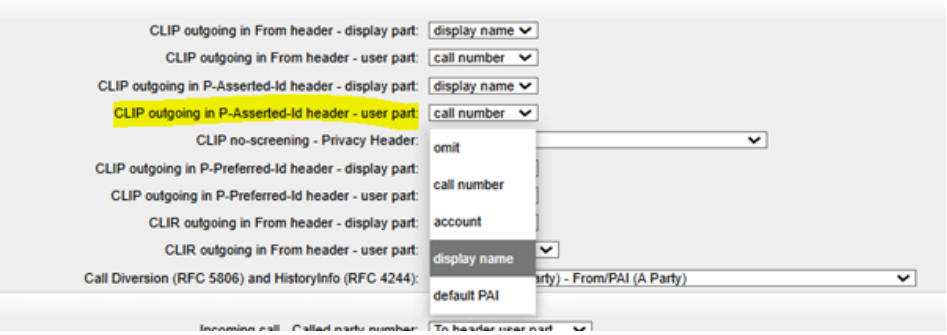


Figure 215: CLIP ausgehend im P-Asserted-Id-Header - {{user}}-Teil

NOTICE: Nicht benutzt.

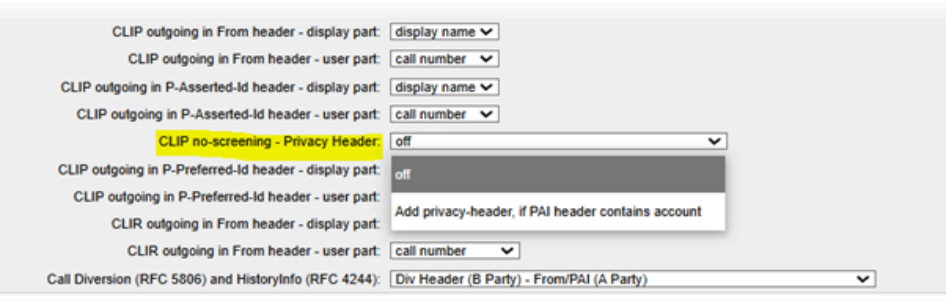


Figure 216: CLIP ausgehend in der P-Preferred-Id-Kopfzeile - Anzeigeteil

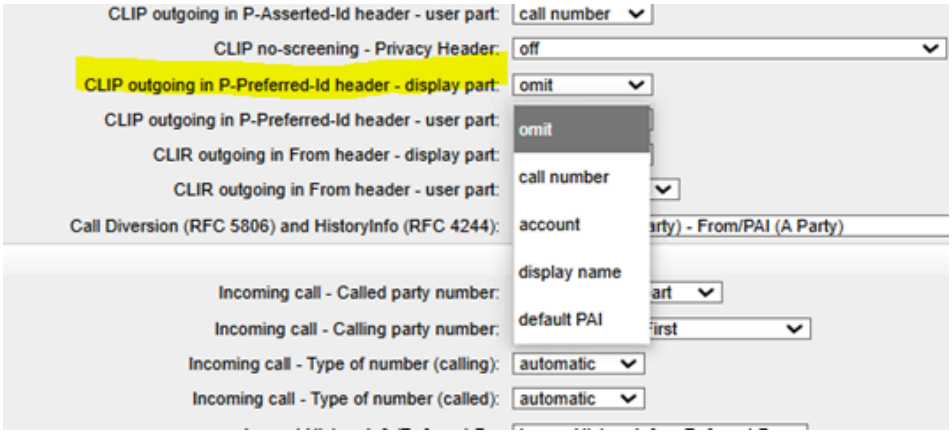


Figure 217: CLIP ausgehend in der P-Preferred-Id-Kopfzeile - Anzeigeteil

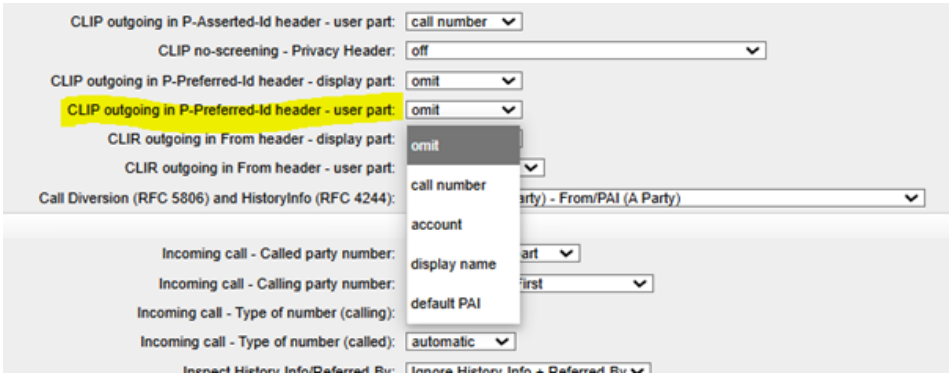


Figure 218: CLIP abgehend im P-Preferred-Id Header - {{user}}teil

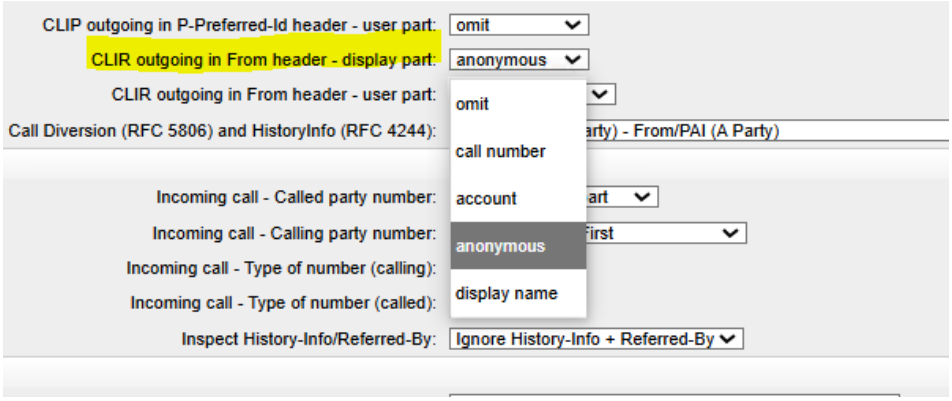


Figure 219: CLIR abgehend im From Header - Anzeigeteil

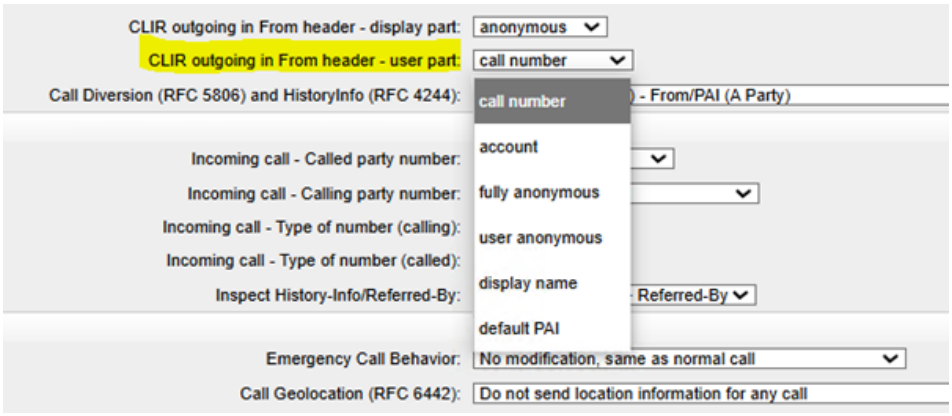


Figure 220: CLIR abgehend im From-Header - {{user}}-Teil

Zusätzliche Informationen zu CLIR:

- Wenn die Nummerndarstellung auf eingeschränkt eingestellt ist (d.h. über den AMO SBCSU-Parameter SSTNO - geheime Rufnummer - auf **ja** gesetzt), wird der **From Header** auf den entsprechenden Wert gesetzt.
- Der Outgoing Privacy Header kann nicht über die GUI eingestellt werden, sondern nur über die Erstellung eines neuen Profils.
- Voreinstellung: Der Privacy Header wird auf **Privacy: id** gesetzt
- Wenn **vollständig anonym** ausgewählt ist, werden sowohl die Nummer als auch der Host-Teil auf anonym gesetzt:

  <sip:anonymous@anonymous.invalid>
- Wenn **{{user}} anonym** ausgewählt ist, wird nur die Rufnummer auf anonym gesetzt:

  d.h.: <sip:anonymous@tel.t-online.de>



Figure 221: Konfiguration der verwendeten Header im {{case}} einer Anrufumleitung

NOTICE: Wenn **History Info Header** ausgewählt ist, wird **Index 1** für die Umleitungsnummer **B** verwendet.

Eingehender Anruf

Behandlung der Rufnummer entsprechend der WBM-Beschreibung.

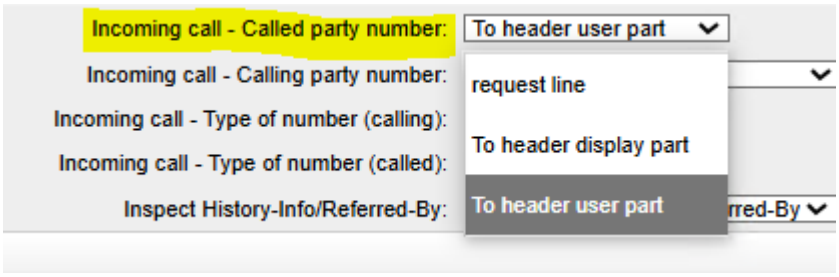


Figure 222: Eingehender Anruf - Rufnummer des angerufenen Teilnehmers

Definition, welcher Header verwendet wird, um die Rufnummer des angerufenen/anrufenden Teilnehmers zu ermitteln.

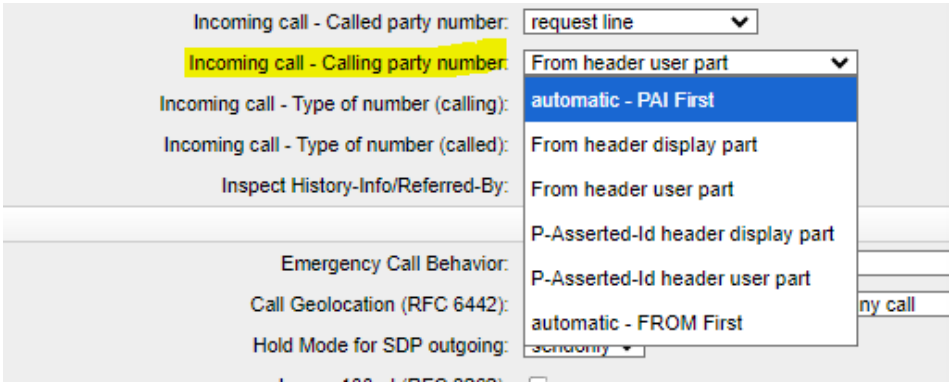


Figure 223: Eingehender Anruf - Rufnummer des angerufenen Teilnehmers

Eingehender Anruf - Rufnummer des anrufenden Teilnehmers - Automatisch:

Überprüfung der verfügbaren Header und wenn es einen PAI-Header gibt, wird die Rufnummer des Anrufers aus dem PAI extrahiert, wenn nicht, wird der From-Header verwendet.

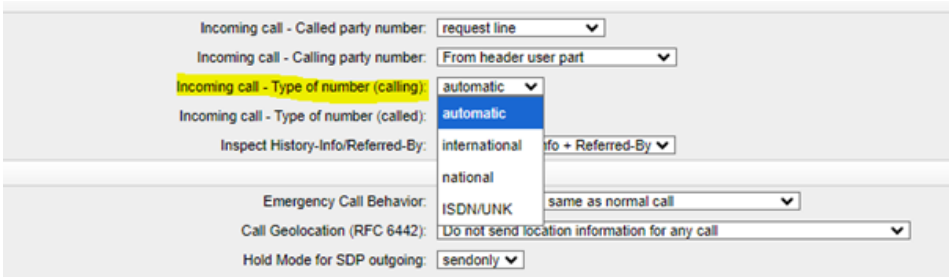


Figure 224: Eingehender Anruf - Art der Rufnummer (anrufender Teilnehmer)

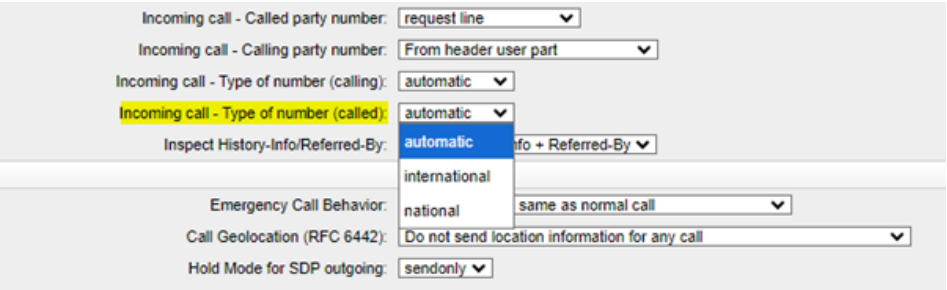


Figure 225: Eingehender Anruf - Art der Rufnummer (angerufener Teilnehmer)

Eingehender Anruf - Art der Nummer - automatisch:

Wenn ein führendes "+" gefunden wird, werden die Ziffern reduziert (kein "+") und TON=international wird gesetzt

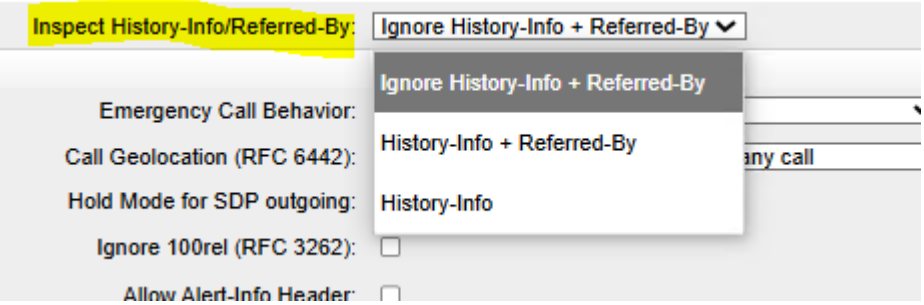


Figure 226: History-Info/Referred-By prüfen

Wenn ausgewählt, werden **SIP History-Info oder Referred-By Header** verwendet, um eine Weiterleitungsnummer anzuzeigen.

Standard: **Ignorieren - Diversion Header** wird verwendet.

Andere Parameter

Verhalten bei Notrufen und **Geolokalisierung von Anrufen (RFC 6442)**

Siehe Kapitel Anrufe

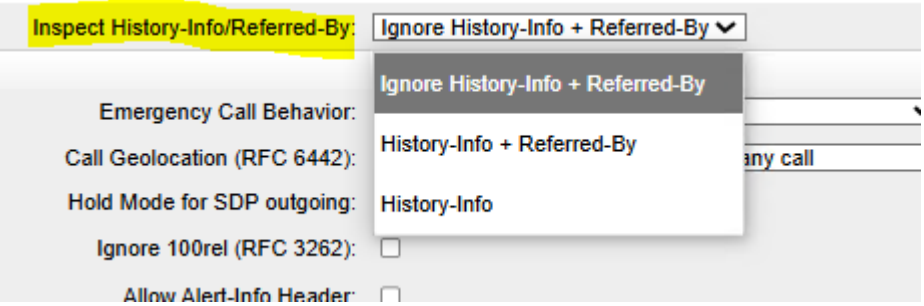


Figure 227: Hold-Modus

Definiert den verwendeten SDP-Wert im Falle eines gehaltenen Anrufs, z. B. „a=sendonly".

Ignorieren 100rel (RFC 3262)

- Wenn ausgewählt, sind vorläufige Antworten deaktiviert.
- Das GW bietet kein SDP bei 180 Ringing an.

- Wenn nicht ausgewählt, bietet das Gateway 100rel (SIP „Supported: 100rel“) bei ausgehenden Einladungen an und fügt ein „Require: 100rel“ zu einem z. B. 180 Ringing, um ein PRACK vom Partner zu erhalten.
- Analog dazu sendet es ein PRACK, falls erforderlich.
- Das Gateway bietet SDP bereits im 180 Ringing an.
- (Siehe auch Parameter "Disable SDP in 1xx unreliable responses")

Alert-Info-Header zulassen

Das OS4K-Gateway unterstützt generell die Bereitstellung von speziellen Arten der akustischen Alarmierung über den Alert-Info-Header (RFC 7462). Auf der nativen SIP-Trunk-Schnittstelle ist dieser Mechanismus standardmäßig ausgeschaltet.

Contact Header Parametrization

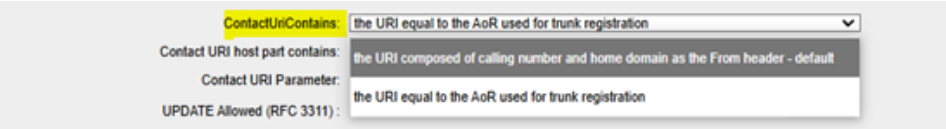


Figure 228: ContactUriEnthält

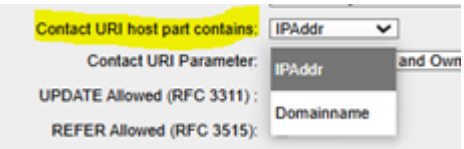


Figure 229: Contact Header Host-Teil

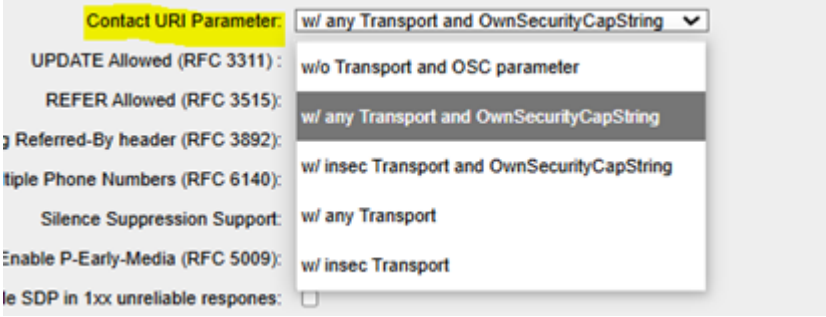


Figure 230: Contact Header URI-Teil

Beispiel Registrierung Contact Header:

- Contact URI enthält: "die URI, die der AoR entspricht, die für die Trunk-Registrierung verwendet wird"
- Kontakt URI Host Teil enthält: "IPAddr"
- Contact URI Parameter: mit beliebigem Transport und OwnSecurityCapString
- Kontakt: <sip:+491234567890@88.77.66.55:5061;transport=tls;+u.www.siemens.com/icn/en/oscar/sip/sec-level=Sicherheit>;expires=480

Beispiel für einen Registrierungs-Kontakt-Header:

- Kontakt-URI enthält: "die URI, die sich aus der Rufnummer und der Heimatdomäne zusammensetzt, als From-Header - Standard"
- Kontakt-URI Host-Teil enthält: "Domain-Name"
- Kontakt-URI-Parameter: mit beliebigem Transport

- <sip:+491234567890@tel.abcd.de:5061;transport=tls>;expires=480

UPDATE Allowed (RFC 3311)

- Das Gateway bietet kein SIP UPDATE im Allow Header an, wenn es nicht ausgewählt ist.
- Standard: Ausgewählt

REFER Allowed (RFC 3515)

- Das Gateway bietet im Allow Header kein SIP REFER an, wenn es nicht ausgewählt ist.
- Voreinstellung: Nicht ausgewählt für SIP Service Provider.
- Beispiel für die Verwendung von REFER: Nativer SIP-Trunk zu OpenScape UC.

Direct Blind Transfer using Referred-By header (RFC 3892)

- Aktiviert: Blind-Transfer direkt zurück zum SIP-Provider mit transparentem Referred-By Header
- Deaktiviert: Traditioneller Blind-Transfer über Trombone-Connect-Verbindung

Registration for Multiple Phone Numbers (RFC 6140)

- Registrierungsformat entsprechend RFC 6140
- Wenn aktiviert, fügt das Gateway die Option gin (generate implicit numbers) zu Proxy-Require und dem Contact URI hinzu, der den URI-Parameter "bnc" (bulk number contact) enthält.

Silence Suppression Support

- Das Attribut a=silenceSupp:on/off wird in den SDP-Daten verwendet,
- (ein/aus wird über `AMO CGWB VAD=on/off` gesteuert)

Enable P-Early-Media (RFC 5009)

- Aktiviert die Unterstützung des SIP P-Early-Media Headers (das Gateway bietet P-Early-Media = unterstützt).

> **NOTICE:** Siehe Release-Notes bezüglich der SW-Versionen, die P-Early-Media vollständig unterstützen

Disable SDP in 1xx unreliable response

- Wenn der Parameter "Ignore 100rel (RFC 3262)" nicht ausgewählt ist, kann das Gateway SDP bereits in vorläufigen Antworten anbieten. Dieses Verhalten kann durch Auswahl dieser Option ausgeschaltet werden.

  Nicht unterstützt - immer aus.

Send response to OPTIONS request

- Legt fest, ob SDP in der SIP OPTION ping Antwort gesendet wird.

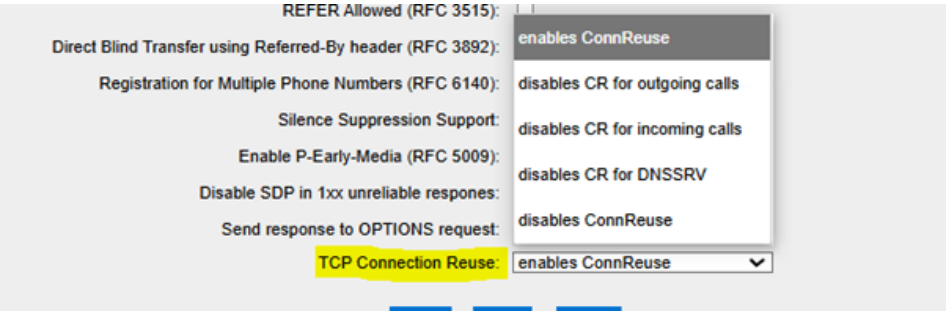


Figure 231: Wiederverwendung von TCP-Connect-Verbindungen

Bei der TCP-Verbindungswiederverwendung wird dieselbe TCP-Connect zum Senden und Empfangen mehrerer SIP-Anfragen und Antworten verwendet.

Wenn deaktiviert, wird eine neue TCP-Verbindung geöffnet, um eine neue Anfrage zu bearbeiten.

Standard: aktiviert

14.3.3.6 Konfiguration von SIP-Trunks mit Registrierung

Die Voraussetzungen für die Verwendung der SIP-Trunk-Profile müssen erfüllt sein (siehe Abschnitt 3.3.3, „Aktivieren der SIP-Trunk Profile“).

14.3.3.6.1 Native SIP-Trunk

1) Profil ändern
2) Verwenden Sie das Profil NatTrkWithRegistration für Native SIP-Trunk-Konfigurationen mit Registrierung. Konfigurieren von Benutzerkennung und Authentifizierung

   Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > (rechte Maustaste) Modify > Kontrollkästchen **Add Account/Authentication aktivieren**

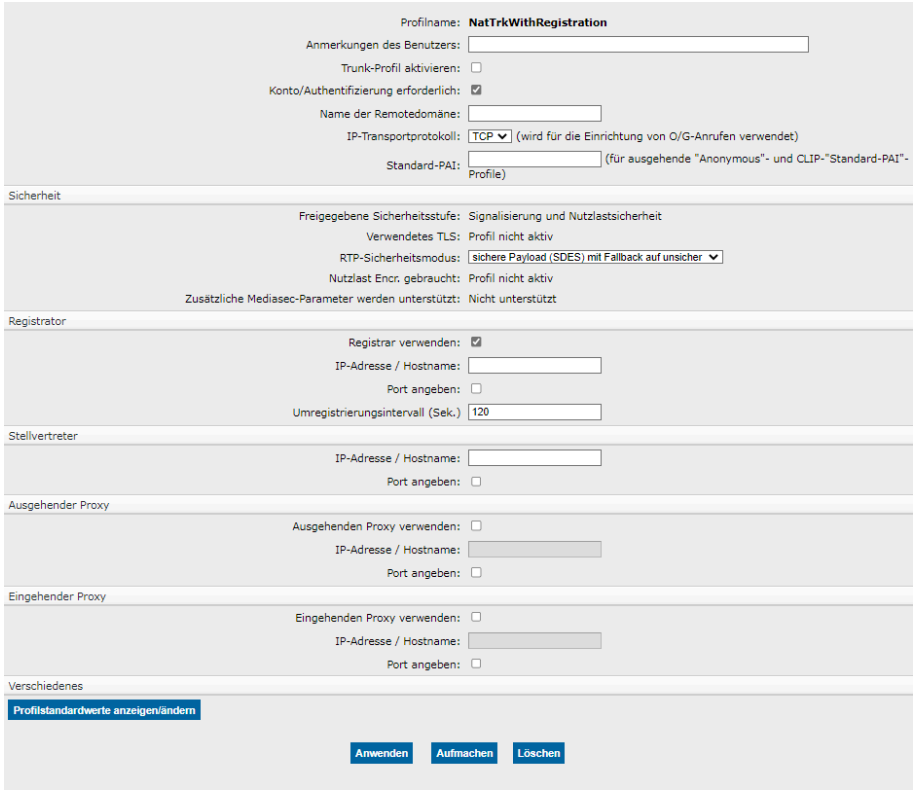


Abbildung 232: Account/Authentifizierungsdaten

3) IP-Adress/Host-Name und Domain-Name konfigurieren
4) **IP-Adresse/Hostname** (z. B. DNS-Name = provider.com) des SIP-Trunk-Partners wird in den Bereichen **Registrar** und **Proxy** konfiguriert. Der Remote-**Domänenname** weist in der Regel denselben Wert auf wie **IP-**

Adresse/Hostname (siehe Abschnitt **Registrar** oder **Proxy**) und dient als Host-Angabe in der URL der SIP-Nachrichten.

Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > (rechte Maustaste) Modify



SIP-Trunk-Profil eines Providers mit Registrierung

5) Profil aktivieren

6) Nach der Konfiguration aktivieren Sie das Profil. Wenn das Profil erfolgreich aktiviert wurde, wird es grün dargestellt.

Configuration > Voice Gateway > SIP Trunk Profile > NatTrkWithRegistration > Aktivieren

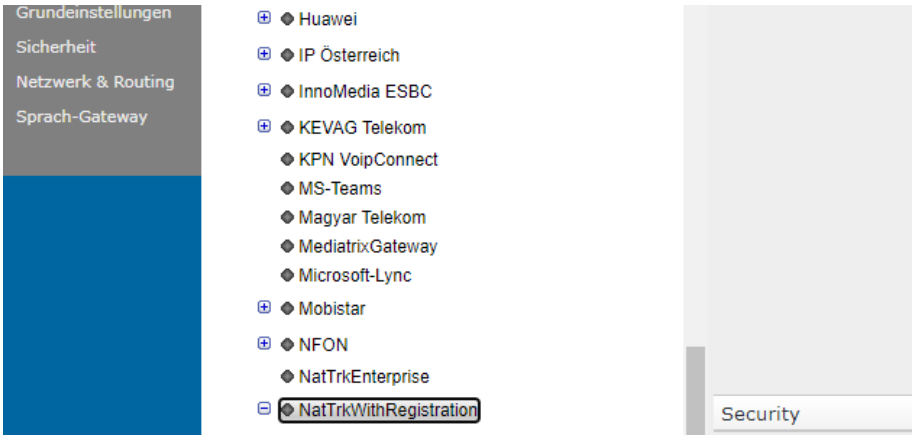


Abbildung 233: Aktiviertes SIP-Trunk-Profil mit Registrierung

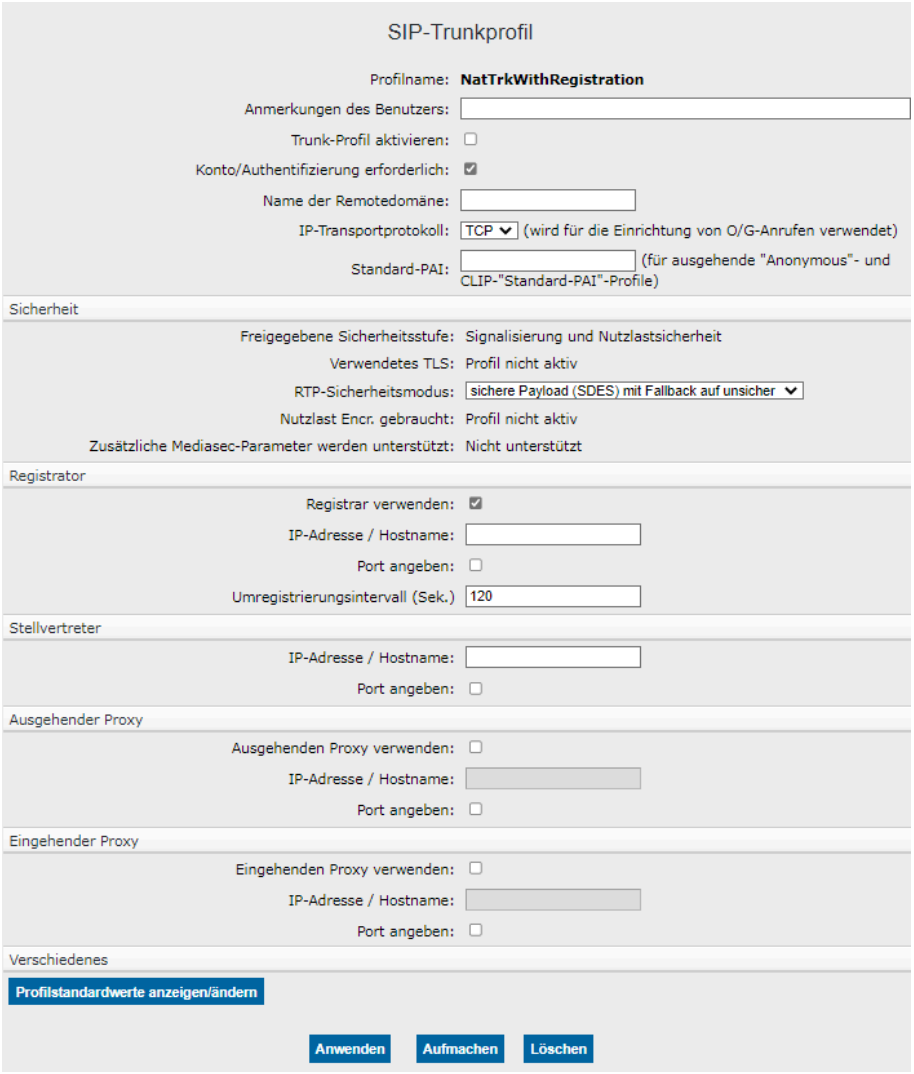


Abbildung 234: Aktiviertes SIP-Trunk-Profil mit Registrierung

14.3.3.6.2 SIP-Q-Trunk

1) Profil ändern

Das angebotene Profil „SIPQTrkWithRegistration“ kann für Trunk-Konfigurationen mit Registrierung verwendet werden. Der Accountname und die Authentifizierungsdaten (wenn benötigt) können konfiguriert werden.

Configuration > Voice Gateway > SIP Trunk Profile > SIPQTrkWithRegistration (SIPQ Trunking mit Registrierung) > (rechte Maustaste) Modify > Kontrollkästchen aktivieren:**Add Account/ Authentication**

2) IP-Adress/Host-Name und Domain-Name konfigurieren

Konfigurieren Sie den Wert **IP address/host name** (z. B. DNS-Name = provider.com) des SIP-Trunk-Partners in den Bereichen **Registrar** und **Proxy**. Der **Domänenname** weist in der Regel denselben Wert auf wie **IP-**

Adresse/Hostname (siehe Abschnitt **Registrar** oder **Proxy**) und dient als Host-Angabe in der URL der SIP-Nachrichten.

Configuration > Voice Gateway> SIP-Trunk-Profile > SIPQTrkWithRegistration > (rechte Maustaste) Modify

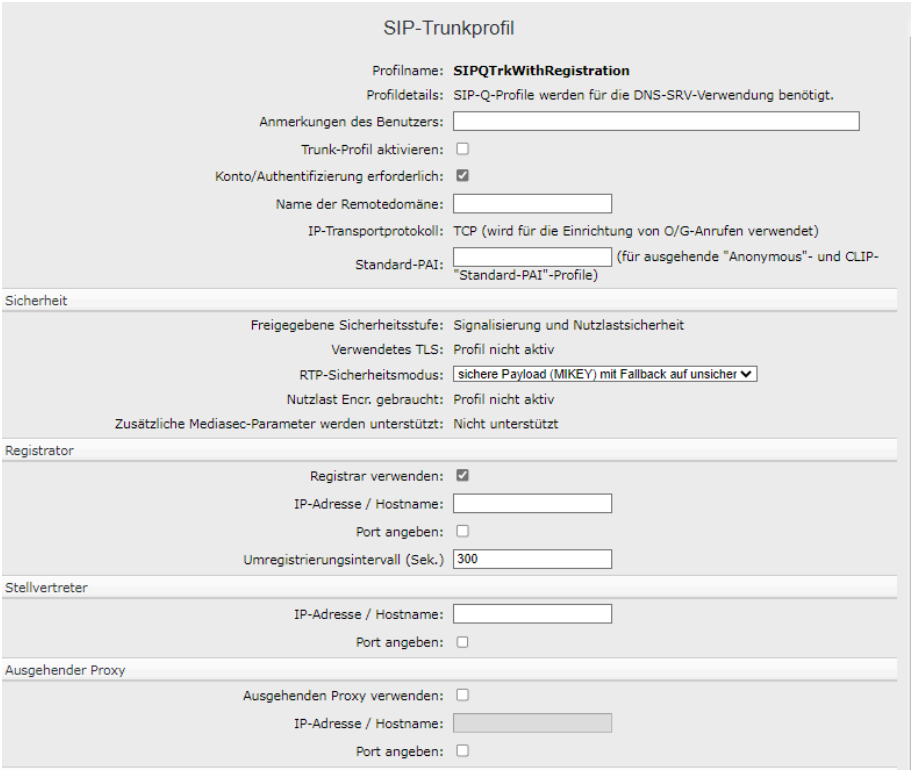


Abbildung 235: SIP-Q-Trunk-Profil mit Registrierung

3) Profil aktivieren

Nach der Konfiguration aktivieren Sie das Profil. Wenn das Profil erfolgreich aktiviert wurde, wird es grün dargestellt.

Configuration> Voice Gateway > SIP-Trunk-Profile > SIPQTrkWithRegistration > (rechte Maustaste) Activate

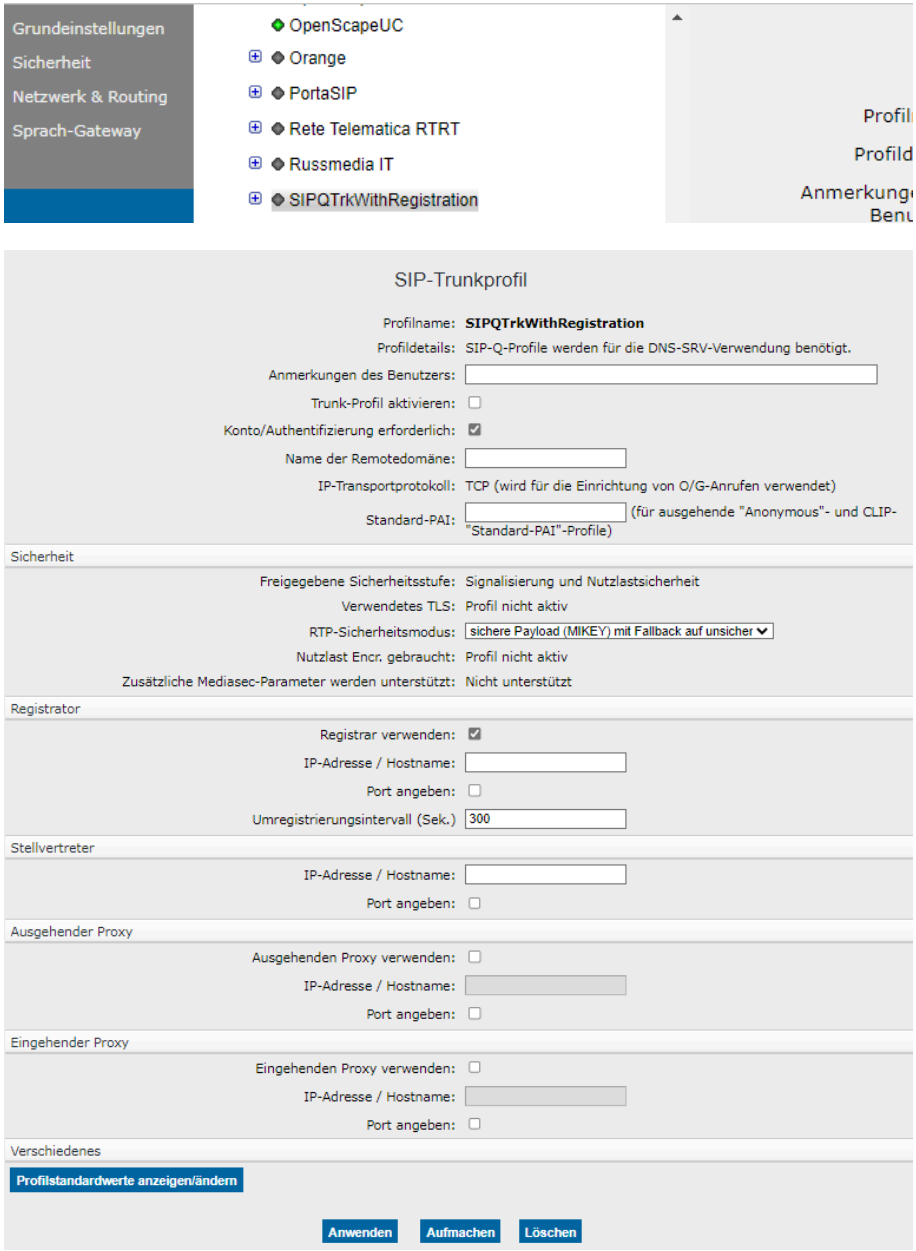


Abbildung 236: Aktiviertes SIP-Q-Trunk-Profil mit Registrierung

DNS SRV-Rückschaltfunktion für SIP-Q-Trunking

FQDNs (ohne Port-Einstellung) können für Registrar, Proxy und Outbound-Proxy (sofern verwendet) genutzt werden.

SIP-Registrierungsvorgang:

- Vor Beginn einer SIP-Q-Registrierung wird der FQDN des Registrars mithilfe des DNS SRV-Verfahrens aufgelöst.

- Dann wird eine TCP/TLS-Verbindung zu der IP-Adresse mit der höchsten Priorität hergestellt.
- Eine SIP OPTIONS-Nachricht wird gesendet, um zu prüfen, ob der Partner SIP-fähig ist.
- Anschließend wird eine REGISTER-Nachricht gesendet.
- Danach werden Anrufe an diese Partner-IP-Adresse gesendet.

Wenn das aktuelle Ziel nicht mehr erreichbar ist (z. B. Abbruch der TCP/TLS-Verbindung oder keine Antwort auf abgehende REGISTER- oder INVITE-Anfrage), wird die IP-Adresse mit der nächstniedrigeren Priorität kontaktiert und der oben beschriebene SIP-Registrierungsvorgang wiederholt.

Der Standardwert für das Abfrageintervall beträgt 60 Sekunden und kann im WBM unter **Configuration > Voice Gateway > SIP Parameters > DNS-SRV** konfiguriert werden. Er gilt auch für die Blacklisting-Dauer für nicht erreichbare IP-Adressen. Sobald eine IP-Adresse mit einer höheren Priorität (wieder) erreichbar ist, wird der oben beschriebene SIP-Registrierungsvorgang wiederholt.

14.4 Built-in SBC

Die folgenden Kapitel beschreiben wie in der OpenScape 4000 generelle Session Border Controller Spezifikationen abgedeckt werden.

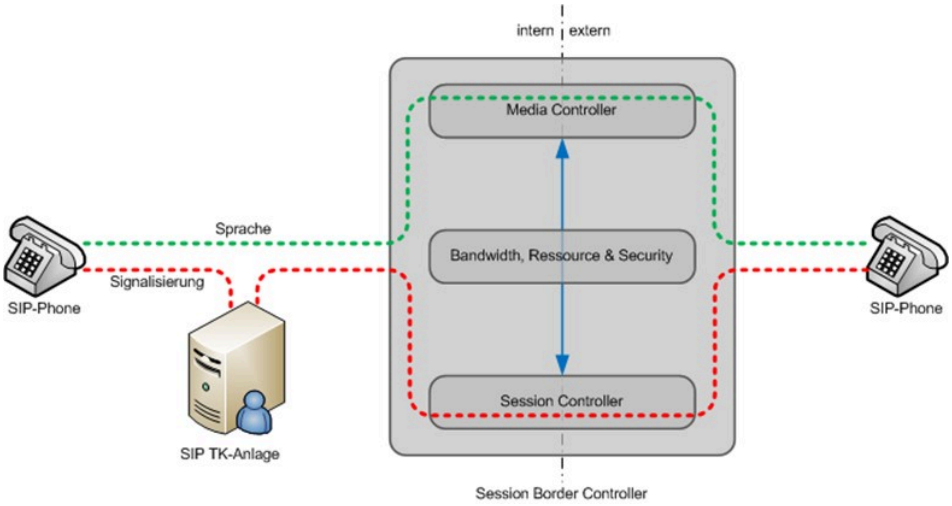
Das erste Kapitel beschreibt generelle Session Border Controller Spezifikationen welche aus Wikipedia als Quelle bezogen wurden.

Im Anschluss zeigt das Kapitel Built-in SBC Funktion auf wie diese generellen Session Border Controller Anforderungen in den OpenScape 4000 Gateways realisiert sind (Klassische HG Baugruppen wie STMIX, STMI4, STMI2 sowie bei virtuellen HGs in OpenScape 4000 SoftGate).

14.4.1 Generelle SBC Anforderungen (Quelle Wikipedia)

Ein Session Border Controller (SBC) ist eine Netzwerkkomponente zur sicheren Kopplung von verschiedenen Rechnernetzen oder Rechnernetzen mit unterschiedlichen Sicherheitsanforderungen. SBC werden hauptsächlich in IP-Telefonie-Netzwerken (VoIP) eingesetzt, um externe (unsichere) Datennetze mit internen (sicheren) IT-Strukturen zu koppeln beziehungsweise sogenannte Sitzungen zu implementieren. Ein SBC ermöglicht die Steuerung und Kontrolle über Signalisierung und in der Regel auch Media Streaming sowie Aufbau, Durchführung und Abbau von Telefongesprächen oder anderen interaktiven Medien die an einer Kommunikation beteiligt sind.

Ein SBC wird an Netzwerkgrenzen eingesetzt und koppelt interne und externe Netze. Der SBC analysiert die verschiedenen Datenströme (engl: sessions) und greift, je nach Konfiguration, in die verschiedenen Datenströme (hier: Sprache oder Signalisierungsdaten) ein. Im Bereich der IP-basierten Telekommunikation (VoIP) werden Signalisierungsdaten und die Sprach-/Bilddaten getrennt übertragen.



Funktionsprinzip des Session Border Controller bei VoIP

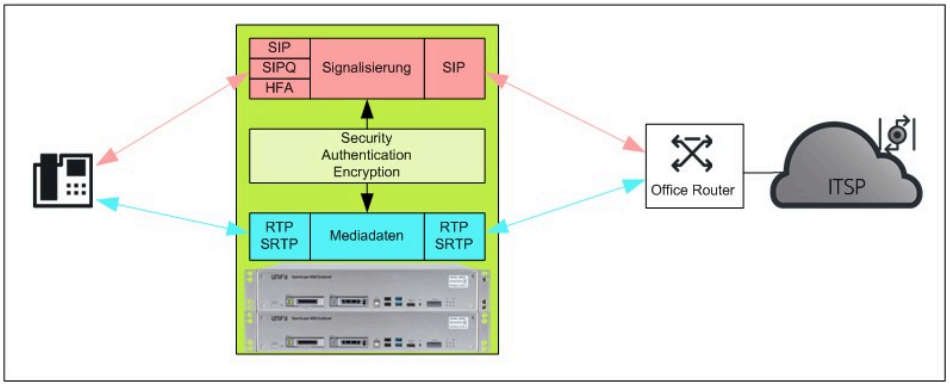
Ein SIP-basiertes Telefon sendet die Signalisierungsdaten in der Regel zur Telefonanlage, während die Sprachdaten in der Regel auf dem kürzesten Weg direkt von Telefon zu Telefon übertragen werden. Durch die Entkopplung von Signalisierungsdaten und Sprachdaten können einerseits die Vorteile von IP-basierten Datennetzen ausgeschöpft werden, andererseits kann die Übertragung der Sprachdaten (besser Mediendaten) nicht durch die Telefonanlage beeinflusst werden. Ein SBC vereint folgende Funktionen:

- **Security Offloading** Unterstützung von Verschlüsselungstechniken (TLS, SRTP)
- **Media Pinholing** Gezielte Freischaltung von UDP/TCP-Ports zur Übertragung von Mediadaten
- **Transcoding** Transkodierung zwischen verschiedenen Sprach/Video-Codecs wie zum Beispiel G.711 nach G.729
- **Protocol Translation** Umwandlung und Anpassungen bei verschiedenen Signalisierungsprotokollen wie zum Beispiel SIP nach SIP-Q (QSIG over SIP)
- **Header Manipulation** Anpassung der SIP und SDP-Header um zum Beispiel Rufnummernformate (E.164) oder IP-Adressen anzupassen
- **Media Anchoring** Kopplung der Sprachdaten von SIP-Endgeräten die nur über Network Address Translation erreichbar sind Sichere Kopplung von Sprach-/Videodaten

14.4.2 Built-in SBC Funktion

In einer OpenScape 4000 Umgebung gibt es diverse SBC Lösungskonzepte, wie z. B. die Nutzung eines OpenScape SBC, eines Hosted OpenScape SBC (hSBC) oder eines 3rd-Party SBC. Davon unabhängig besitzt jede OpenScape 4000 Komponente (Gateways) eine eingebaute „**Built-in SBC**“ Funktion, welche automatisch aktiv ist, wenn VoIP Verbindungen über einen Internet Telephony Service Provider (ITSP) geführt werden. Die Built-in SBC Funktionalität ist nicht zusammenhängend mit dem *Hosted OpenScape SBC (hSBC)* Feature der OS4K V8. Der *Hosted OpenScape SBC* muss gezielt aktiviert werden, wenn benötigt. Die Aktivierung der entsprechenden Built-in SBC Funktion erfolgt automatisch und ist immer aktiv. Eine explizite

Konfiguration ist nicht notwendig und daher in den Administrations Portalen (WBM) nicht vorgesehen.



OpenScape 4000 Built-in SBC Funktion

Die Built-in SBC Funktion wird auch bei der Anschaltung von:

- Secure Remote Subscriber HFA/SIP (@Home)

verwendet.

Die Verwendung eines externen SBC ist daher bei OpenScape 4000 nicht zwingend erforderlich. Nichtsdestotrotz wurde die OpenScape 4000 V8 mit dem Feature eines gehosteten OpenScape SBC (hSBC) erweitert, welcher selbstverständlich zuzüglich genutzt werden kann.

Für den Fall dass mehr wie 120 ITSP Verbindungen/Kanäle genutzt werden sollen, wird für Load Balancing zwischen OS4K Gateways (max. 120 B-Kanäle) - oder gar zwischen mehreren OS4K Standorten - ein OpenScape SBC benötigt.

Anmerkung: ITSP-Zertifizierungen an OpenScape 4000 werden hauptsächlich in Verbindung mit den Built-in SBC Funktionen durchgeführt. In manchen Fällen – z. B. Telekom DeutschlandLAN SIP-Trunk – wurde zusätzlich die Zertifizierung mit dem OpenScape SBC angestoßen.

- **Security Offloading**
- OpenScape 4000 unterstützt die Transport Protokolle UDP, TCP und TLS. Für den Medientransport wird RTP und SRTP unterstützt. Bei SRTP wird die Transcoding Funktion verwendet hierfür gelten die unter dem Punkt **Transcoding** beschriebenen Bedingungen.

  Im Default werden UDP/TCP und RTP verwendet. Bietet ein ITSP das TLS Transportprotokoll an, so kann dies mit der Signalisierungs- und Payload-Verschlüsselung (SPE) der OpenScape 4000 entsprechend konfiguriert und genutzt werden.

  Die Built-in SBC Funktion verfügt zusätzlich über Sicherheitsmerkmale wie:

  – Überlastabwehr (Network overload protection)
  – Adressfilter mit Whitelisting und Registration Blacklist

  Die Einstellung des Adressfilters wird aus den Konfigurationsdaten für Teilnehmer und ITSP Zugangsdaten abgeleitet (u. a. Inbound Proxy im SIP Provider Profil). Es sind keine weiteren spezifischen Konfigurationen notwendig.

- **Media Pinholing**
- Die Built-in SBC Funktion sorgt für eine Freischaltung von UDP-Ports im Internet Router zur Übertragung von Mediadaten. Hierzu ist keine spezifische Konfiguration notwendig.
- **Transcoding**
- Die Built-in SBC Funktion ist als „Routing Engine“ implementiert. Hierbei werden die IP Adressen und UDP Ports in den RTP Paketen entsprechend angepasst, die RTP Daten selbst bleiben jedoch unverändert.

  Das RTP Transcoding wird, wenn gewünscht, durch verschiedene Gateway Konfigurationen Gateway innerhalb der OpenScape 4000 realisiert. Hierfür müssen die jeweiligen Gateway Codecs per Gateway konfiguriert werden.

  Das Transcoding unterstützt alle in der OpenScape 4000 verfügbaren Codecs, wie z. B.:

  – G711
  – G729A
  – G729AB
  – G722
  – OPUS
  – â¦
- **Protocol Translation**
- OpenScape 4000 unterstützt die Anschaltung von IP Endgeräten mit unterschiedlichen Protokollen (HFA, SIP etc.) sowie verschiedene IP Leitungen mit SIPQ und/oder native SIP Protokoll. Die Built-in SBC Funktion übernimmt automatisch alle notwendigen Umwandlungen der Protokolle für einen reibungslosen Ablauf zwischen den verschiedenen Schnittstellen.
- **Header Manipulation**
- Die Built-in SBC Funktion übernimmt alle notwendigen Anpassungen der Protokollelemente wie IP-Adressen in SIP und SDP sowie der Rufnummernformate in allen SIP Header Feldern.

  Alle ITSP spezifischen Header-Parameter sind in Profilen hinterlegt, die bei der Zertifizierung des jeweiligen Anbieters festgelegt werden. Abweichende Konfigurationen sind über Profiländerungen möglich.
- **Media Anchoring**
- Die Built-in SBC Funktion terminiert alle Mediaströme zum ITSP und erlaubt auf diese Weise das Erreichen der internen Endpunkte über Network Address Translation. Pro Verbindung wird maximal ein RTP Stream unterstützt. Daher werden Video Verbindungen über die Built-in SBC Funktion nicht unterstützt.

  Der Portbereich für den RTP Stream ist voreingestellt kann jedoch bei Bedarf verändert werden.

14.5 SIP-Carrier / SIP Service Provider konfigurieren

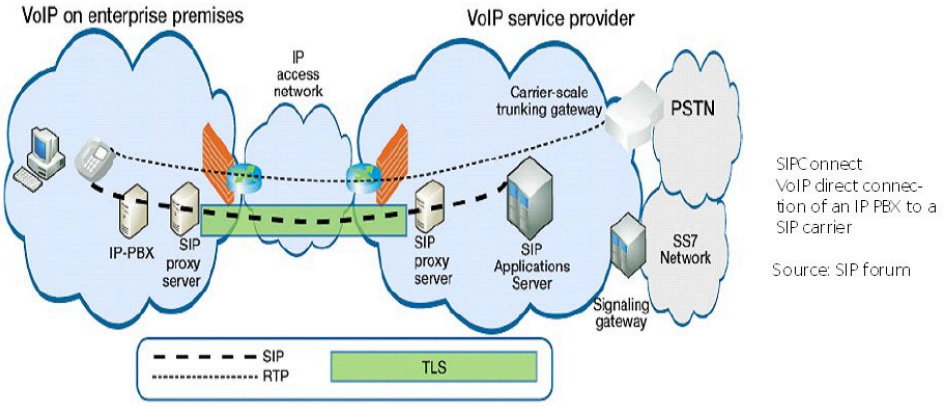
Wichtig: Eine aktuelle Liste zertifizierter SIP Provider finden Sie im G-DMS-Dokument INF-13-000534.

Anmerkung: Falls Sie einen Austausch von Hardware erwägen, lesen Sie Kapitel 3, „Baugruppentausch“

14.5.1 Motivation

Derzeit bieten fast alle Carrier einen direkten, IP-basierten Netzübergang an, an dem das Session Initiation Protocol (SIP) als Verbindungs- und Kommunikationsprotokoll zwischen IP-PBX und SIP-Carrier-Anschluss eingesetzt wird. IP-basierte Netzübergänge können dabei an Stelle oder als Ergänzung zu den existierenden ISDN-Anlagenanschlüssen genutzt werden.

In der folgenden Grafik ist ein Beispiel für einen solchen Netzübergang gezeigt:



SIPConnect Referenzarchitektur

Native SIP ermöglicht die IP-basierte, direkte Verbindung zwischen einem OpenScape 4000-System und einem SIP-Provider. In einem OpenScape 4000-System kann zusätzlich zu den herkömmlichen ISDN-Verbindungen natürlich auch die SIP-Provider-Verbindung konfiguriert werden.

14.5.2 Grundlegendes zur Konfiguration

14.5.2.1 Konfiguration

Das Leistungsmerkmal wird je nach Ausgangssituation in zwei bzw. drei Schritten konfiguriert.

- Ohne Session Border Controller
- Bei der direkten Variante ohne Session Border Controller wird das Leistungsmerkmal über AMOs und über das WBM konfiguriert. In diesem Falle erhält die (v)HG 3500 eine IP-Adresse aus dem WAN. Diese IP-Adresse wird vom Service-Provider fest vergeben.
- Mit Session Border Controller
- Soll ein Session Border Controller verwendet werden, so muss dieser noch zusätzlich konfiguriert werden. Dann hat die (v)HG 3500 eine IP-Adresse im Kunden-LAN, während der Session Border Controller über zwei IP-Adressen verfügt - eine aus dem Kunden-LAN, die andere aus dem WAN des Service-Providers. Der Session Border Controller arbeitet somit als Router für die (v)HG 3500 in das WAN.
- DNS
- Da man es hier mit Internet-Telefonie zu tun hat, und das Internet namensorientiert arbeitet, empfiehlt es sich immer, DNS zu verwenden.

14.5.2.2 Hinweise

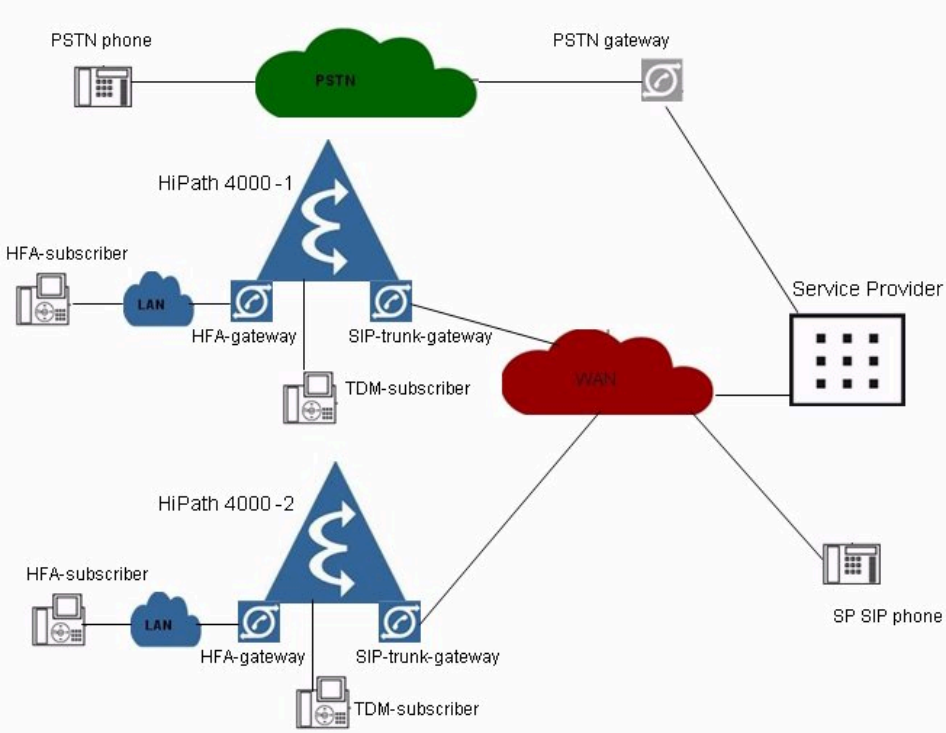
- OpenScape 4000 SoftGate
- Im folgenden Beispiel wird eine HG 3500 als SIP-Trunking-Gateway verwendet. Es kann auch eine virtuelle HG 3500 in einem OpenScape 4000 SoftGate als SIP-Trunking Gateway verwendet werden. Dann muss der AMO-Stapel hinsichtlich der Sachnummer (AMO BCSU) und dem Gerätetyp (AMO TDCSU) angepasst werden.
- Leistungsmerkmale des SIP-Carriers
- In diesem Anwendungsbeispiel geht es nur um die Anbindung an den SIP-Carrier. Welche Leistungsmerkmale über den jeweiligen SIP-Carrier möglich sind, wird vom Service Techniker mittels eines standardisierten Testplans mit Unterstützung der Systementwicklung geprüft.

14.5.3 Szenario 1: Gateway direkt an SIP-Carrier

14.5.3.1 Ausgangssituation

Wichtigste Parameter:

Endpoint/Beschreibung	DN-Name/Telefonnummer	IP-Adresse
SIP-Register/Proxy	sip.iandc.training.com	2.3.3.124
DNS - Service-Provider	iandc.training.com (Domainname)	2.3.3.123
RNR Carrier-Anschluss / HG 3500-1	+49180130100	3.3.3.11
RNR Carrier-Anschluss / HG 3500-2	+49180130200	3.3.3.22



HG 3500 direkt an SIP-Carrier

Nachfolgend soll der folgende Fall konfiguriert werden. Die HG 3500 der OpenScape 4000-1 soll als Native-SIP-Gateway eingerichtet werden und sich beim Service-Provider registrieren. Die Registrierung soll unter der Rufnummer des SIP-Anlagenanschlusses erfolgen (+49180130100).

An dem Service-Provider hat sich noch eine OpenScape 4000-2 eines anderen Kunden registriert. Diese hat die Anlagenrufnummer +49180130200 und einen vierstelligen Nebenstellenbereich. Diese Anlage soll in diesem Beispiel Ziel der Wahl für den Knoten OpenScape 4000-1. Es wird hier also nicht jede Rufnummer über den SIP-Carrier-Anschluss geroutet, sondern nur eine bestimmte.

Es wird nur auf die Einrichtung in der Anlage OpenScape 4000-1 eingegangen. Die Konfiguration der Anlage OpenScape 4000-2 ist nahezu identisch. Deshalb wird darauf verzichtet.

14.5.3.2 AMO-Konfiguration

14.5.3.2.1 Konfiguration mit ISDN-Rufnummernplan (empfohlen)

Für die Einrichtung von SIP-Rufnummern wird die Verwendung des internationalen ISDN-Rufnummernformats als einfachste Methode empfohlen. Bei Verwendung dieses Formats wird den SIP-Rufrufnummern automatisch ein + vorangestellt. Die Notation mit einem + ist auch das bevorzugte Format für den Rufnummernempfang von beliebigen SIP-Providern.

In AMO BFDAT muss ein Funktionsblock für HG 3550 voreingestellt werden:

```
EINRICHTEN-
BFDAT:FCTBLK=3,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;
```

```
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=HG3550,ANZSATZ=2,ANZEINH=3;

AENDERN-BFDAT:CONFIG=OK,FCTBLK=3,ANTW=JA;
```

HG 3550 wird dann mit Function-ID 1 und obigen Funktionsblock 3 eingerichtet:

```
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=10,SACHNR=âQ2324-
X500â, FCTID=1,LW►
VAR=â0â,FCTBLK=3,BKAN3550=60,ALARMNR=0;
```

Im AMO CGWB wird die IP-Adresse der HG 3550 eingetragen. In diesem Fall ist es eine Adresse aus dem WAN, die vom Service-Provider vergeben wird. Der DNS, dessen Adresse als DNSIPADR hier ebenso eingetragen wird, befindet sich ebenso im Bereich des Service-Providers:

```
EINRICHTEN-CGWB:LTU=1,EBT=10,SMODE=NORMAL,IPADR=3.3.3.11,
 NET►
MASK=255.255.255.0,BITRATE=âAUTONEGâ,TRPRSIP=60,DNSIPADR=2.3.3.123;
```

Im AMO CGWB, Abschnitt LEGKDATA, wird die Nummer des Gateways eingetragen (GWNR):

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=LEGKDATA,GWNR=1,REGEXTGK=NEIN;
```

Im AMO CGWB bleibt die externe Registrierung und die Digest-Authentifizierung ausgeschaltet:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=SIPTRERH,GWAUTREQ=NEIN;

AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=SIPTRSSA,SIPREQ=NEIN;
```

Man kann nun ein Bundle für die SIP-Carrier-Anwendung einrichten:

```
EINRICHTEN-BUEND:BUNUM=55,NAME=âSIP CARRIERâ,ANZ=60;
```

Die folgenden COT/COP-Klassen sind empfohlen:

```
EINRICHTEN-
COT:COTNO=55,PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&NOFT&NTON;
EINRICHTEN-COP:COPNO=55,TOLL=TA,TRK=TA;
EINRICHTEN-
TDCSU:ART=NEU,LAGE=1-01-010-0,COTNR=55,COPNR=55,WABE=0,VBZ=0,
COS=1,LCOSS=1,LCOSD=1,SATZNR=âSIP CARRIER
 ",ZLNR=0,PROTVAR=âECMAV2â, SEG►
MENT=8,TREFTYP=AMT,ISDNIP=00,ISDNNP=0,TRACOUNT=31,SATCOUNT=VIELE,
 KNNR=1-40-
155,ALARMNR=2,FIDX=1,COTX=55,AULX=1,UUSCCX=16,UUSCCY=8,FNIDX=1,
 CLASSM►
RK=EC&G711&G729AOPT,BUNR=55,SUCHART=AB,INBETR=J,SECLEVEL=TRADITIO,
 GER=HG3550►
CO,BKANAL=1&&30,BKVER=N,BKGR=1,LWPAR=0;
```

Falls mehr als 30 B-Kanäle benötigt werden, kann der Satz 1-1-10-1 identisch eingerichtet werden.

Für das LCR wird ein RICHT benötigt:

```
EINRICHTEN-
RICHT:ART=LRTGNEU,LRTG=55,LDIENST=ALLE,BUNUM=55,ZKNNR=1-40-155;
```

Des Weiteren braucht man eine Wahlregel:

```
EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=4;
```

```
EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=5;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=6;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=7;

EINRICHTEN-LODR:LWR=56,LWREL=NPI,NPI=ISDN,TON=INTERNAT;

EINRICHTEN-LODR:LWR=56,LWREL=ENDE;
```

und einen LDAT.

```
EINRICHTEN-
LDAT:LROUTE=55,LAUTH=1,LSVC=ALL,LVAL=1,TGRP=55,ODR=56;
```

Im Rufnummernplan wird ein Wählmuster nach Vorgabe eingerichtet, das über den SIP-Carrier-Anschluss geführt werden soll.

```
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=â0â-âWâ-
â00â-â49â-â1801â-â30200â-
âXXXXâ,LRTG=55,LBER=1;
```

Anmerkung: SIP-Provider erwarten alle Ziffern in Blockwahl und unterstützen keine Überlappungswahl. Alternativ zu -X können Sie in LDPLN auch -Z mit entsprechendem Timeout verwenden (LCRWE in AMO CTIME Zweig CPTIME1) verwenden.

Der folgende GKREG-Eintrag ist nicht notwendig und dient nur der Vollständigkeit, da der LEGK die Adressauflösung nicht vornimmt:

```
EINRICHTEN-
GKREG:GWNR=1,GWATTR=INTGW&HG3550V2&SIP,WAPLNUM=0,WABE=0,LBER=1;
```

Der KNDEF-Eintrag dient zum Herauskürzen des Anlagenanteils aus der kommenden Rufnummer:

EINRICHTEN-
KNDEF:KNNR=1-40-155,TYP=EIGEN,ISDNCC=49,ISDNAC=1801,ISDNLC=30100,ISDN

14.5.3.2.2 Konfiguration mit unbekanntem Rufnummernplan

In AMO BFDAT muss ein Funktionsblock für HG 3550 voreingestellt werden:

```
EINRICHTEN-
BFDAT:FCTBLK=3,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;

AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=3,FUNCTION=HG3550,ANZSATZ=2,ANZEINH=3;

AENDERN-BFDAT:CONFIG=OK,FCTBLK=3,ANTW=JA;
```

HG 3550 wird dann mit Function-ID 1 und obigen Funktionsblock 3 eingerichtet:

```
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=10,SACHNR=âQ2324-
X500â, FCTID=1,LW►
VAR=â0â,FCTBLK=3,BKAN3550=60,ALARMNR=0;
```

Im AMO CGWB wird die IP-Adresse der HG 3550 eingetragen. In diesem Fall ist es eine Adresse aus dem WAN, die vom Service-Provider vergeben wird. Der DNS, dessen Adresse als DNSIPADR hier ebenso eingetragen wird, befindet sich ebenso im Bereich des Service-Providers:

```
EINRICHTEN-CGWB:LTU=1,EBT=10,SMODE=NORMAL,IPADR=3.3.3.11,
 NET►
```

```
MASK=255.255.255.0,BITRATE=âAUTONEGâ,TRPRSIP=60,DNSIPADR=2.3.3.123;
```

Im AMO CGWB, Abschnitt LEGKDATA, wird die Nummer des Gateways eingetragen (GWNR):

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=LEGKDATA,GWNR=1,REGEXTGK=NEIN;
```

Im AMO CGWB bleibt die externe Registrierung und die Digest-Authentifizierung ausgeschaltet:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=SIPTRERH,GWAUTREQ=NEIN;

AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=10,TYP=SIPTRSSA,SIPREQ=NEIN;
```

Man kann nun ein Bundle für die SIP-Carrier-Anwendung einrichten:

```
EINRICHTEN-BUEND:BUNUM=55,NAME=âSIP CARRIERâ,ANZ=60;
```

Die folgenden COT/COP-Klassen sind empfohlen:

```
ADD-
COT:COTNO=55,PAR=ANS&CEBC&BSHT&BLOC&LWNC&NLCR&TSCS&LINC&NOFT&NTON;
ADD-COP:COPNO=55,PAR=IMEX,TOLL=TA,TRK=TA;
```

Dann kann der AMO TDCSU eingerichtet werden. Die Parameter ISDNIP und ISDNNP sind verknüpft mit dem Parameter IMEX. Dadurch kann eine implizite Rufnummer in eine explizite Rufnummer gewandelt werden. In diesem Fall ist es so konfiguriert, dass eine ankommende Rufnummer im Format UNKNOWN in eine ISDN INTERNATIONAL Rufnummer transformiert wird, wenn sie mit zwei Nullen beginnt (ISDNIP=00). Beginnt die kommende Nummer mit nur einer Null, wird sie in ISDN NATIONAL umgewandelt (ISDNNP=0):

```
ADD-TDCSU:OPT=NEW,PEN=1-20-010-
0,COTNO=55,COPNO=55,DPLN=0,COS=1,LCOSV=6,LCOSD=1,CCT="SIP_CARRIER",DES
VAR=ECMAV2,SEGMENT=8,ATNTYP=CO,ISDNIP=00,ISDNNP=0,TRACOUNT=31,SATCOUNT
NY,NNO=1-40-
155,FIDX=1,COTX=55,FWDX=1,UUSCCX=16,UUSCCY=8,FNIDX=1,CLASSMRK=EC&G711&
GRP=55,SRCHMODE=DSC,INS=Y,SECLEVEL=TRADITIO,DEV=HG3550CO,BCHAN=1&&20,P
GR=1,LWPAR=0;
```

Falls mehr als 30 B-Kanäle benötigt werden, kann der Satz 1-1-10-1 identisch eingerichtet werden.

Für das LCR wird ein RICHT benötigt:

```
EINRICHTEN-
RICHT:ART=LRTGNEU,LRTG=55,LDIENST=ALLE,BUNUM=55,ZKNNR=1-40-155;
```

Des Weiteren braucht man eine Wahlregel:

```
EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=3;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=4;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=5;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=6;

EINRICHTEN-LODR:LWR=56,LWREL=ECHOFELD,FELD=7;

EINRICHTEN-LODR:LWR=56,LWREL=NPI,NPI=UNKNOWN,TON=UNKNOWN;

EINRICHTEN-LODR:LWR=56,LWREL=ENDE;
```

und einen LDAT.

```
EINRICHTEN-
LDAT:LROUTE=55,LAUTH=1,LSVC=ALL,LVAL=1,TGRP=55,ODR=56;
```

Im Rufnummernplan wird ein Wählmuster nach Vorgabe eingerichtet, das über den SIP-Carrier-Anschluss geführt werden soll.

```
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=â0â-âWâ-
â00â-â49â-â1801â-â30200â-
âXXXXâ,LRTG=55,LBER=1;
```

Der folgende GKREG-Eintrag ist nicht notwendig und dient nur der Vollständigkeit, da der LEGK die Adressauflösung nicht vornimmt:

```
EINRICHTEN-
GKREG:GWNR=1,GWATTR=INTGW&HG3550V2&SIP,WAPLNUM=0,WABE=0,LBER=1;
```

Der KNDEF-Eintrag dient zum Herauskürzen des Anlagenanteils aus der kommenden Rufnummer:

```
ADD-
KNDEF:NNO=1-40-155,TYPE=OWN,ISDNCC=49,ISDNAC=180,ISDNLC=130100,IS
```

14.5.3.3 Konfiguration im WBM des Gateways

Im WBM der HG 3500 findet man unter **Configuration**> **Voice Gateway** den Menüpunkt **SIP-Trunk-Profile**. Hier findet man u.a. vorgeleistete Profile zu freigegebenen Service-Providern. In unserem Fall einer Simulation verwenden wir ein allgemeines Profil mit Registrierung.

Unter diesem Profil (**NatTrkWithRegistration**) werden die folgenden Einstellungen konfiguriert:

- **Domain-Name**: vom Provider geliefert (hier: iandc.training.com).
- **IP-Adresse/Host-Name** vom Registrar: vom Provider geliefert (hier DNS-Name: sip.iandc.training.com).
- **IP-Adresse/Host-Name** vom Proxy: vom Provider geliefert (hier DNS-Name: sip.iandc.training.com).

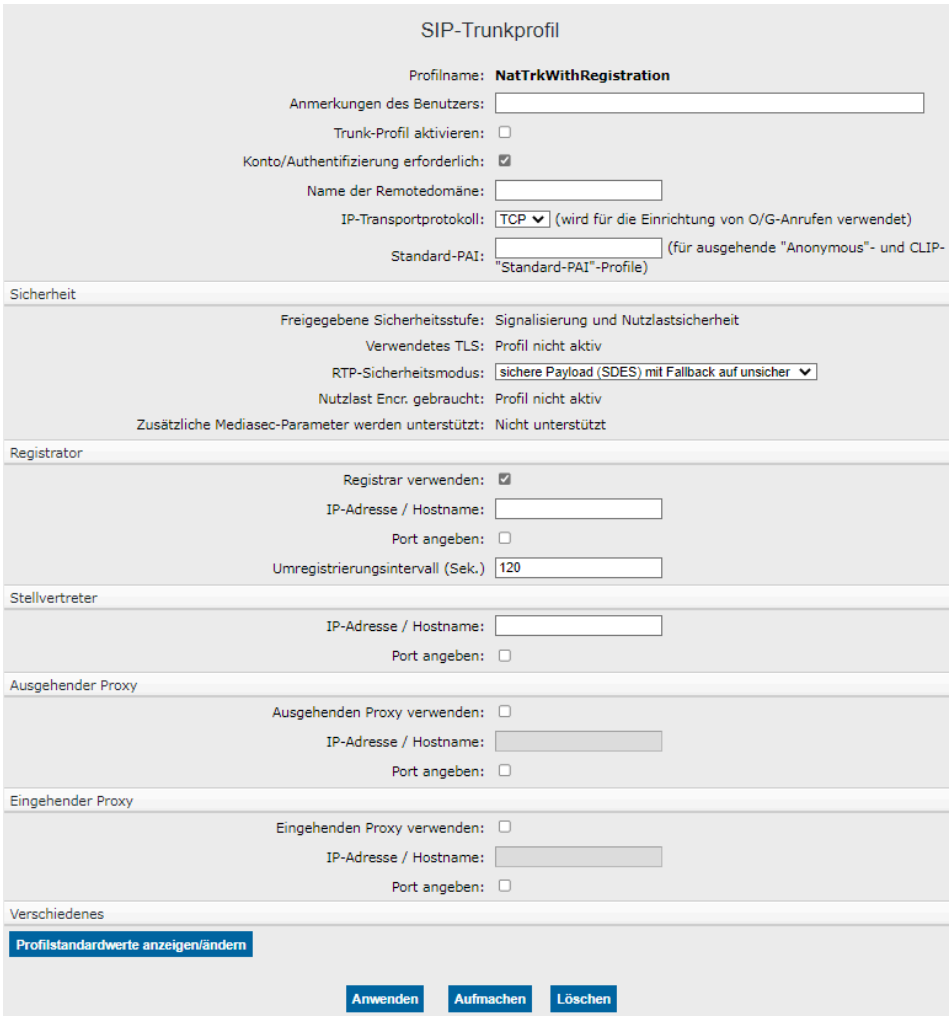


Abbildung 237: SIP Service Profile im HG 3500 WBM (Szenario 1)

Anschließend gibt man den **Account-Namen** an (Rechtsklick auf den Menüpunkt **NatTrkWithRegistration**). In diesem Beispiel registriert man sich unter der Anlagenrufnummer, die der Provider dem Anschluss zugewiesen hat.

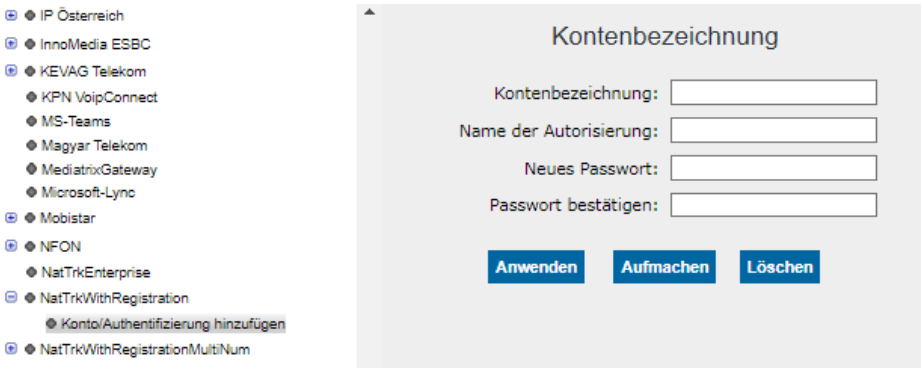


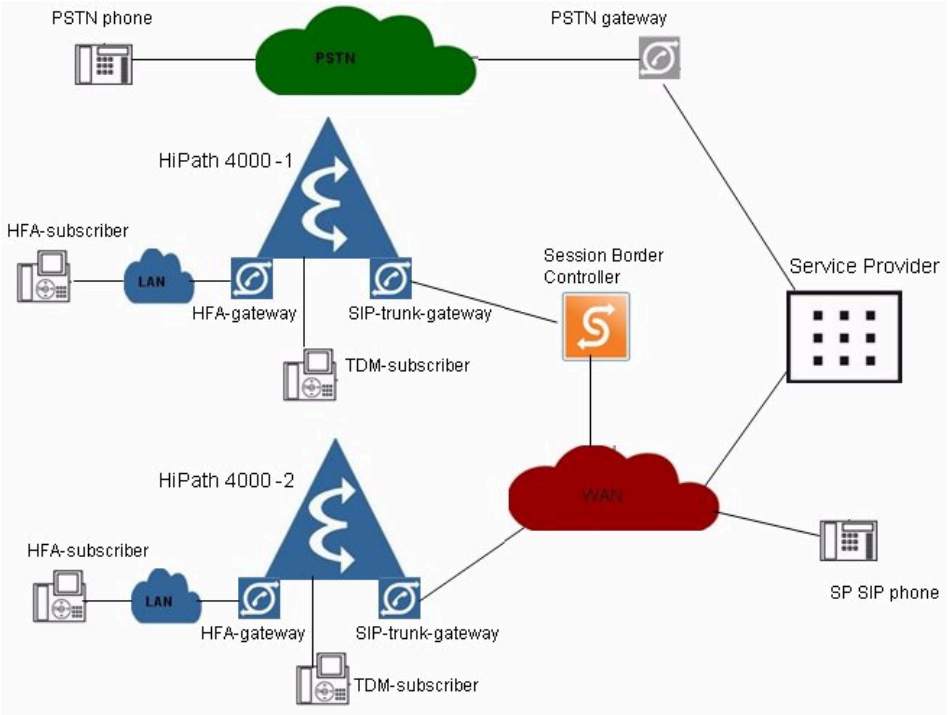
Abbildung 238: SIP Service Profile im HG 3500 WBM (Szenario 1)

14.5.4 Szenario 2: Gateway über Session Border Controller an SIP-Carrier

14.5.4.1 Ausgangssituation

Wichtigste Parameter:

Endpoint/Beschreibung	DN-Name/Telefonnummer	IP-Adresse
DNS - Service-Provider	iandc.training.com (Domainname)	2.3.3.123
SIP-Register/Proxy	sip.iandc.training.com	2.3.3.124
STNO-Betreiberanschluss / SBC-WAN-1	+49180130100	3.3.3.1
RNR Carrier-Anschluss / HG 3500-2	+49180130200	3.3.3.2
HG 3500 -1 (LAN)		1.40.11.82
SBC -1 (LAN)		1.40.11.89



HG 3500 über Session Border Controller an SIP-Carrier

In diesem Beispiel hat sich nun geändert, dass bei der Anlage OpenScape 4000 -1 nun ein Session Border Controller (SBC) zwischen SIP-Trunk-Gateway (HG 3500) und Service-Provider geschaltet ist. Das SIP-Trunk-Gateway wird nun mit einer IP-Adresse aus dem LAN des Kunden eingerichtet (1.40.11.82). Der Session Border Controller verfügt über zwei IP-Adressen, 1.40.11.89 im Kunden-LAN und 3.3.3.1 im Service-Provider-LAN.

Ein Session Border Controller wird beim Einsatz des OpenScape 4000 SoftGates empfohlen, um die Sicherheit zu erhöhen. Dazu verfügt er über Network Address Translation (NAT) und Firewall-Funktionalität.

Bei der AMO-Konfiguration im OpenScape 4000-1 ändert sich nur der HG 3500. Im HG 3500 WBM ist der Session Border Controller als Schnittstelle zum Service Provider (Outbound-Proxy) konfiguriert. Natürlich muss der Session Border Controller auch konfiguriert werden.

Das OpenScape 4000-1 System kann mit dem Ziffernmuster 0049180130100-xxxx vom OpenScape 4000-2 System aus aufgerufen werden.

14.5.4.2 AMO-Konfiguration

Die Konfiguration entspricht dem Szenario 1. Gateway direkt zum SIP-Carrier (Kapitel 5, „Szenario 1: Gateway direkt an SIP-Carrier“), außer CGWB AMO.

Im AMO CGWB wird die IP-Adresse der HG 3550 eingetragen. In diesem Fall handelt es sich um eine Adresse aus dem Kunden-LAN:

```
ADD-CGWB:LTU=1,SLOT=10,SMODE=NORMAL,IPADR=1.40.11.82,
 NETMASK=255.255.255.0,BI►
TRATE="AUTONEG",TRPRSIP=60,DNSIPADR=2.3.3.123;
```

14.5.4.3 HG 3500-Konfiguration in WBM

Die HG 3500-Konfiguration im WBM entspricht nahezu exakt dem Szenario 1: Gateway direkt zum SIP-Carrier. Geben Sie in einem geeigneten SIP-Trunkprofil (in diesem Fall: **NatTrkWithRegistration**):

- **Domain-Name**: vom Provider geliefert (hier: iandc.training.com).
- **IP-Adresse/Host-Name** vom Registrar: vom Provider geliefert (hier DNS-Name: sip.iandc.training.com).
- **IP-Adresse/Host-Name** vom Proxy: vom Provider geliefert (hier DNS-Name: sip.iandc.training.com).
- Outbound-Proxy: Unterschied zu Szenario 1! Hier wird das Häkchen unter **Outbound-Proxy verwenden** gesetzt und die IP-Adresse des Session Border Controller im LAN (**IP-Adresse/Host-Name**: 1.40.11.89) eingetragen. Alle Anrufe werden vom HG 3500 über OpenScape SBC an den SIP-Träger weitergeleitet. Das HG 3500 erlaubt auch nur eingehende Anrufe, die über OpenScape SBC geleitet werden.
- **Inbound-Proxy**: Hier nicht gesetzt! Man kann hier einen Proxy eintragen, der speziell für die kommende Richtung benutzt wird.

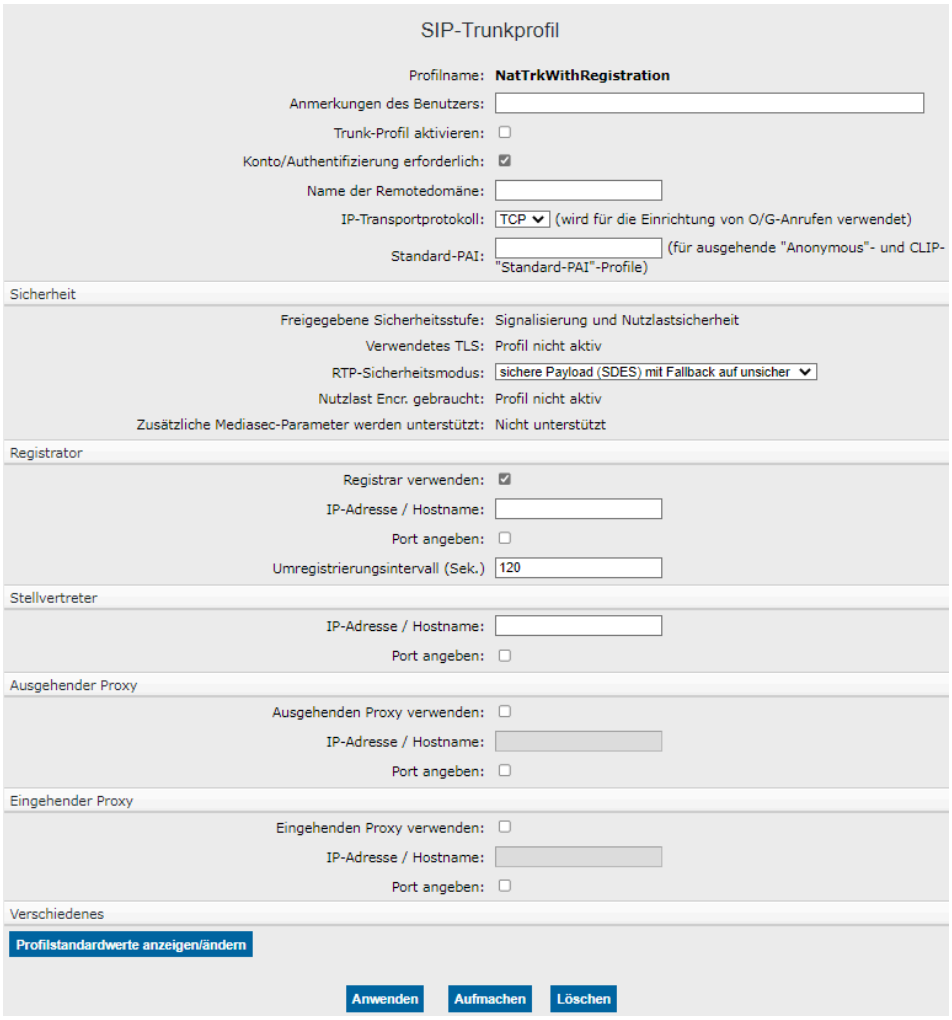


Abbildung 239: SIP-Dienstprofile im HG 3500 WBM (Szenario 2)

Wie in Szenario 1 können Sie mit der rechten Maustaste auf den *Profilnamen* in der Explorer-Leiste klicken, um dem Konto Registrierungsdaten hinzuzufügen. Der Registrierungsname ist in unserem Beispiel die Anlagenrufnummer.

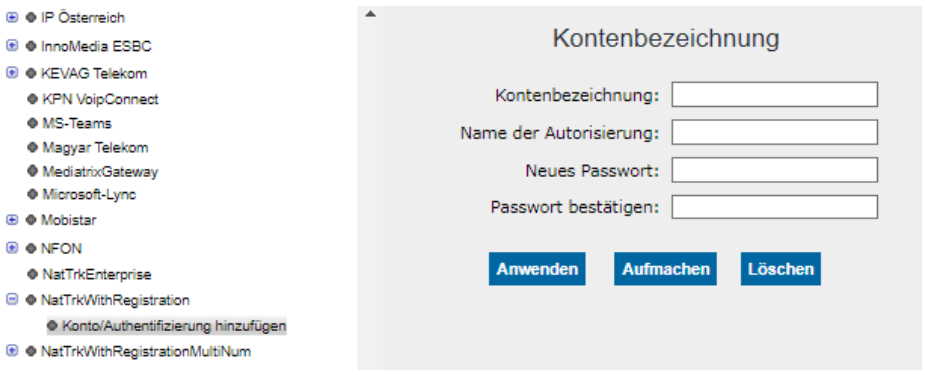


Abbildung 240: SIP-Dienstprofile im HG 3500 WBM (Szenario 2)

14.5.4.4 Konfiguration im Session Border Controller

Möglicherweise müssen Sie die folgenden Parameter im Session Border Controller konfigurieren:

- Zeiteinstellungen
- Externe IP-Adresse für die WAN-Schnittstelle (vom Service Provider vergeben)
- Interne IP-Adresse für die LAN1-Schnittstelle
- DNS
- Firewall-Einstellungen
- IP-Adresse des SIP Service Providers
- SIP-Einstellungen
- IP-Adresse des HG 3500 als Gateway konfigurieren

Bitte beachten Sie den entsprechenden SBC und verwenden Sie ihn.

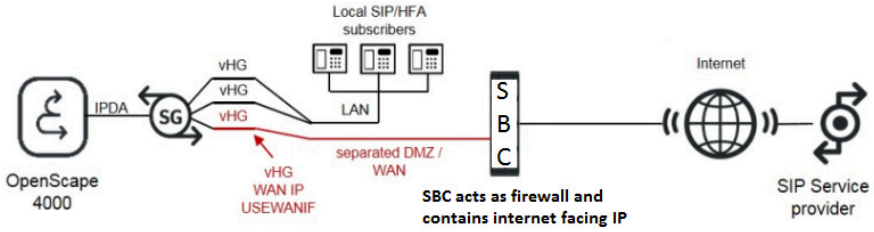
Wenn ein OpenScape SBC verwendet wird, lesen Sie bitte im OpenScape SBC Configuration Guide das Kapitel 3.6 über SBC mit OpenScape 4000 als SIP-Server

14.5.4.5 SG vHG direct connectivity (USEWANIF)

In some cases, the SSP provides its own SBC/Router and a dedicated interface and network address is preferred. This is done by activating USEWANIF in AMO CGWB.

The external SBC contains the Internet facing IP (and will often suffice instead for a firewall), thus no additional configuration is needed to standard SSP configuration.

SPE in the direction of SSP is controlled via TDCSU SECLEVEL. TLS signaling connection with payload encryption is possible if having the correct security certificates, profile configuration and SECLEVEL=SECURE.



14.5.5 SIP Provider: Telekom Deutschland GmbH DeutschlandLAN SIP-Trunk

Bei der Modernisierung der traditionellen TDM-Technologie auf IP-basierte Kommunikation bietet die Telekom Deutschland GmbH nun auch eine Umstellung der ISDN-TK-Anlagenanschlüsse auf SIP-Telefonie an. Diese Umwandlung (oft unter dem Pseudonym „ALL-IP“) beinhaltet den Austausch von ISDN-Multiplexern (S2M) / ISDN NTBA (S0) mit zertifizierten IP-Routern wie z. B. der Telekom. Diese Router stellen die Internetverbindung zwischen der

SIP-Trunking OpenScape 4000 und der Zentrale (CO) für ein- und ausgehende Verbindungen zur Verfügung.

Eine andere Möglichkeit besteht mit einem sogenannten "DeutschlandLAN SIP-Trunk Pure" der Telekom. Dies beinhaltet keinen Zugang (xDSL/FTTH) durch die Telekom und kann mit jeder Internetverbindung (bandbreitenabhängig) genutzt werden, bei der Telekom Sales für weitere Informationen kontaktiert werden sollte. Für eine garantierte Sprachqualität (Quality of Service) durch die Telekom ist ein DeutschlandLAN SIP-Trunk mit Zugangsdienst der Telekom erforderlich (z. B. xDSL, FTTH).

Für die OpenScape 4000-Perspektive bedeutet dies, dass die Verbindung von einer klassischen ISDN-Karte zu einer SIP-kompatiblen Karte sowohl in Bezug auf die Konfiguration des Boards als auch des LCR-Routings verlegt werden muss.

Auf der OpenScape 4000-Seite werden diese Änderungen mit bestehenden virtuellen HG-Boards (SoftGate) sowie den SIP-kompatiblen STMIX- und STMI-Boards unterstützt.

14.5.5.1 Serviceinformationen

Unterstützte OS4K-Gateways:

- SoftGate
- **STMIX**
- STMI (Nur TCP/UDP & RTP)

Unterstützte Verbindungen:

- Direkte Verbindung OS4K Gateway
- OS4K-Gateways, die über Hosted OpenScape SBC / OpenScape SBC verbunden sind

Die Telekom hat für ihre SIP-Trunks DeutschlandLAN und CompanyFlex eine Logik implementiert, die es ermöglicht, eine IP-PBX hinter einem zertifizierten Telekom-Router zu betreiben, obwohl IP Network Address Translation verwendet wird. Die Telekom prüft in ihrer Zentrale (Backend), ob die empfangenen SIP-Nachrichten ursprünglich aus einem privaten Netz (Klasse A, B oder C) stammen. Ist dies der Fall, wird die Kommunikation mit NAT-Traversal realisiert, welches die Payload-Streams auf Basis der empfangenen RTP-Pakete an die richtigen Ports sendet.

Im Gegensatz zu direkten SIP-Provider-Verbindungen ist diese Methode von Vorteil, da das OS4K-Gateway nicht mit einer dedizierten Public IP bedient werden darf. Das verwendete OS4k-Gateway ist daher im NAT-Szenario nicht direkt aus dem Internet erreichbar. Es genügt, das OS4K-Gateway in das lokale Netzwerk des zertifizierten Routers zu leiten. (Bildmäßige Darstellung siehe Abschnitt 5.5.4, „Verbindungsbeispiele“: Gateway (HG/vHG) im lokalen Netzwerk des Telekom-Routers (NAT-Szenario)).

Alle von der Telekom zertifizierten Business-Router (LANCOM, AudioCodes, etc.) beinhalten eine zustandsorientierte Firewall und/oder Netzwerkadressübersetzung. Diese Router durchlaufen nur Pakete von der WAN-Seite zum LAN, wenn der verwendete Port bereits eine ausgehende Verbindung zum WAN/Internet aufgebaut hat (und als aktiv gilt). Alles andere entfällt. Die verwendeten OS4K-Gateways sind daher „nicht im Internet“. Die Konnektivität kann mit einem gewöhnlichen Heim-PC hinter einem

handelsüblichen DSL-Router verglichen werden, bei dem eine permanente Portweiterleitung und offene Verbindung nicht erforderlich ist. Der verwendete Port auf der WAN-Schnittstelle wird vom Router zufällig unter Verwendung der Network Address Port Translation (NAPT) für die SIP-Kommunikation eingestellt. Abhängig vom verwendeten Router kann NAPT nur dann garantiert werden, wenn die SIP-Schnittstelle des OS4K mit Port 5060/5061 verwendet wird. Eine Änderung auf einen höheren Portbereich vom LAN auf die WAN-Schnittstelle des Routers kann nicht ausgeschlossen werden (normales NAT).

Darüber hinaus sind die OS4K-Gateways so konzipiert, dass sie jede SIP- und Mediensitzung am Gateway selbst beenden. Dennoch ist es in allen unterstützten Verbindungsszenarien möglich, einen Session Border Controller anzuschließen und/oder das Szenario in eine DMZ zu integrieren.

Verbindungsszenarien:

Direkte Verbindung OS4K Gateway:

- Gateway (HG/vHG) im lokalen Netzwerk des Telekom-Routers (NAT-Szenario)
- Gateway (HG/vHG) mit eigenem Internet/Public IP (WAN-Szenario)

OS4K-Gateways, die über Hosted OpenScape SBC / OpenScape SBC verbunden sind:

- Gateway (HG/vHG) über Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC im lokalen Netz des Telekom Routers (NAT-Szenario)
- Gateway (HG/vHG) über Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC mit eigenem Internet/Public IP (WAN-Szenario)

Weitere Informationen finden Sie im Kapitel Abschnitt 5.5.4, „Verbindungsbeispiele“

sowie unter

https://hilfe.companyflex.de/de/einrichtung/anschalteszenarien

Bitte auch hier entsprechende Hinweise zum Thema Notruf-Routing beachten.

14.5.5.2 Einschränkungen

Der DeutschlandLAN SIP Trunk Telekom unterstützt Verschlüsselung nur, wenn sowohl Signalisierung als auch Nutzlastverschlüsselung (TLS und SRTP) gemeinsam aktiv sind. Sollte eine davon unverschlüsselt gesendet werden, wird die Verbindung beendet.

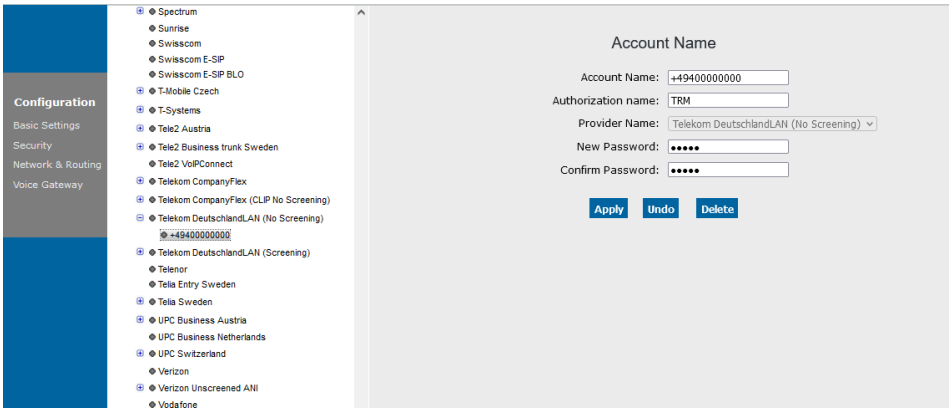
Seitens der Telekom wird für die Sprachverschlüsselung (SRTP) nur SDES unterstützt. Für die Konfiguration und die entsprechende Unterstützung von SDES siehe Unterkapitel „1.5. Session Description (SDES) Protocol“ unter „Signaling and Payload Encryption (SPE)“ von IP Solutions.

Der IPv6-Support befindet sich bei der Telekom noch in der Zertifizierungsphase.

14.5.5.3 Konfiguration

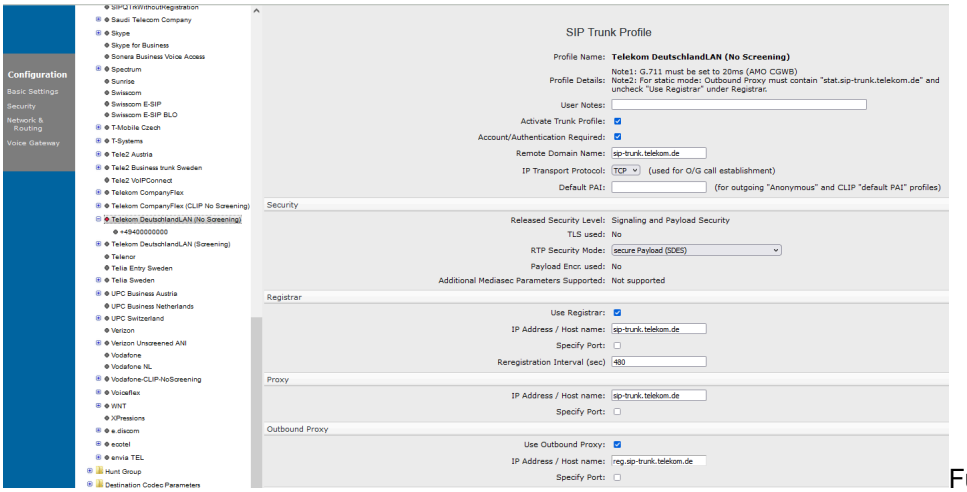
Die HG/vHG Loadware enthält SIP-Providerprofile für die Telekom SIP trunks „DeutschlandLAN“ und „CompanyFlex“. Nur diese Profile dürfen für die Konnektivität verwendet werden.

Die Profile erfordern eine korrekte Eingabe der Telekom-Kontoinformationen, z. B.: Account Konfiguration **DeutschlandLAN**:

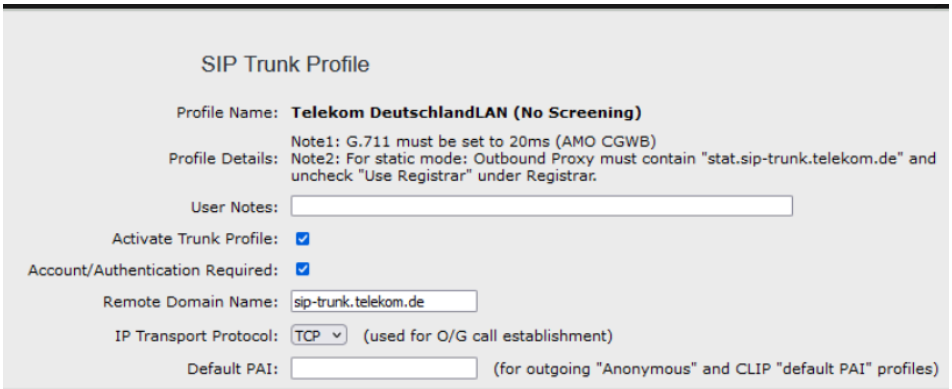


Wie herkömmliche SIP-Provider bietet die Telekom SIP trunk DeutschlandLAN zwei verschiedene Modi an: Registrierung und statischer Modus. Die Telekom bevorzugt den Standardmodus „Registrierung“. Der statische Modus kann bei Bedarf über den Telekom-Kundendienst aktiviert werden. The statische Modus wird mit CompanyFlex nicht mehr unterstützt.OpenScape 4000 verwendet standardmäßig auch den Registrierungsmodus in der Voreinstellung SIP Provider Profile (Outbound Proxy). Bei Bedarf kann dies manuell für den DeutschlandLAN geändert werden (Outbound Proxy: stat.sip-trunk.telekom.de).

Für **CompanyFlex** bestehen entsprechende eigene Profile:



Für CLIPnoScreening muss für CompanyFlex (sollte dies nicht über PUBNUM gelöst sein) ein eigenes Profil selektiert werden: **CompanyFlex** (**CLIP No Screening**) und eine Default PAI Call Nummer (z.B. Kopfnummer) konfiguriert werden.



Die PUBNUM Einträge im SDAT und ACSU müssen im Format ISDN INTERNAT gesetzt werden.

Aufgrund der Verwendung von Hostnamen und DNS-SRV muss das OS4K-Gateway mit einem erreichbaren DNS-Server ausgestattet sein. Der DNS-Server muss die Telekom-Adressen auflösen können. Die Konfiguration erfolgt über AMO CGWB.

Um das Kunden-LAN vom CompanyFlex/DeutschlandLAN Anschluss zu trennen, sollte der Provider über die eth1 angebunden werden. Die Build-in SBC Funktion der vSTMI ist dann automatisch aktiv. Im Zweig MANLANIF wird die Administrierbarkeit des WBM konfiguriert.

Beispiel für ein direkt verbundenes WAN-Szenario mit Public IP:

```
AB-CGWB:21,16,GLOBIF; H500:  AMO CGWB  GESTARTET
------------------------------------------------------------------------
   |
CGW BAUGRUPPEN
DATEN
|
 ------------------------------------------------------------------------
|
HG3550

|
 ------------------------------------------------------------------------
|  LTU = 21      EBT = 16     SMODE = NORMAL
 POOLNO: 0
|
 ------------------------------------------------------------------------

GLOBALE DATEN UND ETHERNET INTERFACE DATEN -
 KONFIGURIERBARE WERTE:
------------------------------------------------------------------------

IPADR     = 88 .217.251.213        TCPP   =       (4060)

NETMASK   = 255.255.255.240        VLAN   = NEIN  (NEIN)

DEFRT     = 88 .217.251.209        (0.0.0.0 = NICHT
 KONFIGURIERT)
BITRATE   =         (SIEHE OS)     VLANID = 0     (0)
```

```
MUSTER    = 213 (213)              TLSP      = 4061  (4061)

TRPRSIP   = 1   (0)                TRPRH323  = 0  (0)

TRPRSIPQ  = 0   (0)                TPRH323A  = 0   (0)
DNSIPADR  = 212.18 .0  .5          SIPTCPP   = 5060 (5060)

DNSIPADR2 = 212.18 .3  .5          SIPTLSP   = 5061 (5061)

USEWANIF  = JA  (NEIN)

WPUBIP    = 0  .0  .0 .0
GLOBALE DATEN - KONSTANTE WERTE:

--------------------------------

AMO INTERFACE VERSION: 0      OPMODE: 1   DATA_VALID: JA
```

Die OpenScape 4000-Standardwerte für RTP-Paketlänge und Dienstart für die Signalisierung (TOSSIGNL) müssen mit AMO CGWB in der Niederlassung ASC manuell geändert werden, um den Anforderungen der Telekom zu entsprechen. RTP für G711 muss auf 20 ms und TOSSIGNL auf 104 geändert werden. Die TOS-Nutzlast muss nicht geändert werden.

TIPP: Die QoS-Einstellungen werden von den Routern im Telekom-Portfolio für die WAN-Schnittstelle übernommen. An dieser Stelle ist die korrekte QoS-Kennzeichnung besonders wichtig, da hier der Engpass der Verbindung vorhanden ist.

Konfiguration:

```
EINRICHTEN-CGWB:LTU=[LTU],EBT=[EBT],SMODE=NORMAL,IPADR=[IP-
Adresse der HG im Netz des Routers],NETMASK=[Netzmaske];

AENDERN-
CGWB:MTYP=CGW,LTU=[LTU],EBT=[EBT],TYP=GLOBIF,DEFRT=[IP-
Adresse des Routers],TRPRSIP=[Anzahl Parallele
 Gespräche],DNSIPADR=[IP-Adresse des Routers],USEWANIF=JA;

AENDERN-
CGWB:MTYP=CGW,LTU=[LTU],EBT=[EBT],TYP=ASC,TOSPL=184,TOSSIGNL=192,
 AENDERN-
CGWB:MTYP=CGW,LTU=20,EBT=7,TYP=MANLANIF,MIPADR=[IP-
Adresse der HG im Netz des
 AP],MNETMASK=[Netzmaske],MDEFRT=[Default Router im Netz
 des AP];
```

Beispiel:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=21,SLOT=16,TYPE=ASC,TOSSIGNL=192,PRIO=PRIO1,
 RTP=20;
DIS-CGWB:21,16,ASC;
H500: AMO CGWB STARTED
-------------------------------------------------------------------

| CGW BOARD DATA
 -------------------------------------------------------------------
```

```
| HG3550 |
 ------------------------------------------------------------------------
| LTU = 21 SLOT = 16 SMODE = NORMAL POOLNO: 0 |
------------------------------------------------------------------------
ASC DATA - CONFIGURABLE VALUES:
---------------------------------
TOSPL = 184 (184) TOSSIGNL = 192 (104)
UDPPRTLO = 29100 (29100) UDPPRTHI = 30099 (30099)
T38FAX = YES (YES) REDRFCTN = YES (YES)
RFCFMOIP = NO (NO) RFCDTMF = YES (YES)
PRIO1 : CODEC = G711A VAD = NO RTP-SIZE = 20
```

Generell sollten Verbindungen zu SIP-Anbietern im internationalen Format erfolgen. Eine gewählte nationale Telefonnummer (z. B. Handy) muss im internationalen Format (NPI = ISDN, TON = INTERNAT) an den CO gesendet werden. Konfigurationsbeispiel:

International gewählte Nummern:

```
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"00"-"X"-"Z",LBER=[LBER];
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=NPI,NPI=ISDN,TON=INTERNAT;
```

National gewählte Nummern:

```
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"0"-"X"-"Z",LBER=[LBER];
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=ZIFFSEND,ZIFFERN=[Landesvorwahl des
 Anschlusses];
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=NPI,NPI=ISDN,TON=INTERNAT;
```

Siehe Sie Abschnitt 5.3.2.1, „Konfiguration mit ISDN-Rufnummernplan (empfohlen)“.

Im LCR müssen die Rufnummernsignalisierung im internationalen Format und die Erreichbarkeit der Sonderrufnummern sichergestellt sein. Im TDCSU sind geeignete COT und COP zu verwenden.

```
EINRICHTEN-COT:COTNU=[COT Nummer],
COTPAR=MVLT&UELM&SAAO&BLOC&LOKN&OLCR&TSCS&VKNN&OLRD&NOFT&KTON;
AENDERN-COP:COPNU=[COP
 Nummer],COPART=COPZU,COPPAR=T311,BERAMT=FBKW,BERFERN=FBKW;
```

Im Falle von CLIP No Scrrening muss der Parameter PDL2 noch zusätzlich gesetzt werden.

```
AENDERN-COT:COTNU=[COT Nummer],COTPAR=PDL2;
```

Beispiel für TDCSU:

```
EINRICHTEN-TDCSU:ART=NEU,LAGE=[EBT Nummer],COTNR=[COT
 Nummer],COPNR=[COP Nummer],
SATZNR="COMPANYFPDL‟LEX",PROTVAR=ECMAV2,SEGMENT=8,TRTBL=GDTR,AULX=5,
CLASSMRK=EC&G711&G729AOPT,BUNR=[BUEND
Nummer],SUCHART=AB,INBETR=J,SECLEVEL=SECURE,GER=HG3550CO,BKGR=1;
```

Ohne Vorwahl gewählte Nummern im Ort.

```
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"X"-"Z",LBER=[LBER];
EINRICHTEN-LODR:LWR=[LODR Nummer],LWREL=ZIFFSEND,
 ZIFFERN=[Landesvorwahl + Ortsvorwahl des Anschlusses];
```

```
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=NPI,NPI=ISDN,TON=INTERNAT;
```

Call-by-Call 010

```
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"010"-"Z",LBER=[LBER]
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=NPI,NPI=ISDN,TON=NATIONAL;
```

Im Falle von Telekom DeutschlandLAN SIP-Trunk und ComapnyFlex gibt es spezielle Tarifnummern mit Vorwahlen, die (nicht im E. 164-Format) an die Telekom geschickt werden müssen. Diese (neun) Sondertarifnummern/ Vorwahlcodes sind:

```
110, 112, 115, 116-X, 118-X, 010-X, 0137-X, 0138-X und
 0900-X
```

Beispiel für Sonderrufnummern:

```
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"11"-"0",LBER=[LBER];
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"11"-"2",LBER=[LBER];
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"11"-"5",LBER=[LBER];
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"116"-"Z",LBER=[LBER]
EINRICHTEN-
LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="0"-"W"-"118"-"Z",LBER=[LBER]
EINRICHTEN-LODR:LWR=[LODR
 Nummer],LWREL=NPI,NPI=ISDN,TON=SUBSCR;
```

Bitte auch hier entsprechende Hinweise zum Thema Notruf-Routing unter

https://hilfe.companyflex.de/de/einrichtung/anschalteszenarien

beachten.

Um Signalisierung und Nutzlastverschlüsselung (SPE) zu verwenden, ist eine Aktivierung im OS4K erforderlich. Bitte beachten Sie dazu das Kapitel aus der Servicedokumentation IP Solutions – Signaling and Payload Encryption (SPE).

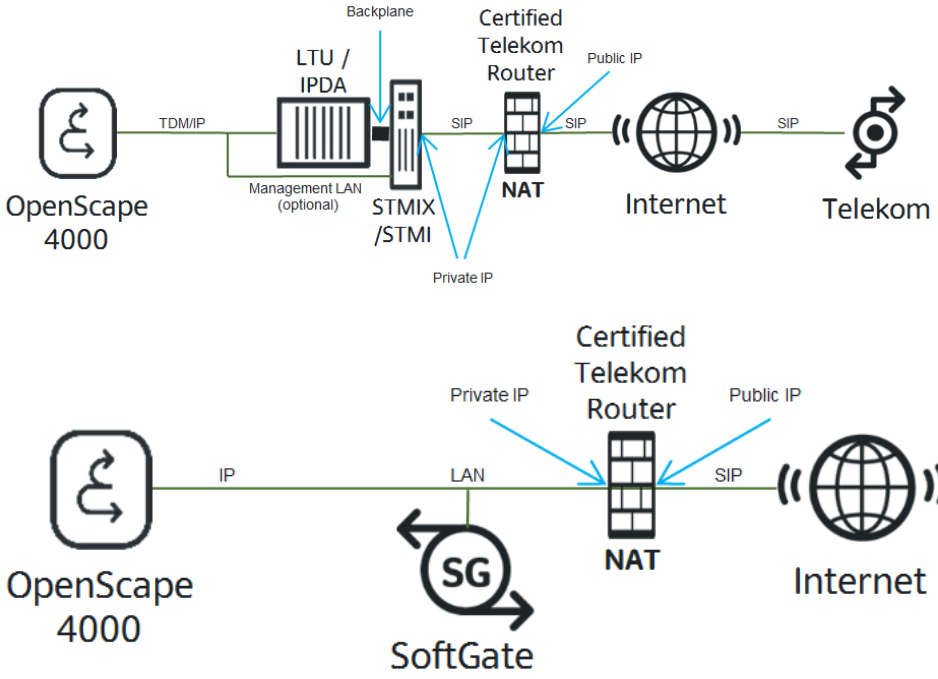
Für den SIP-Trunk stellt die Telekom eigene Zertifikate (CA) zur Verfügung. Die bereitgestellten Telekom CA-Zertifikate müssen auf dem OS4K Gateway importiert werden. Aufgrund des SPE-Designs im OS4K benötigt das OS4K-Gateway neben CA-Zertifikaten auch ein eigenes Server-Zertifikat (z. B. *.p12), um die Aktivierung von SPE (TLS) zu realisieren. Zu diesem Zweck kann jedes beliebige private Serverzertifikat erstellt werden, das dann in das OS4K-Gateway importiert werden muss. Die im Zertifikat des Servers eingegebenen Daten sind irrelevant.

Der Parameter LCRWE für die Blockwahl kann auf z.B. 5 Sekunden angepasst werden.

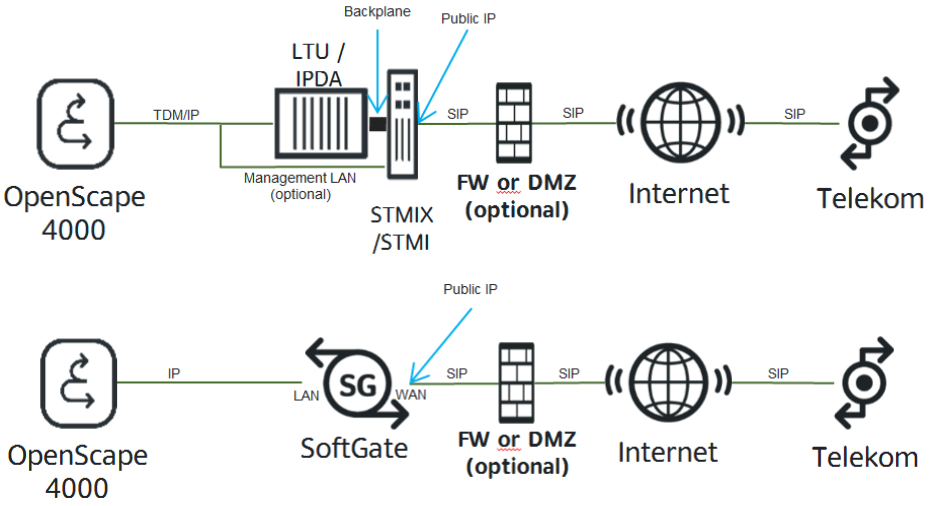
```
AENDERN-CTIME:ARTSWU=CPTIME1,LCRWE=5;
```

14.5.5.4 Verbindungsbeispiele

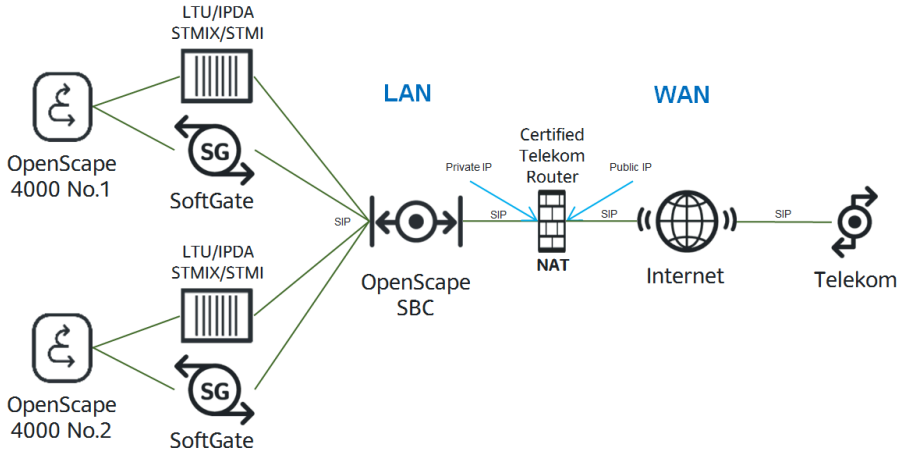
Gateway (HG/vHG) im lokalen Netzwerk des Telekom-Routers (NAT-Szenario):



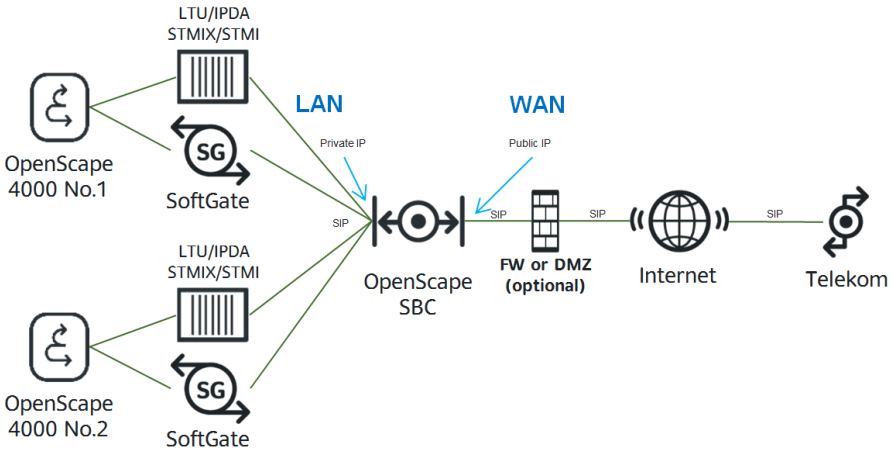
Gateway (HG/vHG) mit eigenem Internet/Public IP (WAN-Szenario):



Gateway (HG/vHG) über Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC im lokalen Netz des Telekom Routers (NAT-Szenario):



Gateway (HG/vHG) über Hosted OpenScape SBC (z. B. OpenScape 4000 Branch)/OpenScape SBC mit eigenem Internet/Public IP (WAN-Szenario):



14.5.5.5 Konfigurationsbeispiel OpenScape SBC

In diesem Kapitel wird eine exemplarische Konfiguration für den OpenScape SBC mit der Telekom Deutschland GmbH (TDG) – DeutschlandLAN SIP-Trunk beschrieben. In diesem Fall meldet sich der OpenScape SBC statt am OS4K-Gateway beim DeutschlandLAN SIP-Trunk an.

Weitere OpenScape SBC-Dokumentationen (z. B. Konfiguration des „Clustered Mode“ zur Verbindung mehrerer Gateways und/oder mehrerer OS4Ks) finden Sie im offiziellen OpenScape SBC-Konfigurationsleitfaden (z. B. OpenScape SBC, Konfigurationsleitfaden, Administratorendokumentation).

Die Konfigurationsdaten sind dem Telekom-Brief zu entnehmen:



ERLEBEN, WAS VERBINDET.

TELEKOM DEUTSCHLAND GMBH

Telekom Deutschland GmbH

Landgrabenweg 151
53227 Bonn

ZUGANGSDATEN

Vertraulich, bitte aufbewahren!

Datum	01. März 2016
Ortsvorwahl	0228
Durchwahlnr.	12345
Abfragestelle	0
Registrierungsrufnummer	+49 228 123450
Rufnummernblock	von 000 bis 299

Sehr geehrte Damen und Herren,

hier sind die Zugangsdaten für Ihren neuen Telekom Anschluss. Sie gelten ab dem Tag der Bereitstellung, das genaue Datum sehen Sie in Ihrer Auftragsbestätigung.

Wie Sie Ihren Anschluss in einfachen Schritten einrichten, erfahren Sie in der beiliegenden Inbetriebnahme-Anleitung. Verwenden Sie für die darin beschriebene Einrichtung folgende Zugangsdaten:

2 Internet-Zugang einrichten

Anschlusskennung:	002529106948
Zugangsnummer: (vormals T-Online Nummer)	5511295012345
Mitbenutzernummer:	0001
Persönliches Kennwort:	25170493

3 Telefonie einrichten

Telefonie-Benutzername:	5511295012345
Telefonie-Passwort:	Yni2Fi84
Outbound-Proxy:	reg.sip-trunk.telekom.de
Registrar:	sip-trunk.telekom.de

Ein Wort in Sachen Sicherheit.
Halten Sie Ihre persönlichen Zugangsdaten vor anderen Personen geheim. Bitte geben Sie bei Fragen hierzu immer nur die Zugangsnummer an.

Wenn Sie Fragen haben, rufen Sie uns einfach an. Sie erreichen uns **kostenfrei unter 0800 33 02524.**

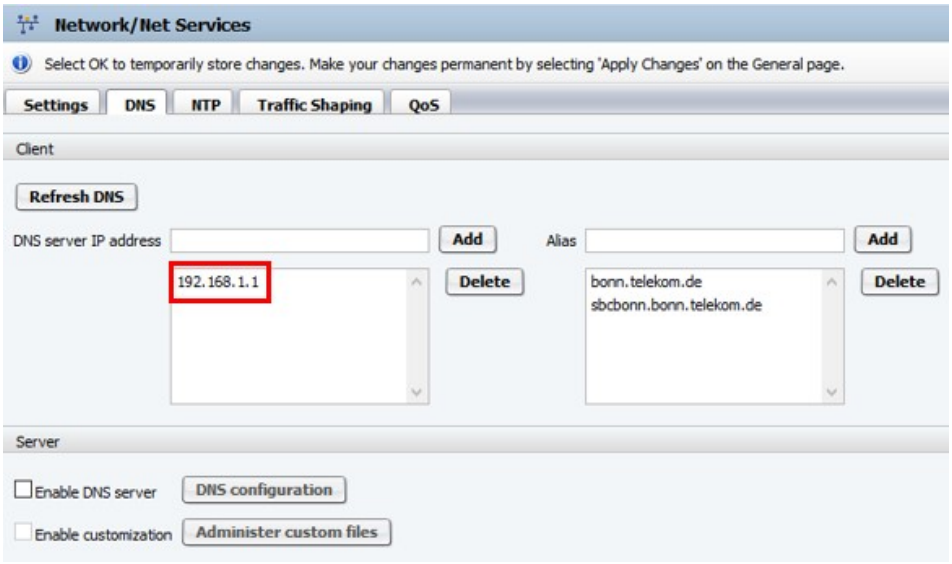
Freundliche Grüße
Ihre Telekom

TELEKOM DEUTSCHLAND GMBH, GESCHÄFTSKUNDENSERVICE

Deutsche Telekom-Brief

1. DNS

Es muss ein DNS-Server konfiguriert werden, der die in den Remote-Endpunkten konfigurierten Telekom-DNS-Einträge auflösen kann:



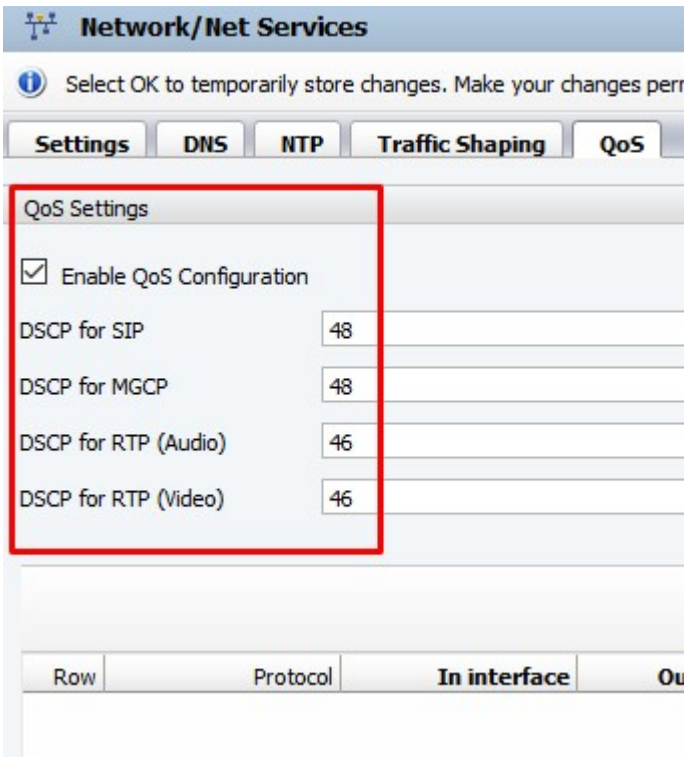
2. Quality of Service (QoS)

Die Telekom hat in ihrem Dokument 1TR114 QoS-Anforderungen festgelegt, die auf OpenScape SBC anzuwenden sind:

8.4.2 Traffic Classes in Layer 3

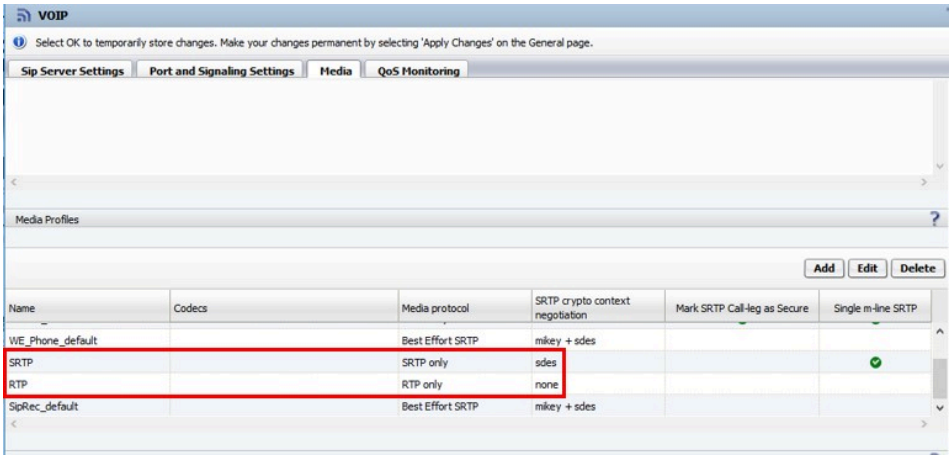
The UE uses the following traffic classes at Layer 3 (according to the Architecture of T-Home)

- Voice Control Class 6 (DSCP 110 000)
- Voice Bearer Class 5 (DSCP 101 110)

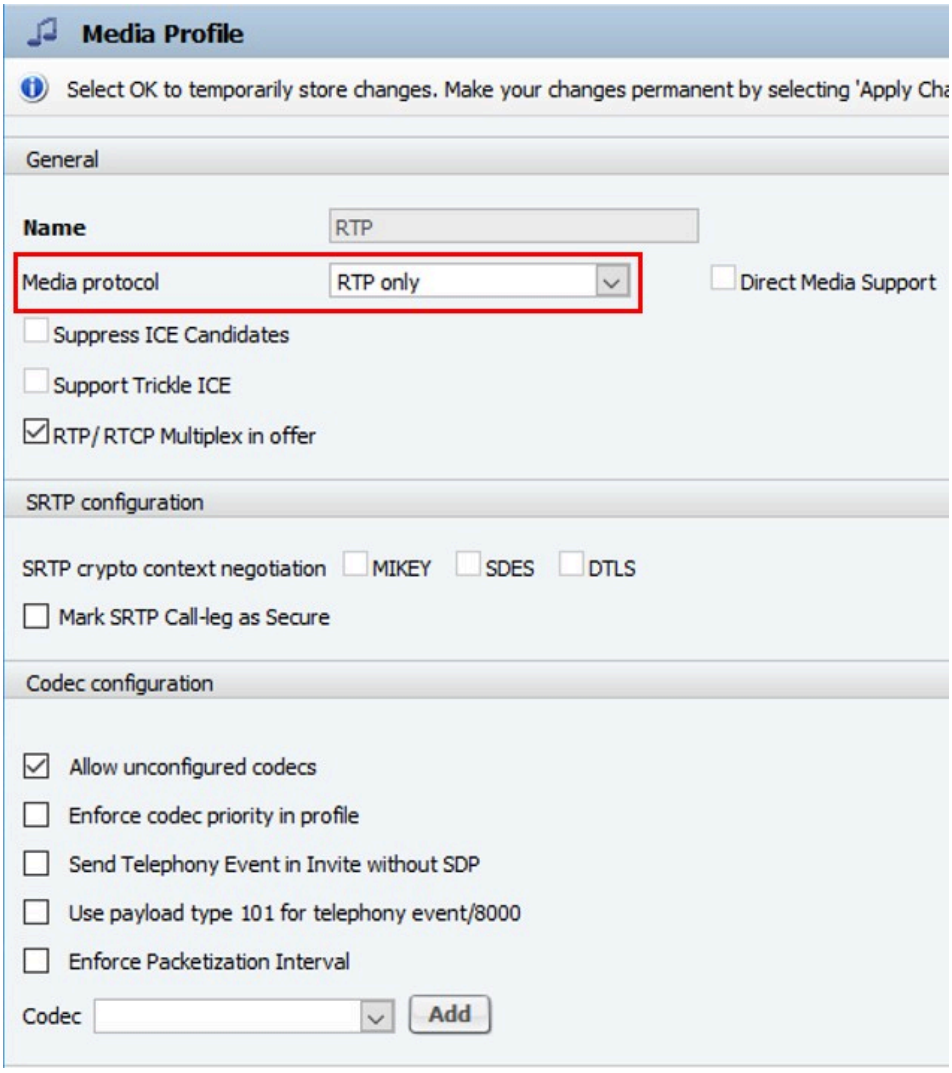


3. Medienprofil

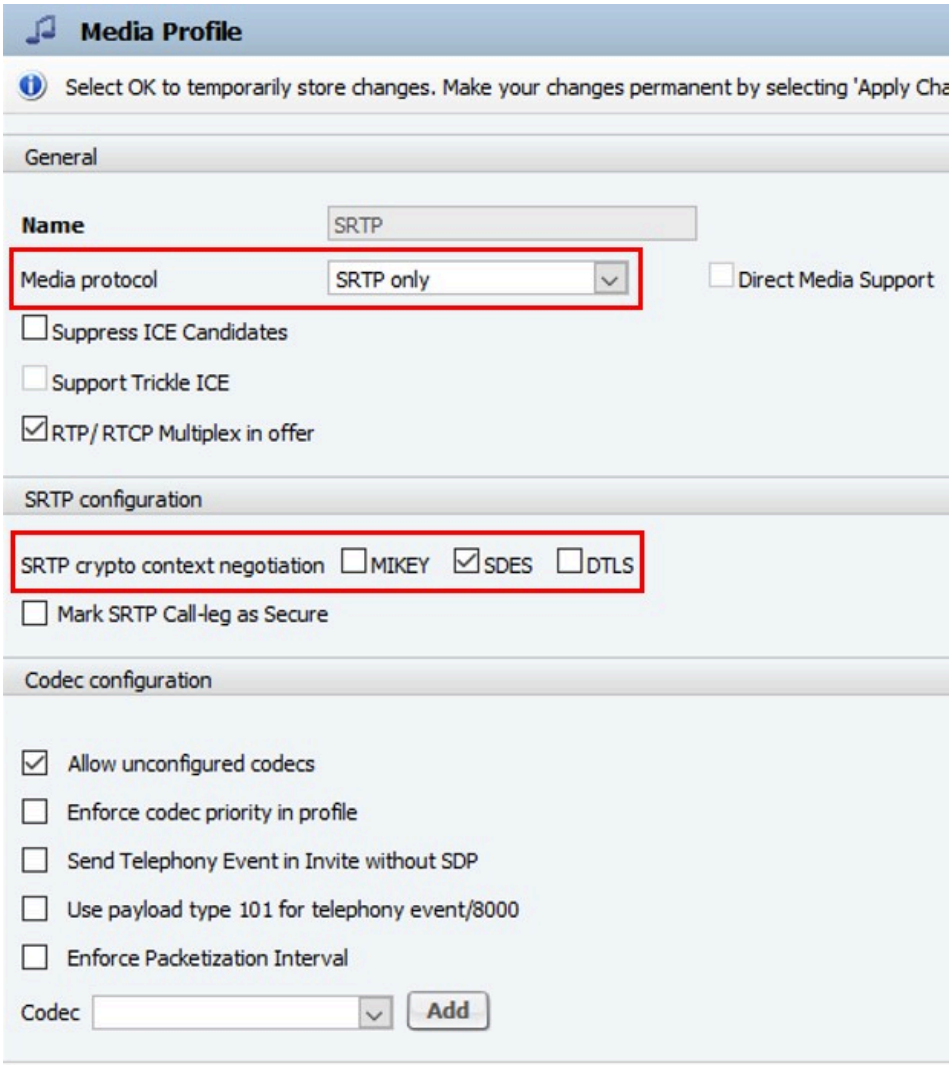
Je nachdem, ob der SIP-Trunk über TLS verschlüsselt ist oder nicht, muss eines der beiden exemplarischen Medienprofile im Screenshot verwendet werden:



Für einen unverschlüsselten SIP-Trunk wurde das Media Protocol RTP verwendet:



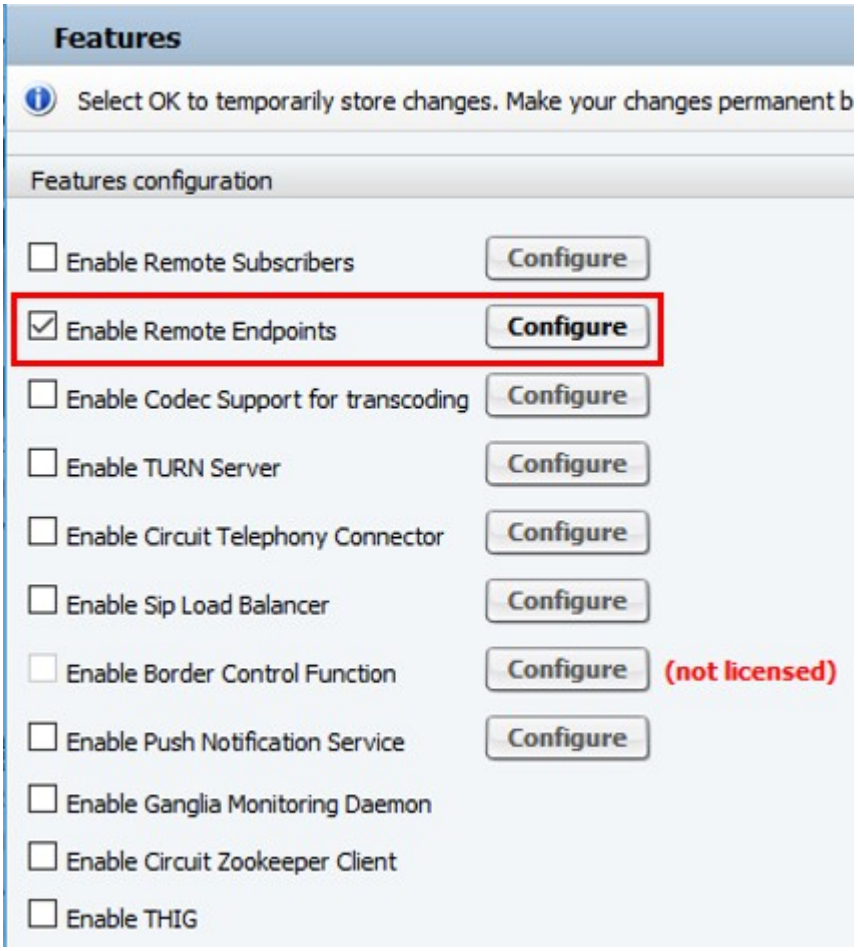
Für einen verschlüsselten SIP-Trunk wurde das Medienprotokoll SRTP und SDES zur Aushandlung der kryptographischen Parameter verwendet. MIKEY ist möglicherweise nicht aktiviert, da es nicht von der Telekom unterstützt wird.



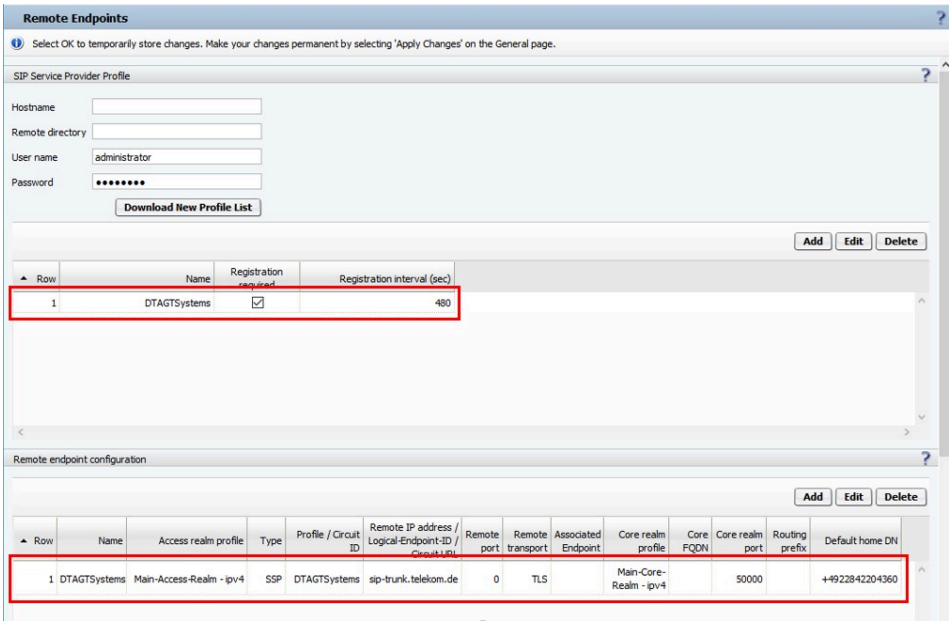
Wie Sie das definierte Medienprofil für den SIP-Trunk aktivieren, ist im Abschnitt Remote Endpoint weiter unten beschrieben.

4. Remote Endpunkt

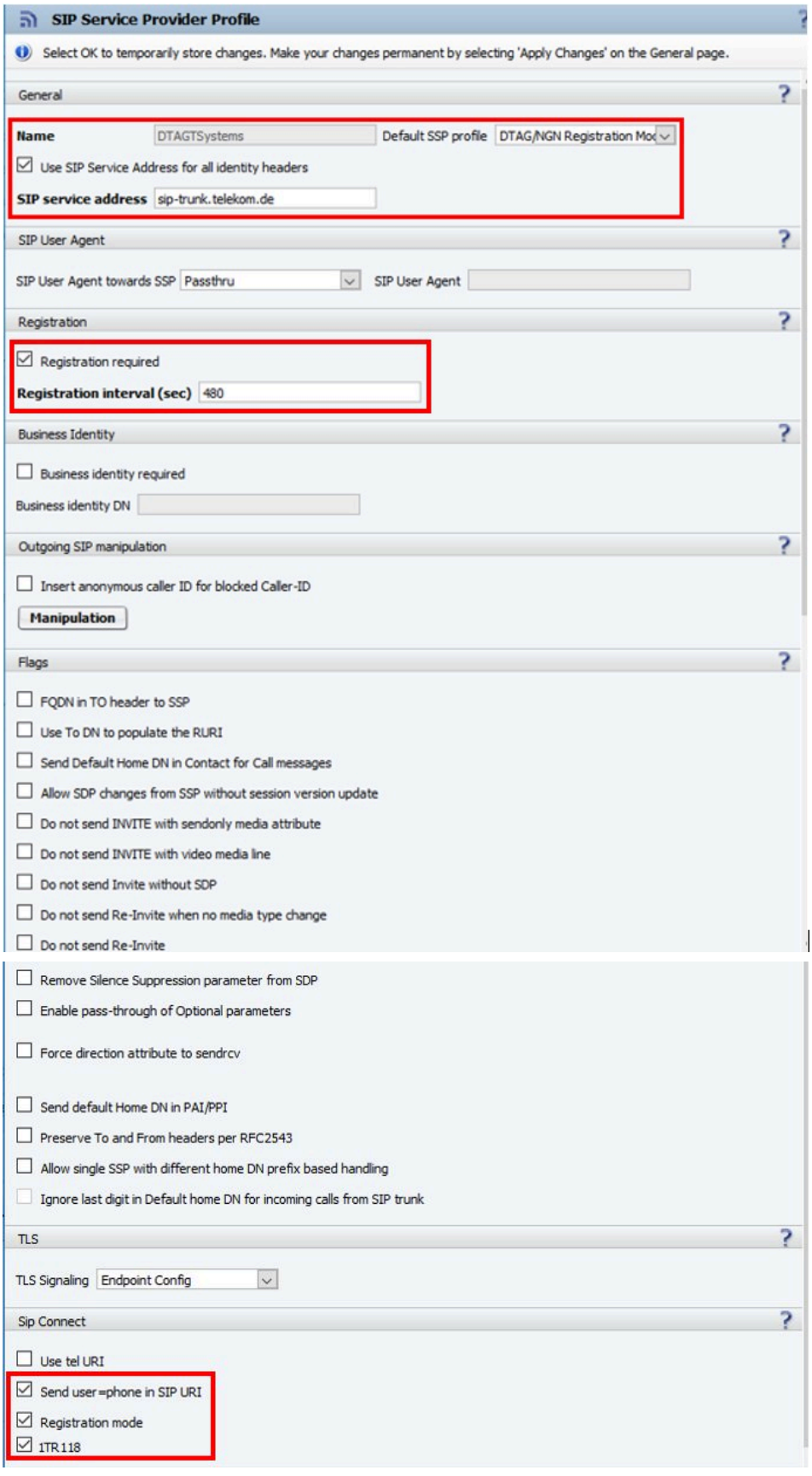
Auf dem OpenScape SBC muss Remote-Endpunkte aktivieren aktiviert sein:



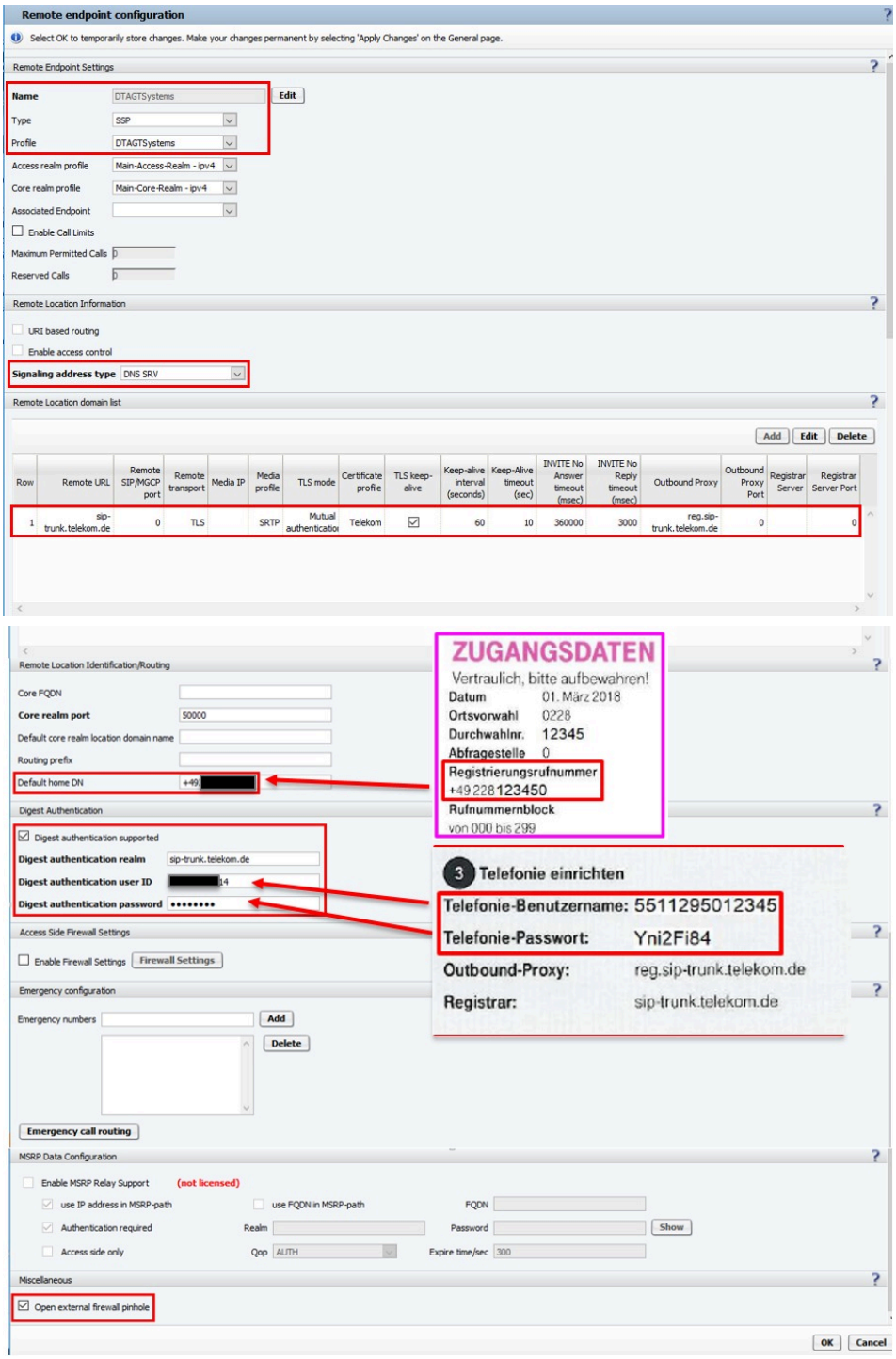
Beim Öffnen des Fensters Remote-Endpunkte müssen das SIP Service Provider Profil und der Remote-Endpunkt konfiguriert werden:



Im Fenster SIP Service Provider Profile muss als Standard-SSP-Profil DTAG/ NGN Registrierungsmodus ausgewählt werden. Das Registrierungsintervall muss auf 480 Sekunden eingestellt werden:

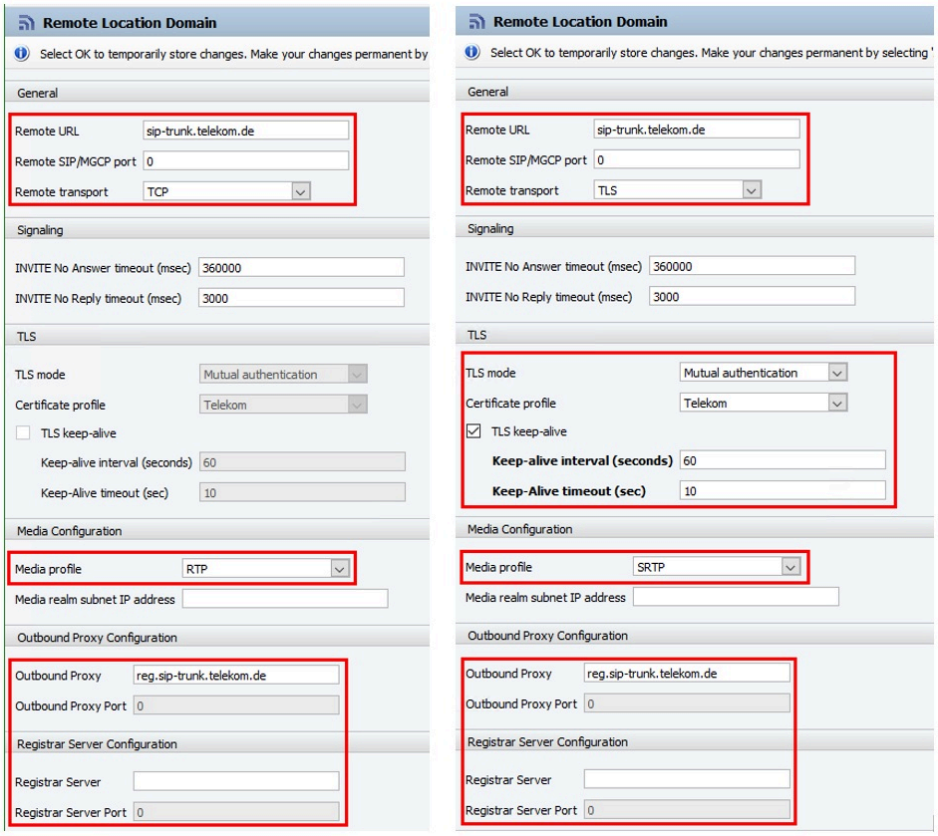

SIP Service Provider Profile
Select OK to temporarily store changes. Make your changes permanent by selecting 'Apply Changes' on the General page.
General
Name
DTAGTSystems
Default SSP profile
DTAG/NGN Registration Mo
Use SIP Service Address for all identity headers
SIP service address
sip-trunk.telekom.de
SIP User Agent
SIP User Agent towards SSP
Passthru
SIP User Agent
Registration
Registration required
Registration interval (sec)
480
Business Identity
Business identity required
Business identity DN
Outgoing SIP manipulation
Insert anonymous caller ID for blocked Caller-ID
Manipulation
Flags
FQDN in TO header to SSP
Use To DN to populate the RURI
Send Default Home DN in Contact for Call messages
Allow SDP changes from SSP without session version update
Do not send INVITE with sendonly media attribute
Do not send INVITE with video media line
Do not send Invite without SDP
Do not send Re-Invite when no media type change
Do not send Re-Invite
Remove Silence Suppression parameter from SDP
Enable pass-through of Optional parameters
Force direction attribute to sendrcv
Send default Home DN in PAI/PPI
Preserve To and From headers per RFC2543
Allow single SSP with different home DN prefix based handling
Ignore last digit in Default home DN for incoming calls from SIP trunk
TLS
TLS Signaling
Endpoint Config
Sip Connect
Use tel URI
Send user=phone in SIP URI
Registration mode
1TR118

Im Fenster Remote-Endpunkt-Konfiguration muss das oben gezeigte SIP Service Provider Profil ausgewählt werden:



Wenn sich ein NAT-Router zwischen SBC und SIP Trunk Open befindet, muss das externe Firewall-Pinhole aktiviert sein, damit OpenScape SBC den RTP-Port auf dem NAT-Router öffnet, indem es UDP-Pakete sendet, damit der NAT-Router RTP-Pakete von einem PSTN-Telefon aus weiterleiten kann.

Die folgenden Abbildungen zeigen das Fenster Remote Location Domain für einen unverschlüsselten SIP-Trunk mit TCP und RTP auf der linken Seite und für einen verschlüsselten SIP-Trunk mit TLS und SRTP auf der rechten Seite:

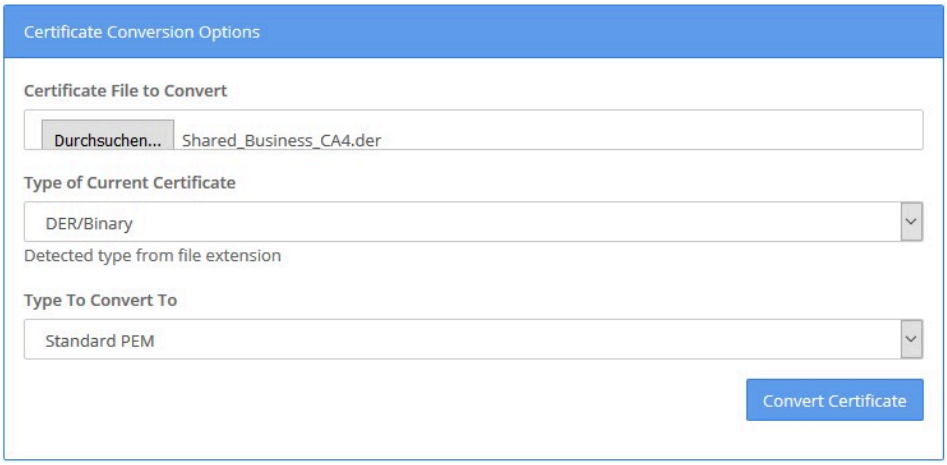


5. Vorbereitung und Installation von TLS-Zertifikaten

Für die Nutzung von TLS und SRTP über den SIP-Trunk ist das Hochladen und Konfigurieren der TLS-Zertifikate auf OpenScape SBC erforderlich:

- Laden Sie das Telekom *Deutsche Telekom Root CA 1*-Zertifikat dt-root-ca-1.cer herunter von der URL
- https://www.telesec.de/de/public-key-infrastruktur/support/root-zertifikate/category/57-deutsche-telekom-root-ca-1
- Laden Sie das Telekom Zertifikat *Shared Business CA* mit dem Namen Shared_Business_CA4.der herunter von der URL
- https://www.telesec.de/de/sbca/support/ca-zertifikate/category/96-shared-business-ca-4

  Da der OpenScape SBC nur Zertifikate im pem-Format unterstützt, muss das Telekom *Shared Business CA*-Zertifikat Shared_Business_CA4.der konvertiert werden
- über die Linux-Shell z. B. auf dem OpenScape SBC über den Befehl
- openssl x509 -inform der -in Shared_Business_CA4.der -out Shared_Business_CA4.pem
- oder über z. B. den Online-Konverter https://www.sslshopper.com/ssl-converter.html



Klicken Sie auf *Zertifikat konvertieren* und speichern Sie das konvertierte Zertifikat mit der Dateiendung .pem.

Erstellen Sie im nächsten Schritt ein verkettetes Zertifikat auf Basis der Zertifikate Deutsche Telekom Root CA 1 und Shared Business CA namens z. B. dt-chain-ca.pem und kopieren Sie den Inhalt dieser Zertifikatsdateien in der folgenden Reihenfolge in dieses Zertifikat:

-----BEGIN CERTIFICATE-----

<dt-root-ca-2.cer>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

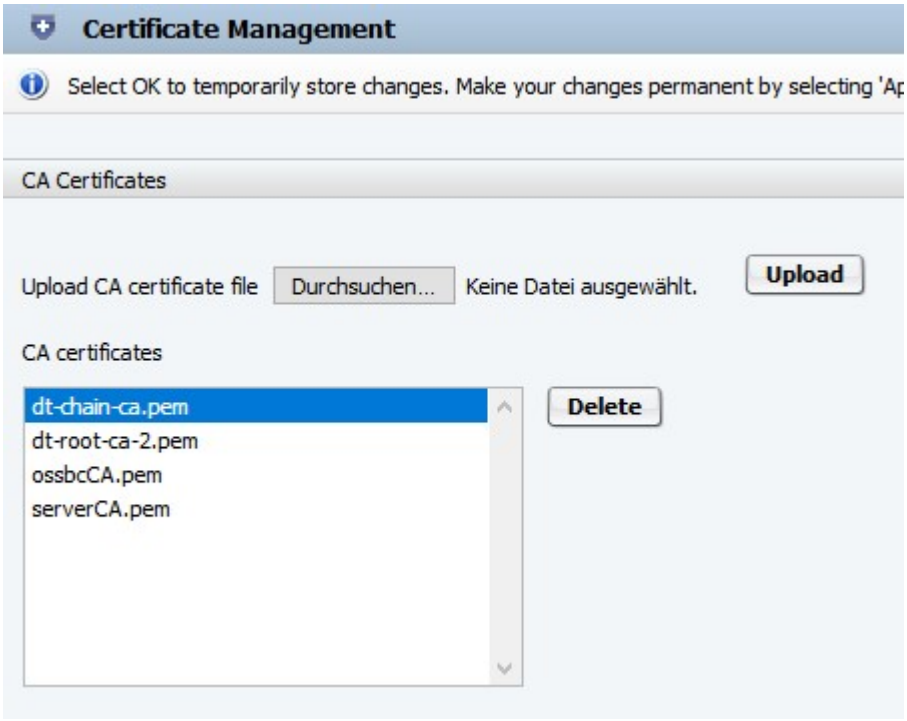
<Shared_business_CA4.cer>

-----END CERTIFICATE-----

Dann sollte das verkettete Zertifikat wie folgt aussehen:

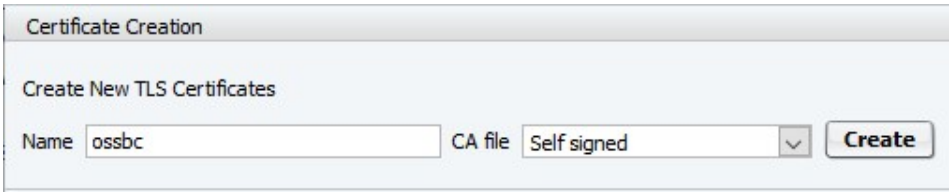
```
-----BEGIN CERTIFICATE-----
MIIGiTCCBXGgAwIBAgIIMBWLWM1WMfUwDQYJKoZIhvcNAQELBQAwcTELMAkGA1UE
...
nfKouiXc6eG1ojopwckO/uEu0JVEnyMOzGoIPU2/PhFvG6aAPsB4tvv/
AHzR
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDnzCCAoegAwIBAgIBJjANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJERTEc
...
Cm26OWMohpLzGITY+9HPBVZkVw==
-----END CERTIFICATE-----
```

Laden Sie dann dieses Zertifikat über die GUI unter Security -> General -> Certificate Management in OpenScape SBC im Abschnitt CA-Zertifikate hoch, indem Sie dieses Zertifikat auswählen und auf Upload klicken. Dann erscheint das Zertifikat in der Liste der CA-Zertifikate:

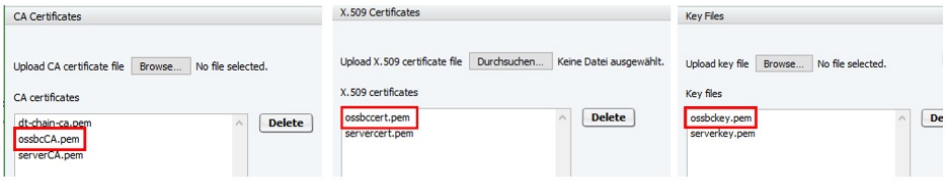


Um die von der Installation bereitgestellten OpenScape SBC-Standard-Zertifikate zu ersetzen, führen Sie die folgenden Schritte aus:

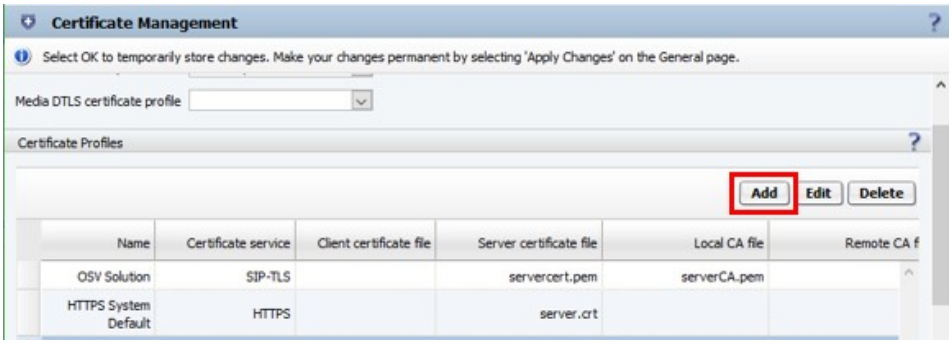
Im Abschnitt Zertifikatserstellung geben Sie z. B. ossbc in das Feld „Name“ ein und klicken Sie auf *Erstellen*, wobei Self signed als CA-Datei unverändert bleibt:



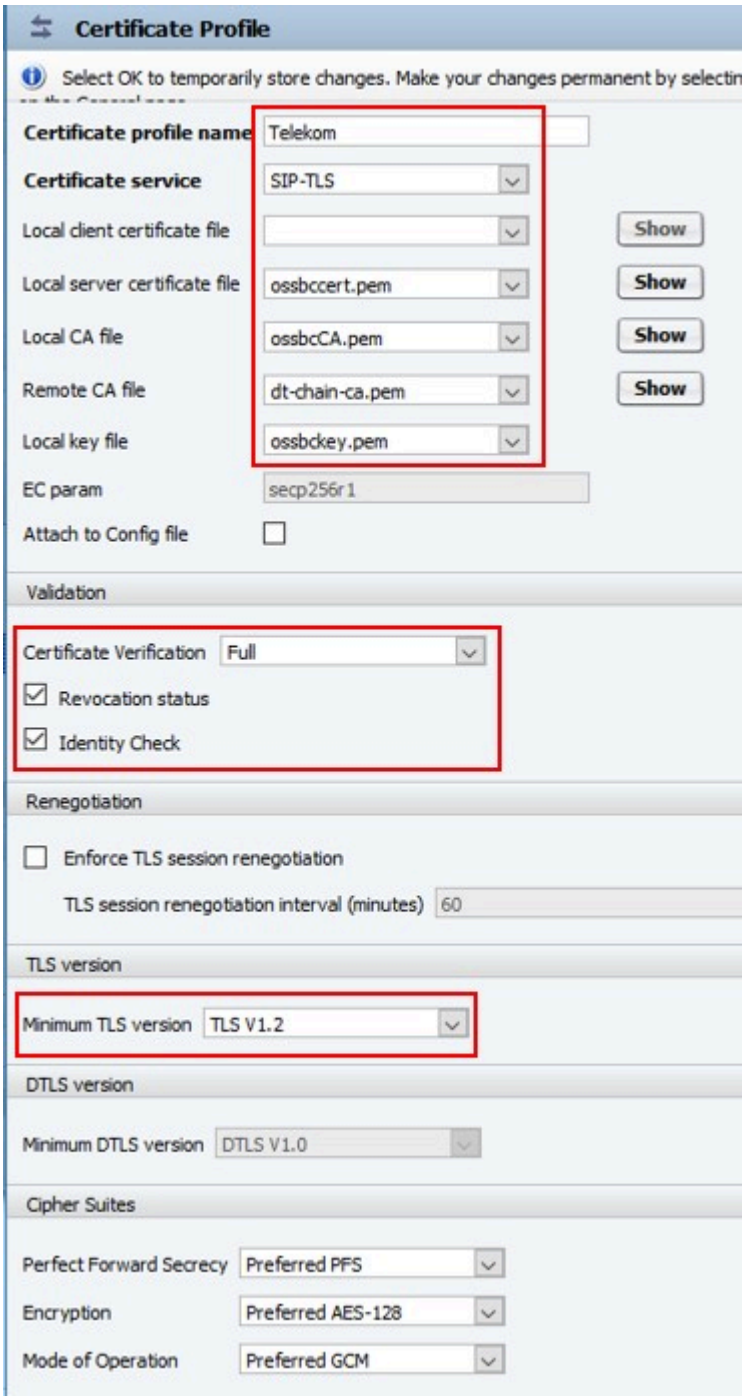
In den Fenstern *CA-Zertifikate*, *X.509 Zertifikate* und *Schlüsseldateien* erscheinen nun die neuen Zertifikate:



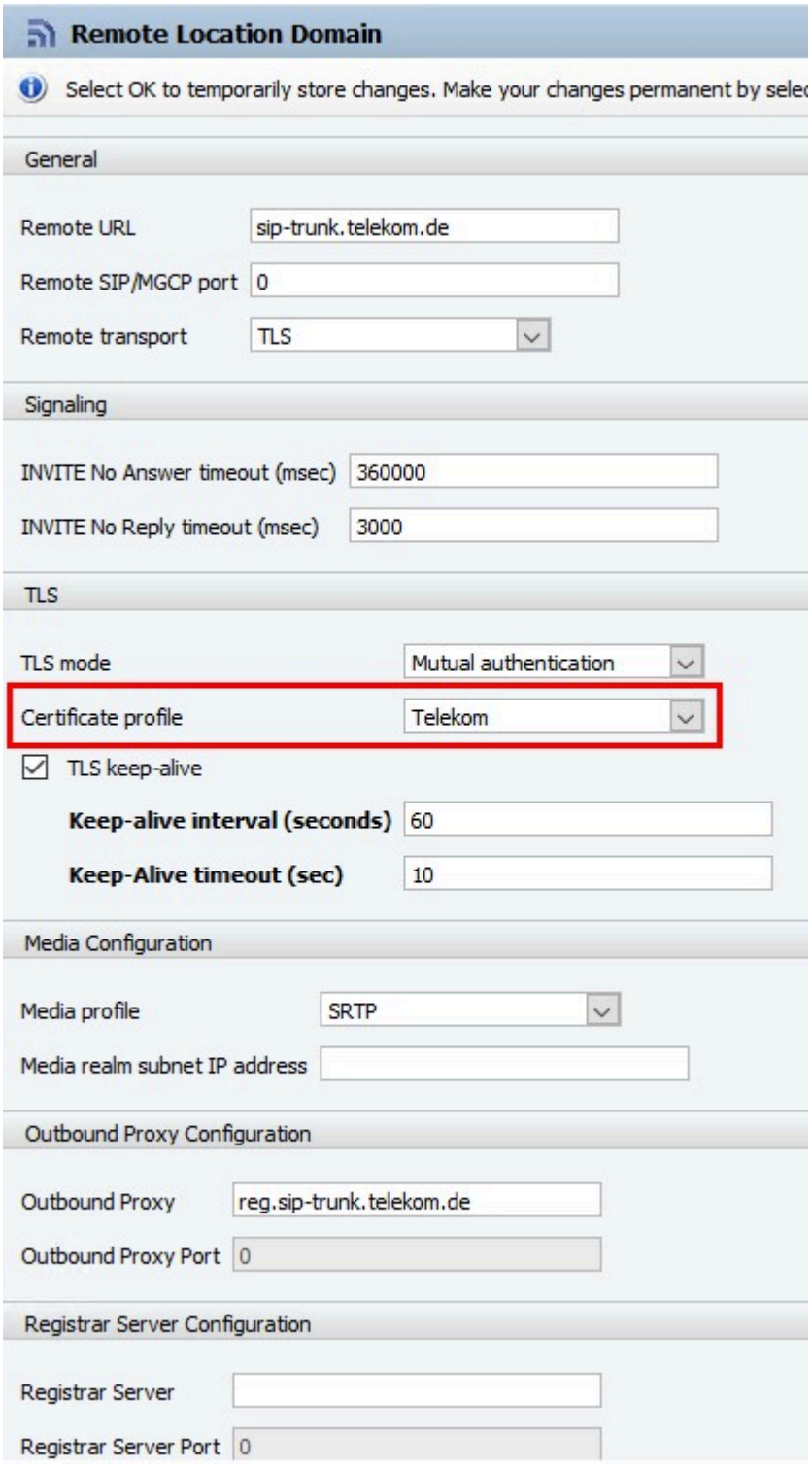
Klicken Sie im Abschnitt *Zertifikatprofile* auf *Hinzufügen*:



Erstellen Sie eine neue Zertifikatsprofil, indem Sie die zuvor erstellten Zertifikate auswählen:

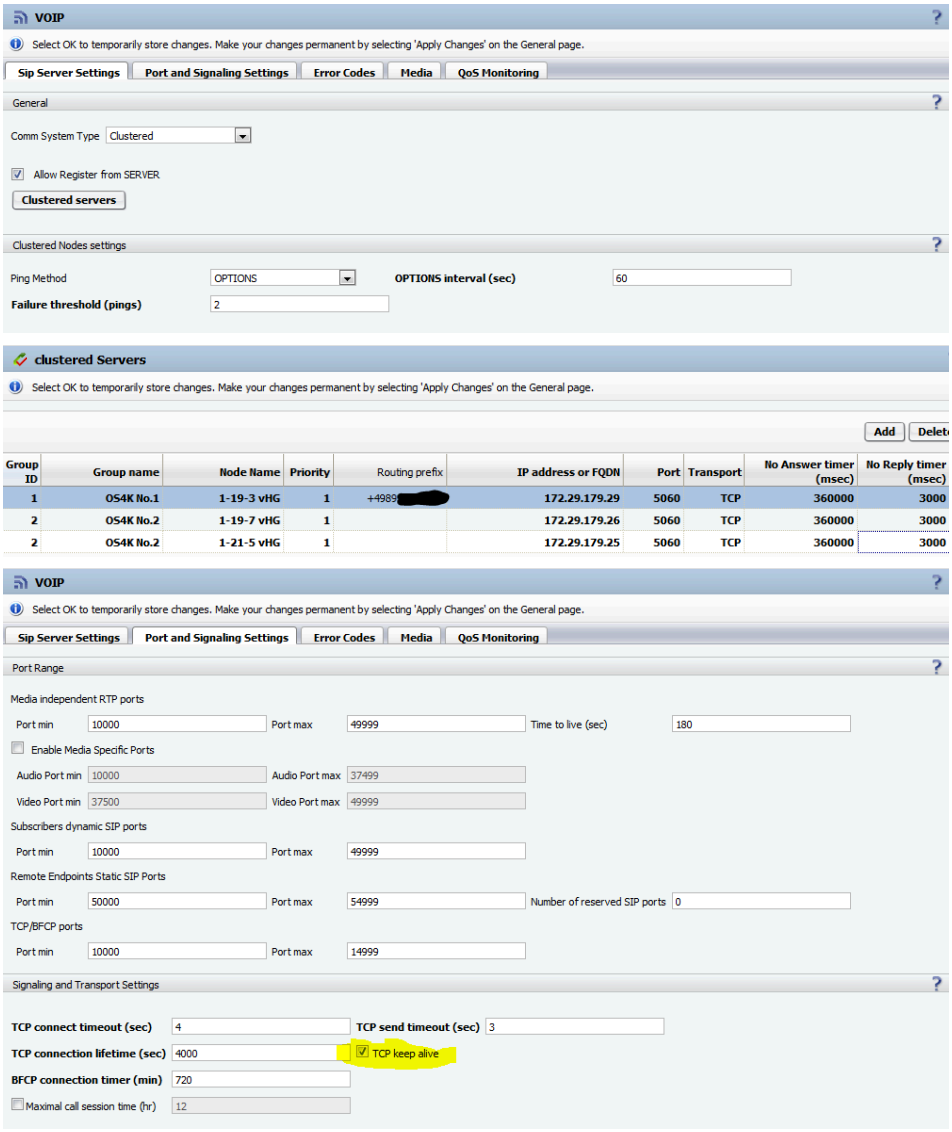


Schließlich muss die erstellte Zertifikatsprofil im Fenster *Remote Location Domain* konfiguriert werden:

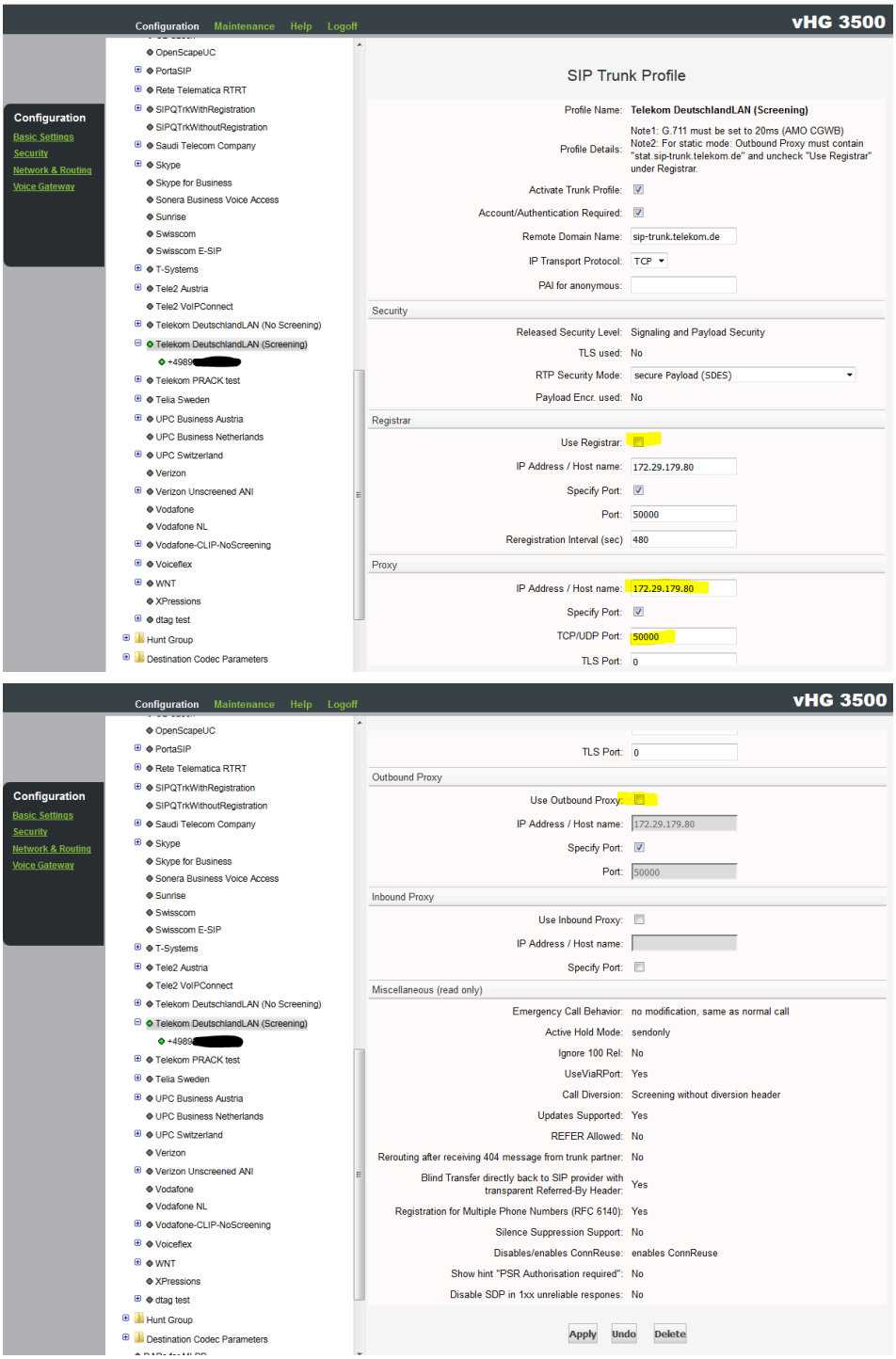


6. Konfiguration der VOIP-Einstellungen für OS4K:

(Beispiel ist die Verwendung von Non-Secure TCP, im Falle von Secure TLS bitte entsprechend anpassen z. B. 5061)



7. OS4K Gateway-Konfiguration (OpenScape SBC Core IP = 172.29.179.80)
(Beispiel ist die Verwendung von Non-Secure TCP, im Falle von Secure TLS bitte entsprechend anpassen, um TLS-Ports etc. zu verwenden)

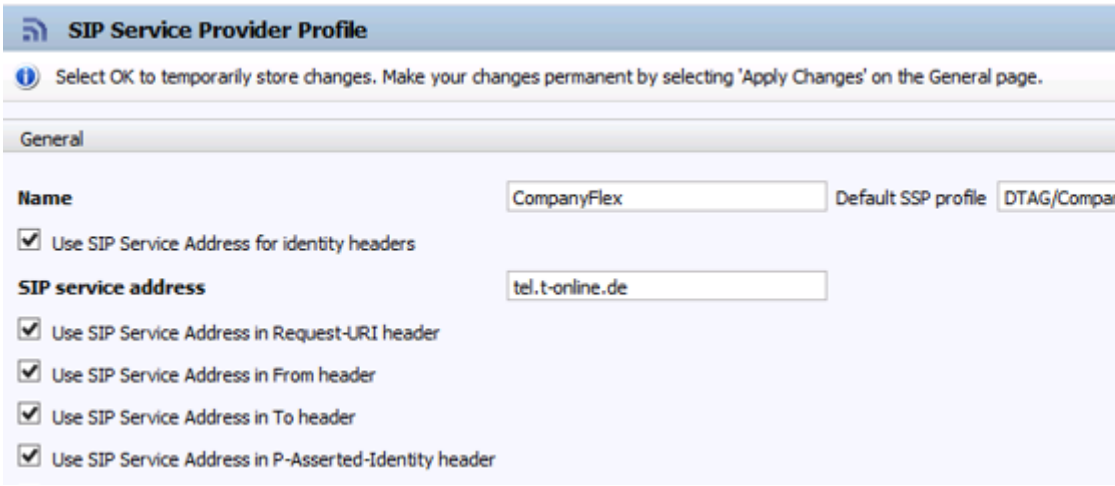


14.5.5.6 Konfigurationsbeispiel OpenScape SBC (CompanyFlex)

Die SBC Konfiguration ist analog zum Telekom DeutschlandLAN SIP trunk.

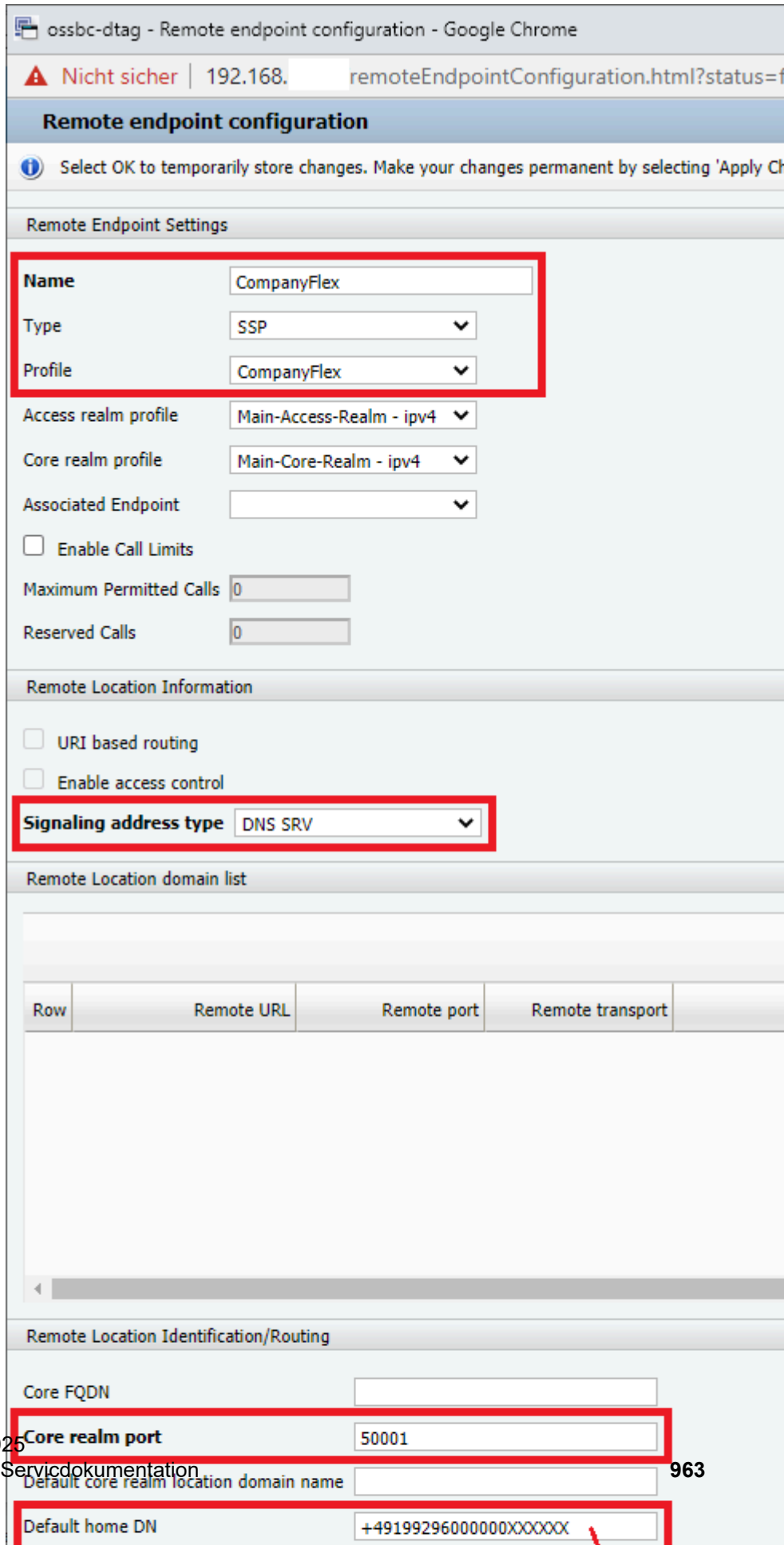
Folgende Deltas müssen beachtet werden:

Eigenes SIP Provider Profil:



„Use SIP Service Address from identity headers“ muss wie im Falle von DeutschlandLAN noch manuell aktiviert werden.

Beispiel für Remote Endpoint Konfiguration and „Remote Location Domain“ Konfiguration (unverschlüsselte Kommunikation per TCP/



14.5.5.7 Häufig gestellte Fragen – FAQ

Telekom Deutschland GmbH (TDG) – DeutschlandLAN SIP-Trunk

F: Welche Setups werden von TDG unterstützt und bevorzugt? A: Alle in der obigen Dokumentation aufgeführten Setups werden unterstützt. Für OS4K-Versionen <V7R2 wird vom TDG eine TDM-Lösung bereitgestellt. Der TDG-Router registriert sich über SIP zu TDG, verbindet sich aber über S2M/S0 mit dem OS4K. Bevorzugte Konfiguration von TDG ist die direkte Verbindung eines STMIX/STMI oder SoftGate mit den zertifizierten TDG-Routern => Fahren Sie den „ALL IP“-Rollout

F: Wird NAT unterstützt oder ist eine DMZ obligatorisch? A: Beide Setups werden mit TDG unterstützt. Aufgrund einer speziellen Logik prüft das TDG-Backend/CO, ob eine NAT-IP-Adresse verwendet wird. Wenn ja, dann erkennt und sendet das TDG Backend/CO die Nutzlast entsprechend.

F: Ist eine spezielle Konfiguration für DeutschlandLAN SIP-Trunk erforderlich? A: Ja, neben dem vordefinierten SIP-Profil, das verwendet werden soll, müssen auch einige spezielle Tarifnummern explizit in der LCR von OS4K konfiguriert werden. Diese müssen im Abonnenten- und nationalen Typ des Zahlenformats, z. B. 110 oder 112, gesendet werden. Weiterhin müssen einige Standardeinstellungen der Nutzlast geändert werden. Eine detaillierte Beschreibung finden Sie in Kapitel 4.5.3 „Konfiguration“.

F: Werden für DeutschlandLAN SIP-Trunk Secure Calls (TLS) unterstützt? A: Ja, unterstützt für STMIX und SoftGate. TDG unterstützt nur SDES. STMI unterstützt TCP/UDP & RTP.

F: Welcher ist der bevorzugte Verbindungsmodus – Registrierung oder statisch? A: Am Ende kommt es auf das Netzwerk oder Ihre Bedürfnisse an. Beide Modi haben Vor- und Nachteile. Im Falle von Einfachheit und NAT kann der Registrierungsmodus Vorteile bieten. Im Falle von fixed host/ip kann der statische Modus sinnvoll sein.

14.5.6 Nahübersprechen NAT Unterstützung für SG vHG Boards

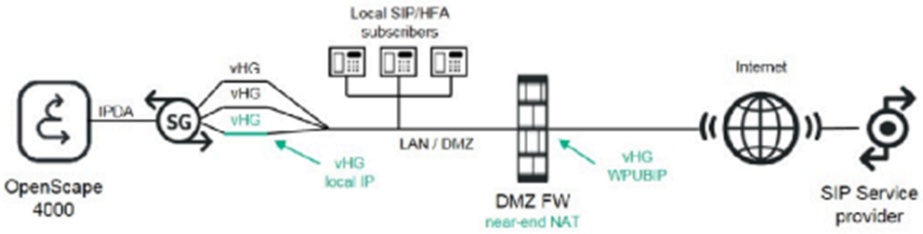
Die Nahübersprechen NAT Unterstützung kann je SG vHG SIP Board unter Verwendung von AMO-CGWB aktiviert werden. WPUBIP Parameter:

- WPUBIP = 0.0.0.0 gibt an, dass die Nahübersprechen NAT Unterstützung nicht aktiv ist
- WPUBIP = <gültige IPv4 Internet Adresse> aktiviert die Nahübersprechen NAT Unterstützung für das angegebene vHG Board
- Die Nahübersprechen NAT Unterstützung kann mit einem separaten WAN/DMZ Netzwerk kombiniert werden:
- USEWANIF=YES gibt an, dass das vHG Board mit dem DMZ Firewall mittels einem separaten WAN/DMZ Netzwerk verbunden ist
- USEWANIF=NO gibt an, dass ein freigegebenes LAN / DMZ-Netzwerk verwendet wird.

Die Nahübersprechen NAT Funktion unterstützt sowohl TRADITIO als auch SECURE SIP Amtsleitungen

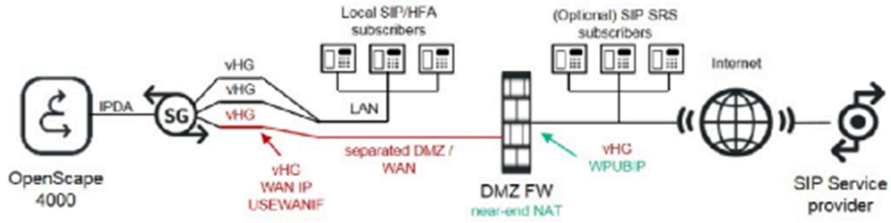
Das SG vHG Board kann so konfiguriert werden, dass es die SIP-SRS-Funktionalität (Secure Remote Subscriber) zusammen mit der

Nahübersprechen NAT SIP Amtsleitung hostet, wenn USEWANIF = YES aktiv ist.



Dediziertes SG vHG SIP Amtsleitungs Board- mit konfiguriertem Nahübersprechen NAT - gemeinsame LAN / DMZ zwischen vHG- und DMZ-Firewal

1) I



Dediziertes SG vHG SIP Amtsleitungs Board mit konfiguriertem Nahübersprechen NAT und WANIF (optional kombiniert mit SIP-SRS-Teilnehmerfunktionalität)

14.5.6.1 AMO-CGWB Konfigurationen

1. Dediziertes SG vHG SIP Amtsleitungs Board- mit konfiguriertem Nahübersprechen NAT - gemeinsame LAN / DMZ zwischen vHG- und DMZ-Firewall

```
ADD-
CGWB:LTU=<ltu>,SLOT=<vHG_slot>,SMODE=NORMAL,IPADR=<local_vHG_IP>
,NETMASK=<netmask>,USEWANIF=NO;
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=GLOBIF,WPUBIP=<ext
ernal_internet_IP_address>;
```

Es wird zusätzlich empfohlen DMC und SMP auf dem Board zu de-aktivieren

```
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=DMCDATA,DMCCONN=0,
SMP=NO,SMP4OSV=NO;
```

2. Dediziertes SG vHG SIP Amtsleitungs Board mit konfiguriertem Nahübersprechen NAT und WANIF (optional kombiniert mit SIP-SRS-Teilnehmerfunktionalität)

```
ADD-
CGWB:LTU=<ltu>,SLOT=<vHG_slot>,SMODE=NORMAL,IPADR=<WAN_vHG_IP>,N
ETMASK=<netmask>,USEWANIF=YES;
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=GLOBIF,WPUBIP=<ext
ernal_internet_IP_address>;
```

Es wird zusätzlich empfohlen DMC und SMP auf dem Board zu de-aktivieren
```
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<vHG_slot>,TYPE=MANLANIF,MIPADR=<l
ocal_vHG_mngmt_IP>,â¦;
```

14.5.7 SIP Amtsleitungen mit Nahübersprechen Ziel NAT (STMIX)

14.5.7.1 Wichtige Informationen

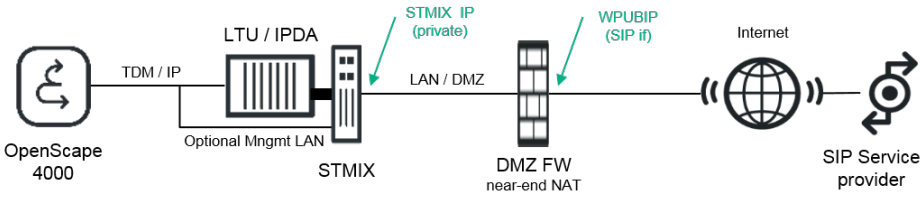
Ursprünglich gab es keine Möglichkeit, „WAN Public IP“ auf STMIX zu verwenden, da es keine Möglichkeit gab, eine eigene WAN-Schnittstelle zu definieren. Daher waren die Parameter WPUBIP und USEWANIF der CGWB AMO-Befehle voneinander abhängig. Die Aufteilung der Funktionalität in zwei unabhängige Parameter brachte uns den Vorteil, Near-End-NAT auf dem STMIX-Board (mit begrenzter Anzahl von Schnittstellen oder als Multiple-Feature mit lokalen HFA-Teilnehmern und SIP-Trunk) oder auf SoftGate einzusetzen. Near-End-NAT wird hauptsächlich in Szenarien mit SIP-Trunk zwischen OpenScape 4000 und PSTN-Anbieter angefragt.

WPUBIP ist eine abgetrennte lokale IP-Adresse, die für das SIP-Protokoll und lokale Medien verwendet wird (= NAT-Unterstützung für das Near-End-Ziel).

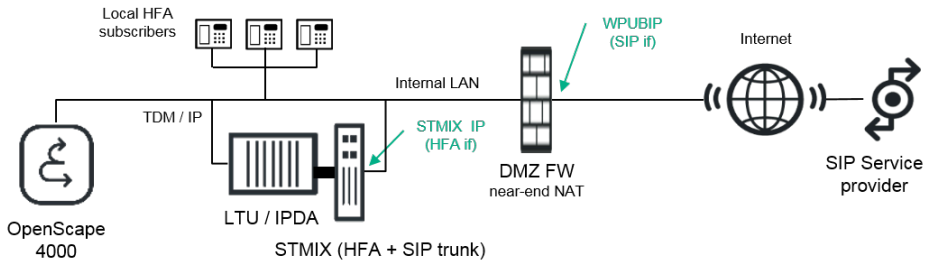
USEWANIF aktiviert zusätzliche Firewall-Sicherheit zur Durchsetzung der Teilnehmersicherheit (CIPHER) und zur Aktivierung der Unterstützung für die Umgehung von Far-End-NAT (Home-basiert) (SIP@Home-Teilnehmer)

Unterstützte Konfigurationen:

- Dedizierter STMIX für die SIP-Trunk-Konnektivität zum PSTN-Provider im lokalen Netzwerk oder in der DMZ mit (optionalem) Near-End-NAT für das Internet. D. h. WPUBIP ist (optional) so konfiguriert, dass die öffentliche IP-Adresse aus dem Internet sichtbar ist.

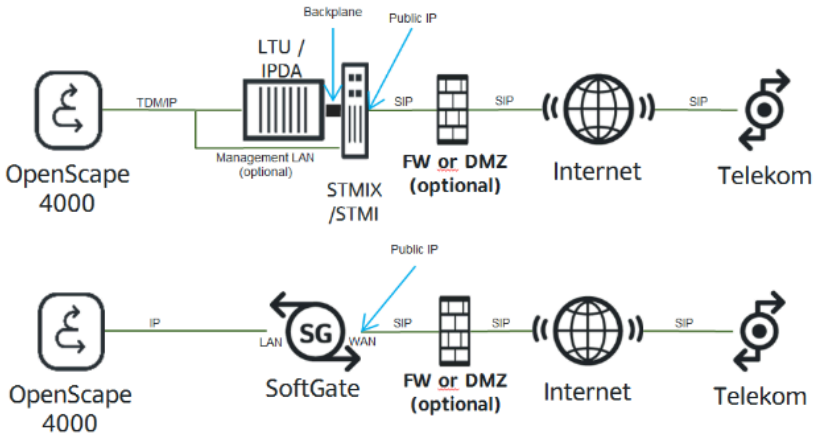


- MFS STMIX-Konfiguration zur Unterstützung der SIP-Trunk-Konnektivität zum PSTN-Anbieter über (optionale) DMZ-Firewall mit Near-End-NAT und lokal angeschlossenen HFA-Teilnehmern. D. h. WPUBIP ist konfiguriert. Der STMIX kann lokale SIP/UFIP-Teilnehmer und SIP-Trunk über Near-End NAT nicht parallel unterstützen, da nur eine SIP-Schnittstelle an eine externe öffentliche IP-Adresse angebunden ist.



Die Funktion definiert keine neuen Sicherheitsanforderungen und erfordert keine Änderungen an der unterstützten LAN-Konfiguration auf STMIX. AMO-Befehle und die Schnittstelle zwischen RMX und GW sind nicht betroffen.

Original STMIX/STMI/SoftGate Konfiguration – Öffentliche IP ist entweder im lokalen Netzwerk oder in der DMZ:



14.5.7.2 Konfigurationsmöglichkeiten

Die beiden Parameter sollten über AMO CGWB eingestellt werden:

- AMO CGWB: TYPE=GLOBIF, **WPUBIP**=<öffentliche IP-Adresse Near-end NAT>
- AMO CGWB: TYPE=GLOBIF, **USEWANIF**=<YES/NO> (optional konfigurierbar zur Unterstützung von Far-End-NAT (Home-basiert) für SIP@Home-Teilnehmer)

NOTICE: Dieser AMO-Befehl ist nur für SoftGate und STMIX relevant. Bei klassischem STMI darf dieser Parameter nicht durch den AMO-Befehl geändert werden. Der Standardwert ist „NEIN“.

14.5.8 Notrufe von mehreren Standorten über zentralisierten SIP-Trunk

Es ist möglich, SIP-Trunks nur am Hauptstandort zu installieren und alle Anrufe von den Zweigstellen über die SIP-Trunks des Hauptstandorts weiterzuleiten. Damit Notrufe an den richtigen PSAP weitergeleitet werden, muss der SIP-Carrier den Ursprung des Notrufs kennen.

Für einige SIP-Provider (z. B . Vodafone) ist die Registrierung von mindestens einem SIP-Trunk pro Zweigstelle erforderlich. Dadurch kann der Carrier den Ursprung von Notrufen feststellen.

OpenScape 4000 muss von Zweigstellen ausgehende Notrufe an den SIP-Trunk weiterleiten, der der betreffenden Zweigstelle zugewiesen ist.

Über die OpenScape SBC-Lösung wird eine Verbindung zum SIP-Carrier hergestellt, sodass mehrere SIP-Trunks, z. B. ein Trunk pro Zweigstelle, für den Carrier verwaltet werden können.

Diese Native SIP-Trunks sind an Kern-Ports an der SIP-Schnittstelle zu den SIP-Gateways von OpenScape 4000 angeschlossen.

Beispiel:

SIP-Trunk 1 ist Zweigstelle A zugewiesen. SIP-Trunk 2 ist Zweigstelle B zugewiesen.

Kern-Port 50000 des SBC ist mit Amtsleitung 1 verbunden. Kern-Port 50001 des SBC ist mit Amtsleitung 2 verbunden.

OpenScape 4000 leitet von Zweigstelle A kommende Notrufe an den Kern-Port 50000 des SBC weiter. OpenScape 4000 leitet von Zweigstelle B kommende Notrufe an den Kern-Port 50001 des SBC weiter.

Dies wird durch die LCR-Routing-Funktion von OpenScape 4000 ermöglicht.

Die entsprechenden Kern-Ports müssen in AMO GKREG festgelegt werden. Siehe unten stehendes Beispiel.

```
ADD-
GKREG:GWNO=99,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=10.140.102.208,
GWDIRNO=701,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="TRUNK_MULTI",
SECLEVEL=TRADITIO,PORT=50000;
ADD-
GKREG:GWNO=100,GWATTR=EXTGW&HG3550V2&SIP,GWIPADDR=10.140.102.208,
GWDIRNO=702,DIPLNUM=0,DPLN=0,LAUTH=1,INFO="TRUNK_MULTI",
SECLEVEL=TRADITIO,PORT=50001;
```

14.5.9 Notrufe

Bei Notrufen werden der SIP-PAI-Header und die Geolokalisierungsinformationen (die über Native SIP empfangen oder mit AMO LIN vom System generiert werden) über das **SIP-Provider**-Profil (Modify Profile Defaults) gehandhabt, indem der Parameter "**Emergency {{case}} Behav**iour" und/od**er "Anruf Geolocation (RFC** 6442)" von "No modification"/"Do not send location information for any Anruf" auf einen der in den folgenden Abbildungen dargestellten Werte geändert wird.

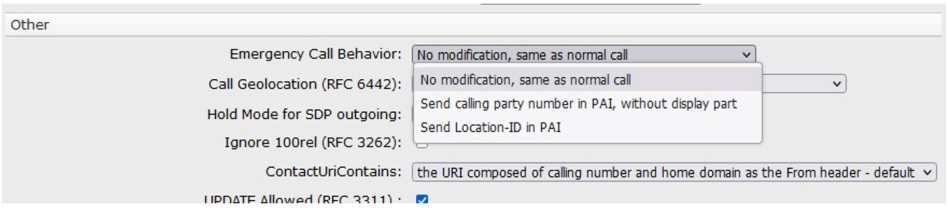


Figure 241: Änderung des Parameters des Notrufverhaltens

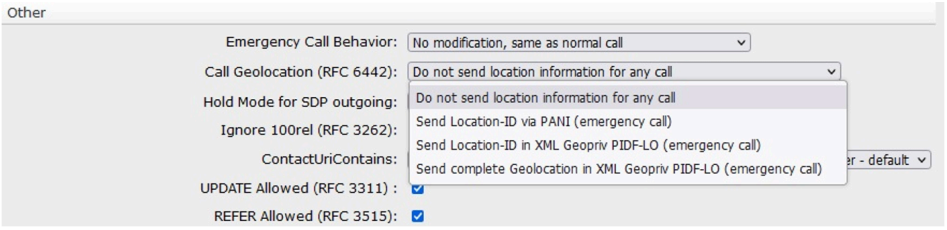


Figure 242: Änderung des Anruf-Geolokation-Parameters (RFC 6442)

Bei nativen SIP-Transitanrufen sollten die Einstellungen der eingehenden SIP-GW **für das Verhalten bei Notrufen bzw. die Anrufgeolokalisierung (R**FC 6442) mit den Einstellungen des Quellsystems übereinstimmen, um die Weiterleitung, Filterung oder Änderung aller empfangenen Informationen auf der ausgehenden Transit-GW zu ermöglichen.

Im {{case}} von Transit-Native-SIP-Trunking mit aktivem SMP wird **der RIC**HT-Parameter EMCYRTT (Notfallroute) ignoriert.

Es ist nicht möglich, den Typ der im PAI-Header gesendeten Nummer automatisch zu bestimmen (ob es sich um eine Telefonnummer oder eine Standort-ID handelt). Bei nativen SIP-Transitanrufen, bei denen das Quellsystem die Standort-ID in PAI sendet, ist die Entfernung möglich, indem Sie das SIP-Profil vom OpenScape 4000 Gateway für eingehenden Transit ändern. Auf diese Weise wird der empfangene PAI durch die im **FROM**-Header empfangene Nummer ersetzt.

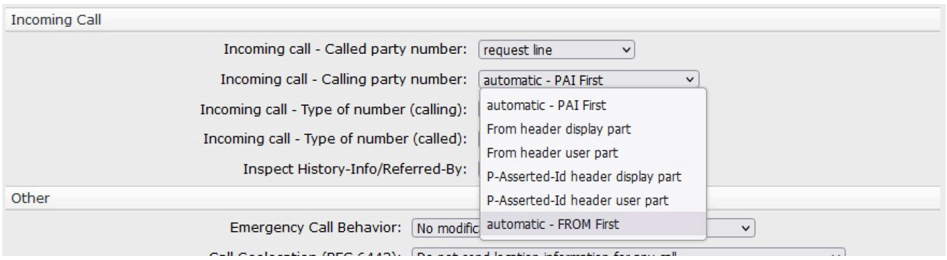
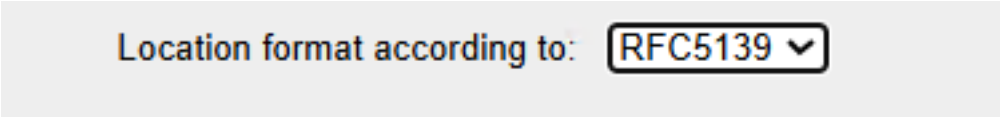


Figure 243: Änderung des eingehenden Anrufs - Nummer des Anrufers

Die Voreinstellung des "Presence-based GEOPRIV Location Object Format" basiert eigentlich auf RFC 4119.

Über den folgenden Profilparameter kann es je nach Bedarf des Notrufanbieters auf RFC 5139 umgestellt werden.



14.6 Konfiguration SIP-Q-Trunking / Native SIP Trunking

14.6.1 Konfiguration mit Hilfe von AMOs

Wichtig: Zusätzlich zu der AMO Konfuguration **muss** für einen **native SIP Trunk** bzw. **kann** für einen **SIP-Q-Trunk** im WBM

der Trunking-Partner mit Hilfe der SIP-Trunk-Profile konfiguriert werden (siehe Abschnitt 3.3, „SIP-Trunk Profile“).

14.6.1.1 Trunking-Protokoll

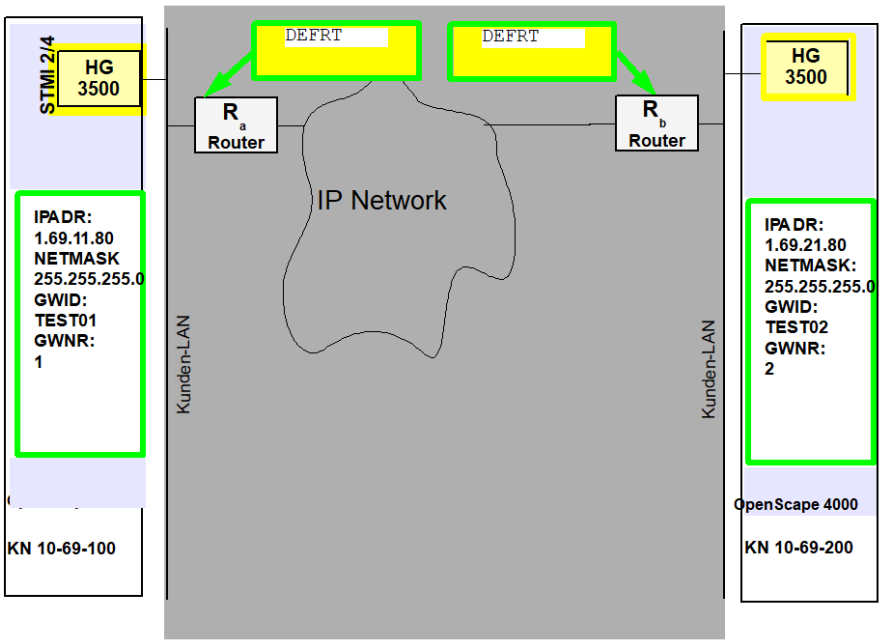
Im AMO CGWB und AMO GKREG müssen immer die selben Protokolle eingestellt werden.

Tabelle 80: Protokolle im AMO CGWB und AMO GKREG

AMO CGWB	AMO GKREG	Protokoll
TRPRSIP	SIP	native SIP
TPRSIPQ	SIPQ	SIP-Q V2

14.6.1.2 Einrichten einer (v)HG 3500 als internes Gateway

Die folgende Abbildung zeigt die auf HG 3500 reduzierte Situation bei einem fiktiven Kunden in Frankfurt. Dargestellt sind der Knoten 10-69-100 (Frankfurt-Bockenheim) und der Knoten 10-69-200 (Frankfurt-Sachsenhausen). Beide Anlagen verfügen über je eine Common Gateway-Baugruppe, die als HG 3500 eingerichtet werden soll. Auf beiden Anlagen soll der LEGK laufen (zwei Mal local Gateway). Diese Konstellation ist daher relativ einfach zu erklären, weil dann die beiden Knoten quasi symmetrisch eingerichtet werden können. Im Bild sind alle benötigten Parameter eingetragen. Der Knoten 10-69-100 befindet sich im IP-Netz 1.69.11.0 /24 und der Knoten 10-69-200 liegt im IP-Netz 1.69.21.0 /24. Beide Netze erreichen sich über die Router Ra und Rb.



Einrichtebeispiel: beide Knoten sind LEGK

14.6.1.2.1 Konfiguration in Knoten 10-69-100

Im Knoten 100 beginnt man mit der Einrichtung der Baugruppe als HG 3500. Es empfielt sich, die Baugruppe erst am Ende der Konfiguration zu stecken, um sich mehrere Neustarts zu ersparen.

Schritt 0:

LEGK im Knoten 10-69-100 einrichten.

```
AENDERN-ZANDE:TYP=DATENALL,GATEKPR=JA;
```

Schritt 1:

Die Common Gateway Baugruppe Q2316-X wird als HG 3500 eingrichtet. Die Q2316-X ist die Ausgabe mit 60 B-Kanälen. Sie können die Baugruppe als reine IP-Trunking Baugruppe einrichten oder auch im Mischbetrieb mit IP-Trunking und LAN-Connectivity (WAML) und diversen anderen Leistungsmerkmalen.

Konfiguration der Baugruppe nur für IP-Trunking:

```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;
CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,UNITS=3; /
* 30 B-Kanäle für HG3550-Funktion (H323-Trunking, SIP-
Trunking, SIP Subscriber)
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-
X",FCTID=1,LWVAR="0",FCTBLK=1,BCHL3550=30,ALARMNO=0;
```

oder

IP-Trunking & WAML:

```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=HG3550&WAML,BGBKAN=BKAN60&BKAN120;
CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,UNITS=3; /
* 30 B-Kanäle für HG3550-Funktion (IP-Trunking, SIP-
Trunking, SIP Subscriber)
CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=WAML,UNITS,LINECNT=1; /
* Baugruppe wird mit einem Satz, d. h. 10 B-Kanälen für
 WAML, eingerichtet
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=1,SLOT=37,PARTNO="Q2316-
X   ",FCTID=1,LWVAR="0",FCT►
BLK=1,BCHL3550=30,BCHLWAML=10,ALARMNO=0;
```

Schritt 2:

Die Baugruppe erhält über den AMO CGWB die IP-Adresse im Kunden-LAN (LAN1), die Subnetzmaske und die Protokollvariante (SIP-Q / H323A / KEIN (Baugruppe wird nur für SIP Subscriber konfiguriert)).

Wichtig: Pro Baugruppe kann nur ein Trunking-Protokoll konfiguriert werden! Mischung mit anderen Funktionen ist uneingeschränkt möglich!

```
ADD-
CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NETMASK=255.255.255.
PRHSIPQ=10;/*10 B-Kanäle für SIP-Q-Trunking
```

oder

```
ADD-
CGWB:LTU=1,SLOT=37,SMODE=NORMAL,IPADDR=1.69.11.80,NETMASK=255.255.255.
PRHSIP=10; /*10 B-Kanäle für natives SIP-Trunking
```

=> Es bleiben 20 B-Kanäle für andere Funktionen

Schritt 3:

Nun wird der Default Router im Kunden LAN eigestellt:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=GLOBIF,DEFRT=1.69.11.254;
```

Schritt 4:

Die HG 3500-Baugruppen werden über eine Gateway-Nummer (**GWNO**) verwaltet. Diese muss eindeutig sein.

```
CHANGE-CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1;
```

Schritt 5:

Konfiguration ohne Authetifizierung und ohne Registrierung (Default-Werte im AMO CGWB.

```
CHANGE-
CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=LEGKDATA,GWNO=1, REGEXTGK=NO;
```

SSA:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=SIPTRSSA,SIPREQ=NEIN;
```

ERH:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=1,SLOT=37,TYPE=SIPTRERH,GWAUTREQ=NO;
```

Wichtig: Die **Parameter SIPREG** und **REGEXTGK** müssen stets den gleichen Wert aufweisen.

Schritt 6:

Wichtig: Es sind mehrere Baugruppen in einem Bündel erlaubt!

Dieser Schritt umfasst nun mehrere Einrichtekommandos. Es wird das Bündel und der Satz eingerichtet, über den die B-Kanäle zwischen Gateway und OpenScape 4000 geschaltet werden.

Zunächst braucht man ein Bündel:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 1
 ",NO=30,TRACENO=0, ACDTHRH=*, PRIONO=2, TDDRFLAG=ON,
 GDTRRULE=0, ACDPMGRP=0, CHARCON=NEUTRAL;
```

Dann wird ein digitaler Leistungssatz (AMO TDCSU) benötigt. Der Gerätetyp ist **HG3550IP** (für H323/H323A und natives SIP/SIP-Q-Trunking). Wenn Sie DMC zulassen möchten, setzen Sie DMCALLWD **=Y**. Dies ist nur möglich, wenn das Partnersystem DMC unterstützt.

```
ADD-TDCSU:OPT=NEW,PEN=1-01-037-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT from GW2",PROTVAR="ECMAV2",SEGMENT=8,
 ISDNIP=00,ISDNNP=0,TRACOUNT=31,SATCOUNT=MANY,

NNO=1-69-499,ALARMNO=12,
 COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,

TCCID="IP RS",TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,

BCHANNEL=1&&30,BCNEG=N,BCGR=1,LWPAR=0,DMCALLWD=YES;
```

Wenn für die native SIP-/SIP-Q-Trunkingstrecke DMC aktiviert wurde, sollte auch Voice Activity Detection aktiviert werden. Andernfalls benötigt man auf der Masterverbindung die gleiche Bandbreite wie auf der Slaveverbindung!

```
CHANGE-CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,

PRIO=PRIO1,VAD=YES;
```

Andernfalls benötigt man auf der Masterverbindung die gleiche Bandbreite wie auf der Slaveverbindung.

Wichtig: Es empfiehlt sich ein Rücksetzen der Baugruppe:
`RESET-BSSU:ADDRTYPE=PEN,LTG=1,LTU=1,SLOT=37;`

Wichtig: Über das Kommando AENDERN-FUNSU kann das komplette Neuladen der STMI Baugruppe verhindert werden. Ein Neuladen ist nur bei Loadware-Änderungen erforderlich. `CHANGE-FUNSU:PIT=FLASH,PARTNO="Q2316-X ",FCTID=2, ACTION=RESET;`

Schritt 7:

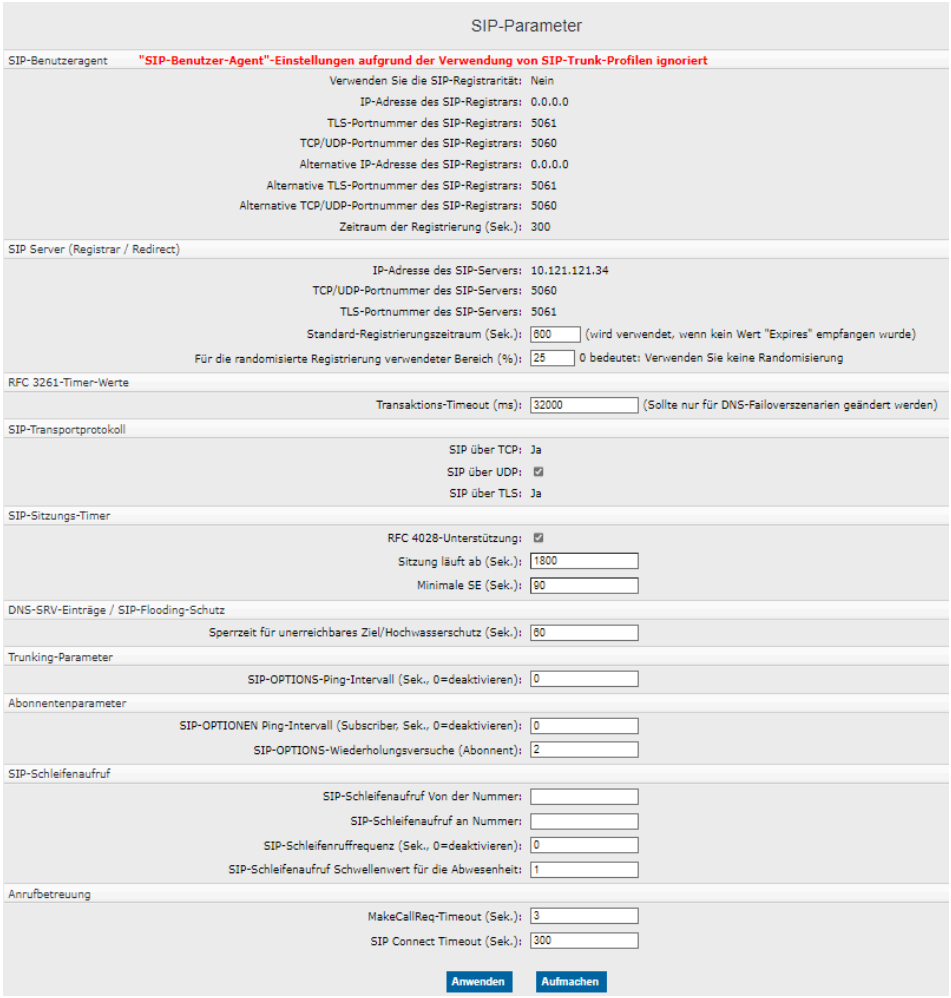
Der LEGK muss nun noch im AMO GKREG über die Existenz des HG 3500 Gateways informiert werden. **GWNO** muss mit dem Eintrag aus AMO CGWB übereinstimmen. Bei einem lokalen Gateway lädt AMO GKrEG automatisch die IP-Adresse (**IPADR**) aus AMO CGWB. Sie müssen auch die Attribute **INTGW** (internal -local- Gateway) und **HG3550V2** (Versions-ID) festlegen. Der Parameter **REGGW** ist nicht erforderlich, da sich das Gateway nicht bei einem anderen Gateway registrieren muss.

```
ADD-GKREG:GWNO=1,GWATTR=INTGW&HG3550V2&SIPQ or
 SIP,NUM=0,DPLN=0,LAUTH=1;
```

Wenn ein lokales Gateway konfiguriert ist, wird **REGISTERED=NO** stets mit `DISPLAY-GKREG;` angezeigt.

Schritt 8:

Die Konfiguration des Transportprotokolls (TCP, UDP) muss in allen Anlagen übereinstimmen. Das verwendete Transportprotokoll kann mit WBM unter **Konfiguration** > **Voice Gateway** > **SIP-Parameter** eingestellt werden.



Damit ist die HG 3500-Baugruppe im Knoten 10-60-100 funktionsfähig und kommuniziert mit dem LEGK. Es fehlt aber noch das Gateway im Partnerknoten.

14.6.1.2.2 Einrichtung in Knoten 10-69-200

Im Knoten 10-69-200 soll ebenfalls ein LEGK laufen. Die Einrichtung von 10-69-200 ist spiegelbildlich zur Einrichtung im Knoten 10-69-100. Daher werden nur die entsprechenden AMO-Kommandos zu den oben genannten Schritten aufgeführt.

Schritt 0:

```
CHANGE-ZANDE:TYPE=ALLDATA,GATEKPR=YES;
```

Schritt 1:

```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;
CHANGE-
BFDAT:CONFIG=CONT,FCTBLK=1,FUNCTION=HG3550,LINECNT=1,
```

```
UNITS=3; /* 30 B-Kanäle für HG3550-Funktionalität (IP-
Trunking, SIP-Trunking,
SIP-Teilnehmer)
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
ADD-BCSU:MTYPE=IPGW,LN=1,LTU=2,SLOT=49,PARTNO="Q2316-X   ",

FCTID=1,LWVAR="0",FCTBLK=1,BCHL3550=30,ALARMNO=0;
```

Schritt 2:

```
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,

IPADDR=1.69.21.80,NETMASK=255.255.255.0,TRPRHSIPQ=10;
ADD-CGWB:LTU=2,SLOT=49,SMODE=NORMAL,

IPADDR=1.69.21.80,NETMASK=255.255.255.0,TRPRHSIP=10;
```

Schritt 3:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=GLOBIF,DEFRT=1.69.21.254;
```

Schritt 4:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=LEGKDATA,GWNO=2;
```

Schritt 5:

```
CHANGE-CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=LEGKDATA,

GWNO=2,REGEXTGK=NO;
```

SSA:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=1,SLOT=49,TYPE=SIPTRSSA,SIPREG=NO;
```

ERH:

```
CHANGE-
CGWB:MTYPE=CGW,LTU=2,SLOT=49,TYPE=SIPTRERH,GWAUTREQ=NO;
```

Wichtig: Die **Parameter SIPREG** und **REGEXTGK** müssen stets den gleichen Wert aufweisen.

Schritt 6:

```
ADD-BUEND:TGRP=50,NAME="IP TRUNK GWID 2 ",NO=30;
ADD-TDCSU:OPT=NEW,PEN=1-02-049-0,COTNO=36,

COPNO=32,DPLN=0,ITR=0, COS=2,LCOSV=1,LCOSD=1,

CCTN="CIRCUIT von
 GW2",PROTVAR="ECMAV2",SEGMENT=8,ISDNIP=00,

ISDNNP=0,TRACOUNT=31,SATCOUNT=MANY,NNO=1-69-499,

ALARMNO=12, COTX=36,CCHDL=SIDEA,CLASSMRK=EC&G711,TCCID="IP
 RS",
```

```
TGRP=50,SRCHMODE=DSC,INS=Y,DEV=HG3550IP,BCHANNEL=1&&30,BCNEG=N,BCGR=1,
PAR=0(=Master),DMCALLWD=YES;
CHANGE-
CGWB:MTYPE=CGW,LTU=<ltu>,SLOT=<slot>,TYP=ASC,PRIO=PRIO1,

VAD=YES;
```

Schritt 7:

Das GKREG enthält die Konfiguration für beide HG 3500-Baugruppen. Hier ist **GWNO=2** jetzt der lokale Gateway in Knoten 10-69-200 mit den Attributen **INTGW**, **HG3550V2** und **SIPQ/SIP**, während **GWNO=1** (der Partner-Gateway in Knoten 10-69-100) in diesem System die Attribute **EXTGW**, **HG3550V2** und **SIPQ/SIP** enthält. Der Parameter **REGGW** ist nicht erforderlich, da sich das Gateway nicht bei einem anderen Gateway registrieren muss.

```
ADD-GKREG:GWNO=1,GWATTR=EXTGW&HG3550V2&SIPQ oder SIP,GWIPAD▶
DR=1.69.11.80,DIPLNUM=0,DPLN=0,LAUTH=1;
ADD-GKREG:GWNO=2,GWATTR=INTGW&HG3550V2&SIPQ oder
 SIP,DIPLNUM=0,DPLN=0,LAUTH=1;
```

14.6.1.2.3 Ergänzung im Knoten 10-69-100

Im Knoten 10-69-100 muss für den LEGK noch die HG 3500 im Knoten 10-69-200 nachgetragen werden (AMO GKREG). Diese HG 3500 (**GWNR=2**) ist für den Knoten 10-69-100 ein externes Gateway (Attribute **EXTGW&HG3550V2&SIPQ/SIP**), dass sich im Knoten 10-69-100 nicht registriert.

```
EINRICHTEN-GKREG:GWNR=2,GWATTR=EXTGW&HG3550V2&SIPQ oder
 SIP,GWIPA▶
DR=1.69.21.80,WAPLNUM=0,WABE=0,LBER=1;
```

14.6.1.2.4 Ruf von Knoten 10-69-100 zu Knoten 10-69-200

Exemplarisch soll nun das LCR für den Knoten 10-69-100 so eingerichtet werden, das ein Teilnehmer dieses Knotens über eine offene Nummerierung (**UNKNOWN**) einen Teilnehmer des Knoten 10-69-200 über den IP-Trunk erreicht. Verdeckte Nummerierung oder ISDN-Rufnummernpläne werden ebenso unterstützt und vergleichbar eingerichtet.

Der Teilnehmer des Knotens 10-69-100 erreicht den Knoten 10-69-200 über die Querkennziffer 902.

```
EINRICHTEN-WABE:RNR=902,KZP=QUER;
```

LRTG 520 soll zu Knoten 10-69-200 führen und das Bündel 50 (s.o.) benutzen:

```
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=520,LDIENST=ALLE,

NAME="IP ZU KN 69 200 ", BUNUM=50,ZKNNR=1-69-499;
```

Eine einfache Wahlregel:

```
EINRICHTEN-LODR:LWR=520,LWREL=ECHOFELD,FELD=2;

EINRICHTEN-LODR:LWR=520,LWREL=ENDE;

EINRICHTEN-LODR:LWR=520,INFO="QUER ZU GW2";
```

In der LRTG 520 trägt man nun unter **GW1=2-0** ein. Die **2** verweist auf den Parameter **GWNR** im AMO GKREG (siehe Abschnitt 6.1.2.3, „Ergänzung im Knoten 10-69-100“). Im AMO GKREG des Knotens 10-69-100 ist die HG 3500 mit **GWNR=2** die IP-Adresse 1.69.21.80. Die **0** steht für die Sektorpfadnummer. Sektorpfad 0 bedeutet, dass für diesen Weg unbegrenzt Bandbreite zur

Verfügung steht. Sollte das Zielgateway nicht erreichbar sein, kann man über die Parameter **GW2** bis **GW5** ein Alternativrouting konfigurieren.

```
EINRICHTEN-
LDAT:LRTG=520,LDIENST=ALLE,LWERT=1,BUNUM=50,LWR=520,

LBER=1, GW1=2-0;
```

> **Wichtig:** Im Gegensatz zu S0-/S2-Verbindungen (Punkt zu Punkt) ist eine IP-Verbindung eine Punkt- zu Mehrpunkt-Verbindung, und somit wird im AMO LDAT immer die gleiche Bündelnummer zu unterschiedlichen Zielgateways (**GW1-GW5**) verwendet!

Die Querkennziffer wird in den AMO LDPLN eingetragen. Die Rufnummer wird in den Standardwählplan mit **WAPLNUM=0** eingetragen. Anstelle von LRTG kann auch ein Profilindex verwendet werden (AMO LPROF):

```
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="902"-"X",

LRTG=520,LBER=1;
```

Möchte man den Fall einrichten, dass man vom Knoten 10-69-200 den Knoten 10-69-100 erreicht, so ist diese Konfiguration entsprechend durchzuführen. Man verweist dann im AMO-LDAT auf die **GWNR=1**.

14.6.1.3 Backup & Restore der WBM-Konfigurationsdaten

Alle Konfigurationsdaten, die über das WBM der Baugruppe eingerichtet werden, müssen über einen Backup-Server gesichert werden. Andernfalls würden nach einem Baugruppentausch, einem Reset der Baugruppe oder einem Loadware-Upgrade alle Konfigurationsdaten verloren sein und die native SIP-/SIP-Q-Trunking-Verbindung könnte nicht automatisch wieder hergestellt werden. Dies geschieht über den OpenScape 4000 Assistant > Backup & Restore.

Hierfür ist es wichtig sicherzustellen, dass der Backup-Server immer erreichbar ist. Falls der Backup-Server nicht erreichbar ist, können die Konfigurationsdaten auch im Flash der Baugruppe gesichert werden und von dort geladen werden.

OpenScape 4000 Assistant > Backup & Restore

Verbindung zum OpenScape 4000 Assistant und Backup-Server konfigurieren:

```
AENDERN-CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=MGNTDATA,

MGNTIP=<ip_adresse_assistant>,MGNTPN=<port_nr_assistant>,

BUSIP=<ip_adresse_backup_server>,BUSPN=<port_nr_backup_server>};
```

Hinweis: Nach einem Restart der Baugruppe werden die Werte für **MGNTPN** und **BUSPN** nicht wiederhergestellt. Diese müssen neu konfiguriert werden.

Lokaler Flashspeicher

> **Wichtig:** Es wird empfohlen den Flash ebenfalls als Backup-Medium einzurichten. Wenn der Backup-Server nicht erreichbar sein sollte, so wird auf diesen lokalen Speicher zurückgegriffen.

WBM> Wartung > Aktionen > Automatische Aktionen > Konfigurationsdateien im lokalen Flash speichern

Für mehr Informationen siehe „Gateways HG 3500 und HG 3575“, Kapitel 6, „Konfigurationsdaten im lokalen Flash speichern (local Backup & Restore)“.

Wichtig: Wenn der Restore notwendig ist (z.B. nach einer Hochrüstung der Loadware) und der Backup-Server während der Hochlaufphase nicht erreichbar ist, wird die Baugruppe mit Defaultkonfiguration geladen bzw. in Betrieb genommen. Sollte danach der HBR-Server erreichbar sein, wird der Restore nachträglich gemacht und ein Reboot mit der neuen Konfiguration angestoßen! Ein zusätzlicher Reboot wird ebenfalls während der Hochlaufphase angestoßen, wenn betriebsnotwendige Konfigurationen/Daten durch den Restore zurückgespielt werden (z.B. SPE-Zertifikate).

Wichtig: Um Probleme bei Hochrüstungen/Loadware-Tausch zu vermeiden, sollte nach dem Austausch einer Baugruppe (Hardware-Tausch) unbedingt ein Backup angestossen werden, da der Backup auch mit der MAC-Adresse verknüpft ist.

14.6.1.4 Abfragen des Linkstatus

Der Linkstatus der LAN-Schnittstelle (Linksignal Ethernet, LAN-Geschwindigkeit und LAN-Schnittstelle) kann mittels AMO SDSU auf den einzelnen Ebenen abgefragt werden, und zwar über die üblichen Kommandos (**PERI1**, **PERI2,** and **PERI3**):

```
ABFRAGEN-SDSU:TYP=LAGE,EBENE=PERI1,LTG=1,LTU=<ltu nr>,

EBT=<ebt nr>;
```

14.6.1.5 Vorgehen bei Erweiterung um weitere HG 3500 Gateways im Netz

Weitere LEGKs können analog zu Knoten 10-69-100 konfiguriert werden. Dann sind AMO BFDAT, AMO BCSU, AMO CGWB, AMO GKREG und AMO LDAT in einem Knoten.

Wichtig: Wichtig ist, der GKREG muss alle im Netz befindlichen (v)HG 3500 Baugruppen kennen.

14.6.1.6 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BCSU	TYP=IPGW	d	CGW einrichten

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	TYPE=IPGW	e	Configure CGW
	BKAN3550	d	Anzahl der B-Kanäle für IP-Trunking
	BCHL3550	e	Number of b channels for IP trunking
BFDAT	FUNCTION=HG3550	d	CGW mit IP-Trunking
	FUNCTION=HG3550	e	CGW with IP trunking
	BGBKAN	d	Maximale Anzahl der verfügbaren B-Kanäle der Baugruppe (entweder 60 oder 120)
	BRDBCHL	e	Maximum number of available b channels (60 or 120)
	ANZSATZ	d	Anzahl der Sätze für IP-trunking
	LINECNT	e	Number of lines for IP trunking
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.
CGWB	DEFRT	d	IP-Adresse des Default Routers
	DEFRT	e	IP address of the default router
	GWAUTREQ	d	Ziffern-Authentifizierung wird benötigt
	GWAUTREQ	e	Digest authentication is required
	GWREALM	d	Security Zone of the gateway
	GWREALM	e	Security Zone of the gateway
	GWRNR	d	Gateway Rufnummer
	GWDIRNO	e	Gateway Directory Number
	GWSECRET	d	Passwort des Gateways
	GWSECRET	e	Password of the gateway
	GWUSERID	d	User Identifizierung des Gateways
	GWUSERID	e	User identification of the gateway
	REGIP1	d	IP-Addresse des primären SIP Registrars

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	REGIP1	e	IP address of the primary SIP registrar
	REGIP2	d	IP-Addresse des sekundären SIP Registrars
	REGIP2	e	IP address of the secondary SIP registrar
	PORTTCP1	d	Port Nummer für die primäre SIP Registrierung über TCP/UDP
	PORTTCP1	e	Port number of the primary SIP registration via TCP/UDP
	PORTTCP2	d	Port Nummer für die sekundäre SIP Registrierung über TCP/UDP
	PORTTCP2	e	Port number of the secondary SIP registration via TCP/UDP
	REGTIME	d	Zeit in Sekunden wie lange die SIP-Registrierung gültig ist
	REGTIME	e	Time in seconds the SIP registration is valid
	SIPREG	d	Gateway an einem SIP Registrar registrieren
	SIPREG	e	Register gateway at a SIP registrar
	TRPRSIP	d	Anzahl der B-Kanäke für Trunking-Protokoll SIP
	TRPRSIP	e	Number of b channels for trunking protocol SIP
	TRPRSIPQ	d	Anzahl der B-Kanäke für Trunking-Protokoll SIP-Q
	TRPRSIPQ	e	Number of b channels for trunking protocol SIP-Q
	TYP=SIPTRSSA	d	SIP Trunking Daten für SSA (SIP Stack Agent)
	TYPE=SIPTRSSA	e	SIP trunking data for SSA (SIP Stack Agent)
	TYP=SIPTRERH	d	SIP Trunking Daten für ERH (Endpoint Registration Handler)
	TYPE=SIPTRERH	e	SIP trunking data for ERH (Endpoint Regustration Handler)

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	VAD	d	Voice Activity Detection
	VAD	e	Voice Activity Detection
GKREG	GWATTR	d	Gateway Attribut
	GWATTR	e	Gateway attribute
	GWNR	d	Gateway ID (muss dem Eintrag im AMO CGWB entsprechen)
	GWNO	e	Gateway ID (must correspond to the value in AMO CGWB)
TDCSU	DMCERL=NEIN	d	DMC wird verhindert
	DMCALLWD=NO	e	DMC not allowed
ZANDE	GATEKPR=JA	d	PBX mit Gatekeeper
	GATEKPR=YES	e	PBX with gatekeeper

14.6.2 Konfiguration mit Hilfe des OpenScape 4000 Assistant

14.6.2.1 Gateway HG 3500 konfigurieren

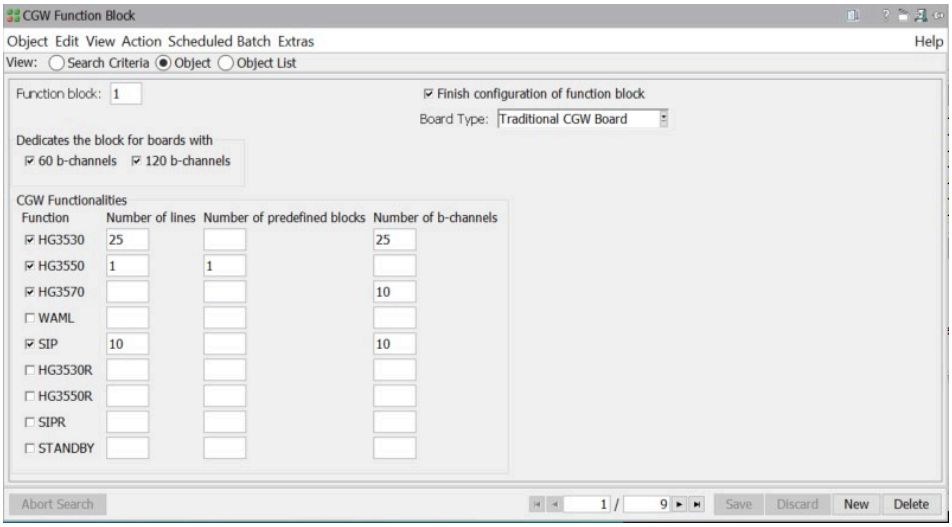
Um eine (v)HG 3500 zu konfigurieren, gehen Sie bitte folgendermaßen vor:

- Schritt 1: Funktionsblock erzeugen
- Schritt 2: Verfügbare Einbauteilung (EBT) suchen
- Schritt 3: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen
- Schritt 4: Neue Baugruppe hinzufügen
- Schritt 5: Maske ausfüllen
- Schritt 6: Dialog STMI2-IGW-Baugruppendaten öffnen und Pflichtfelder ausfüllen

Schritt 1: Funktionsblock erzeugen

Starten Sie **Configuration Management > Anlagendaten > Baugruppe > CGW-Funktionsblock**

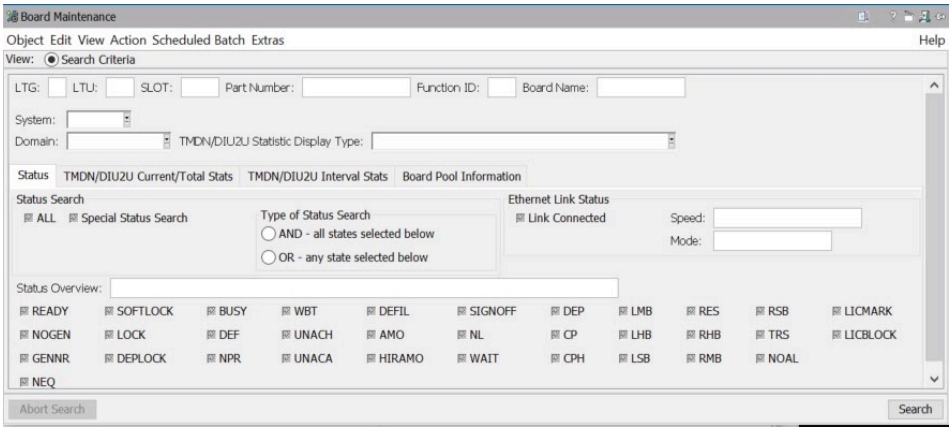
Suchen Sie nach einem freien Funktionsblock mit Hilfe der Schaltfläche **Suchen**. Um einen neuen Funktionsblock zu erzeugen, wählen Sie nun die Schaltfläche **Neu**. Geben Sie die erforderlichen Daten ein und speichern Sie diese mit der Schaltfläche **Sichern**.



Schritt 2: Verfügbare Einbauteilung (EBT) suchen

Vor der Eingabe von LTU- und EBT-Nummer sollten Sie erst prüfen, ob die gewünschte EBT auch verfügbar ist. Dafür rufen Sie bitte **CM > Anlagendaten > Wartung > BG-Wartung** auf.

Nach Abschluss der Suche in der Ansicht Objektliste sind in der Spalte **Statusübersicht** freie LTUs und Einbauteilungen mit **NOGEN/NPR/UNACH** gekennzeichnet.



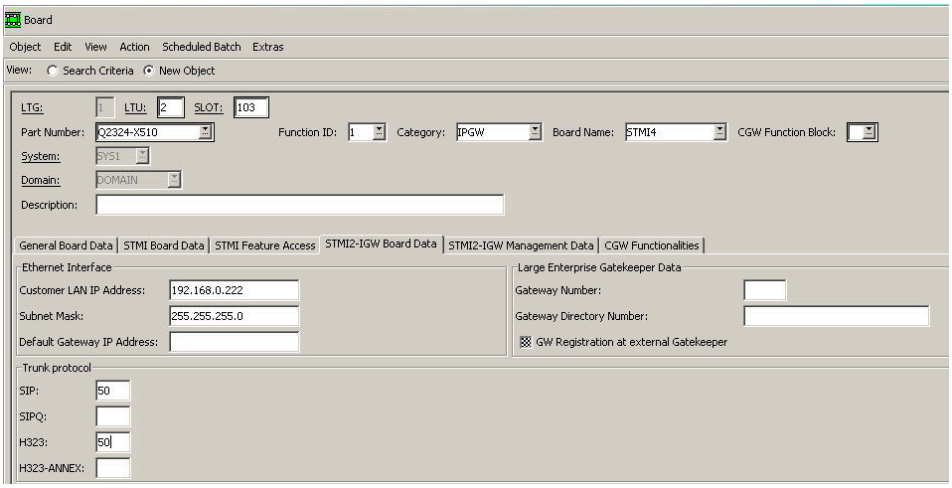
Schritt 3: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 4: Neue Baugruppe hinzufügen

Um die neue Baugruppe hinzuzufügen, klicken Sie auf die Schaltfläche **Neu**.

Schritt 5: Maske ausfüllen



- **Sachnummer**: Q2316-X oder Q2316-X10 oder Q2324-X500 oder Q2324-X510
- **Funktions-ID**: ist immer 1
- **Kategorie**: IPGW
- **BG-Name**: STMI2 oder STMI4
- **CGW-Funktionsblock**: geben Sie den zuvor erzeugten Funktionsblock für Trunking ein (siehe Schritt 1: Funktionsblock erzeugen)
- **LTU** und **EBT**: Wählen Sie eine verfügbare Einbauteilung (siehe Schritt 2: Verfügbare Einbauteilung (EBT) suchen)

Schritt 6: Dialog STMI2-IGW-Baugruppendaten öffnen und Pflichtfelder ausfüllen

IP-Adresse des Kunden-LAN und **Subnetzmaske**.

Amtsprotokoll: Anzahl der B-Kanäle pro Protokoll (z.B. **SIP/SIPQ**: 50).

Wichtig: Pro Baugruppe wird nur ein Amtsprotokoll unterstützt! Eine Kombination von mehreren Amtsprotokollen auf einer Baugruppe ist nicht möglich!

Nach Eingabe der Daten in die entsprechenden Felder bitte die Schaltfläche **Sichern** anklicken.

Die Baugruppe ist nun hinzugefügt und wird unter **Baugruppendialog** und **BG-Wartung** angezeigt.

14.6.2.2 IPGW löschen

Um eine IPGW-Baugruppe zu löschen, gehen Sie bitte folgendermaßen vor:

- Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen
- Schritt 2: Nach IPGW suchen
- Schritt 3: IPGW auswählen und löschen

Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 2: Nach IPGW suchen

Search Criteria > Kategorie: IPGW

Schritt 3: IPGW auswählen und löschen

Aus der Trefferliste zu löschendes Gateway aussuchen und Schaltfläche **Löschen** wählen. Nachdem die Schaltfläche **Löschen** betätigt wurde, erscheint eine Meldung, die die Entfernung der Baugruppe aus der Anlage bestätigt.

14.6.2.3 IPGW-Baugruppendaten ändern

Um die Daten einer IPGW-Baugruppe zu ändern, gehen Sie bitte folgendermaßen vor:

- Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen
- Schritt 2: IPGW auswählen
- Schritt 3: Gewünschte Änderungen durchführen
- Schritt 4: Überprüfung der Änderungen

Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 2: IPGW auswählen

In der Liste **Kategorie** bitte **IPGW** wählen und danach die Schaltfläche **Suche** anklicken.

Schritt 3: Gewünschte Änderungen durchführen

Gewünschte Änderungen (z.B. IP-Adresse) im Baugruppendialog durchführen und durch Anklicken der Schaltfläche **Speichern** sichern.

Nachdem die Änderungen gespeichert wurden, erscheint eine entsprechende Bestätigungsmeldung.

Schritt 4: Überprüfung der Änderungen

Führen Sie eine erneute Baugruppensuche durch, um zu überprüfen, ob die neuen Daten angenommen wurden.

14.6.3 Konfiguration mit Hilfe von SIP-Trunk-Profilen im WBM

siehe Abschnitt 3.3.5, „Konfiguration von SIP-Trunks mit Registrierung“

14.6.4 SIP-Q-Trunking zwischen OpenScape 4000 und OpenScape Voice

Über SIP-Q V2 Trunks kann eine Verbindung zwischen OpenScape 4000 und OpenScape Voice hergestellt werden.

Die OpenScape Voice stellt über diese Verbindung nur einen eingeschränkten Leistungsmerkmalumfang zu Verfügung. Details dazu entnehmen sie bitte der Dokumentation der OpenScape Voice.

Die Rufnummern zwischen OpenScape 4000 und OpenScape Voice müssen das Format **INTERNATIONAL** haben.

14.6.4.1 Einschränkungen

- Wahl mit Ziffernüberlappung wird bei OpenScape Voice nicht unterstützt (Unterstützung für überlappten Empfang)
- Bei einem OpenScape 4000 - OpenScape Voice (Transit) - OpenScape 4000-Szenario wird die Nachricht-wartet-Anzeige nicht über die OpenScape Voice geleitet.
- HG 3500 unterstützt keine Ziffernauthentifizierung.
- In einem HiPath 400-/OpenScape 4000-Netzwerk können die Payload-Partner mit DMC eingestellt werden. Ein OpenScape 4000-Telefon kann die Payload jedoch nicht direkt an den OpenScape Voice-Partner senden bzw. von ihm empfangen. Es kommt stets zu einem „Hop“ auf dem HG 3500-Modul.
- Wenn für die HG 3500 mehr als zwei Partner konfiguriert sind (z.B. Proxy) und **REGIP1** ausfällt, bleibt **REGIP2** registriert, bis **REGIP2** nicht mehr verfügbar ist. Eine automatische Rückschaltung auf **REGIP1** ist nicht möglich.

14.6.4.2 Konfiguration OpenScape 4000

Siehe auch „Abschnitt 6.1, „Konfiguration mit Hilfe von AMOs“.

Folgende Einstellungen müssen abweichend zu obiger Konfiguration durchgeführt werden:

- **Konfiguration der IP-Adresse**
- Die IP-Adresse (IPADR), die mit dem AMO CGWB konfiguriert ist, ist die IP-Adresse der OpenScape 4000. Die IP-Adresse muss die gleiche sein, wie der Aliasname in der OpenScape Voice.
- **Konfiguration der Gatewayrufnummer**
- Wenn man eine SIP-Q Trunking-Verbindung zu einem OpenScape Voice-System einrichten will, muss der Parameter **GWRNR** konfiguriert werden. Der Wert von **GWRNR** muss mit dem Alias Name in der OpenScape Voice übereinstimmen.

```
AEN-CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=LEGKDATA,GWNR=1,

GWRNR=816901;
```

- **Konfiguration des externen Registrars**

- Bei einer Trunking-Verbindung zu einer OpenScape Voice muss sich die OpenScape 4000 dynamisch beim OpenScape Voice-Partner-System registrieren. Hierfür muss ein externes Registrar eingerichtet werden.

  Die Konfiguration des externen Registrars erfolgt über den AMO CGWB.

  – Der Betrieb an einem externen Registrar (**SIPREG=JA**) muss aktiviert werden.
  – In **REGTIME** muss die Gültigkeitsdauer der Registrierung eingetragen werden. In die Felder **REGIP** (OpenScape Voice Adresse oder Proxy-Adresse) und **REGPORT** müssen die Daten des Registrars des Partnersystems eingetragen werden.

```
AEN-CGWB:MTYP=CGW,LTU=<ltu>,EBT=<ebt>,TYP=SIPTRSSA,

SIPREG=JA, REGIP1=127.28.45.54,PORTTCP1=5060,

REGTIME=<Sekunden>,REGIP2=0.0.0.0,PORTTCP2=5060;
```

  Im Parameter **REGTIME** akzeptiert die OpenScape Voice nur Werte, die größer als 300 Sekunden sind.

  – IM AMO CGWB muss der Parameter **REGEXTGK** auf JA gesetzt werden.

```
AEN-CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=LEGKDATA,GWNR=1,

GWRNR=816901,REGEXTGK=JA;
```

  Anmerkung: REGEXTGK kann auch auf NEIN gesetzt werden, jedoch muss dann ein GWNR hinzugefügt werden.

- **Konfiguration von Authentifizierung**
- Wenn die Authenfizierung im Partner-System aktiviert ist, müssen die Authentifizierungsdaten (SIP-UserId im Feld **GWUSERID**, Kennwort im Feld **GWSECRET** und **Realm** im Feld **GWREALM**) für die Registrierung am Partner-System konfiguriert werden. Das Senden der Authenfizierungsdaten kann mit dem Paramter **GWAUTREQ** ein- und ausgeschaltet werden.

```
AEN-CGWB:MTYP=CGW,LTU=<ltu>,EBT=<ebt>,TYP=SIPTRERH,

GWAUTREQ=JA,GWSECRET=<string>,GWUSERID=<string>,

GWREALM=<string>;
```

- **AMO TDCSU**
- – **DESTNO** darf nicht auf 0 eingestellt sein (der Wert 0 deaktiviert die Schleifenerkennung).
  – Setzen Sie den Parameter **TRACOUNT** auf die in Ihrem Netzwerk zulässige Anzahl von Hops.

```
EINRICHTEN-
TDCSU:ART=NEU,LAGE=1-01-037-0,COTNR=36,COPNR=32,

WABE=0,VBZ=0, COS=2,LCOSS=1,LCOSD=1,SATZNR="SATZ VON
 GW2", ZLNR=81,PROTVAR="EC►
MAV2",SEGMENT=8,
 ISDNIP=00,ISDNNP=0, TRACOUNT=10,SATCOUNT=VIELE,KNNR=1-69-
1499,ALARMNR=12,
 COTX=36,CCHDL=ASEITE,CLASSMRK=EC&G711,TCCID="IP TR",
```

```
BUNR=50,SUCHART=AB, INBETR=J,GER=HG3550IP,BKANAL=1&&30,
 BKVER=N,BKGR=1,LW►
PAR=0,DMCERL=J;
```

- **AMO COP**

```
EINRICHTEN-COP:COPNO=36,TOLL=TA,TRK=TA;
AENDERN-COP:COPNO=36,COPTYPE=COPADD,DEV=INDEP,

INFO="36: S0/2 QUER ECMA2 AB V3.0";
```

- **AMO COT**
- Überprüfen Sie außerdem, ob der COT-Parameter **TRCA** gesetzt ist.

```
EINRICHTEN-COT:COTNR=200,

PAR=RCL&UASE&MELD&AMGL&UELM&QUER&RRBN&RRFN&AWTE&ASAO&BLOC&LOKN&
NN&KLHT&OLRD&SPKN&GBNS&GBKI&NCDR&NOFT&VNCO&KTWM&NOSD&NPIS&PGEP&
NI&KTON&OSCV&AULN&RWSN;
AENDERN-COT:COTNR=200,COTTYP=COTZU,GER=UNAB,INFO="HP8K";
```

Hinweise:

– Wenn das gesamte Netzwerk e164-Nummerierung verwendet, muss für alle digitale Amtsleitungen der COT-Parameter **NPIS** gesetzt werden. Bei Verwendung des Rufnummernplans **UNKNOWN/UNKNOWN** sollte der Parameter **NPIS NICHT** gesetzt werden!

– Die COT-Parameter **AULN** und **FWAN** können Probleme verursachen, wenn nicht im gesamten Netzwerk ein konsistenter Rufnummernplan verwendet wird.

– Der COT-Parameter **OSCV** muss gesetzt werden.

- **Konfiguration von Blockwahl**
- Für die Trunkingverbindung zur OpenScape Voice muss Blockwahl eingestellt werden.
- **Hinweis für Inlands- und Ortsgespräche**
- Für OpenScape 4000-Benutzer ist auch die Anwahl mit nationaler Rufnummer sinnvoll. Beispiel: Der Anschluss +49(89)722-31256 ist unter den folgenden Nummern erreichbar:

31256	Wenn verdeckte Nummerierung konfiguriert ist
000498972231256	Immer
0-722-31256	Ortsgespräch
0-089-722-31256	Inlandsgespräch

Wenn die Orts- oder Inlandsanwahl von OpenScape 4000-Benutzern gewünscht wird, müssen einige weitere spezielle LCR-Konfigurationen vorgenommen werden. Diese Konfiguration ist nicht Gegenstand der vorliegenden Beschreibung, da sie für OpenScape Voice nicht relevant ist.

Beispiel für verdeckte Nummerierung:

Für die verdeckte Nummerierung muss auch das LCR konfiguriert werden.

Dies ist ein Beispiel für die Zielnummer **31256**.

DN **31256** bleibt für +49(89)722-31256

Verwenden Sie den e164-Rufnummernhaushalt für das OpenScape 4000 / OpenScape Voice-Interworking. In den internen ISDN-Meldungen sollte auch

der Anschluss des gerufenen Teilnehmers e164 mit der Rufnummernplan-ID ISDN verwenden.

Rufnummerntyp: INTERNATIONAL

Fehlende Ziffern müssen mit AMO LODR ##out pulse werden (z.B. 4989722).

AMO WABE definiert die Kennzahl

Beispiel für:

DN 31256 NETZRTG=224.

```
EINR-WABE:KZ=224,KZP=NETZRTG;
EINR-WABE:KZ=31256,KZP=TLN,CHECK=N;
AEND-WABE:KZ=31256,ZLRN=218;
```

AMO RICHT richtet das Bündel ein

Beispiel für:

KZ=224 (definiert mit AMO WABE) LRTG=224 (später mit AMO LDAT verwendet) BUNR=240 (vorkonfiguriert mit AMO BUEND)

```
EINR-RICHT:ART=KZ,LRTG=224,KZ=224,VKS=0,DIENST=ALLE,

NAME=âHP 8K MEDIATRIXâ,BUNU1=240,ZLNR=240,ZKNNR=218,

PZKNNR=1-1-218,ZEICHUM=NEUTRAL,KPRCAUL=NEIN,CLNAMEDL=NEIN;
AENDERN-RICHT:ART=KZ,KZ=224,VKS=0,DIENST=SPR,TYP=MFV,M

FVUMS=FIX,MFVPULS=PP300;
```

AMO LODR definiert die Wahlregel

Beispiel für:

LWR=240 (verwenden für AMO LDAT)

```
EINRICHTEN-LODR:LWR=240,LWREL=ZIFFSEND,ZIFFERN=4989722;

EINRICHTEN-LODR:LWR=240,LWREL=ECHOFELD,FELD=1;

EINRICHTEN-LODR:LWR=240,LWREL=NPI,NPI=ISDN,TON=INTERNAT;

EINRICHTEN-LODR:LWR=240,LWREL=ENDE;

EINRICHTEN-LODR:LWR=240,INFO=âHP8Kâ;
```

AMO LDAT definiert die LCR-Daten

Beispiel für:

TRRP240 (definiert mit AMO BUEND) LWR=240 (definiert mit AMO LODR) LRTG=224 (definiert mit AMO RICHT)

```
EINR-
LDAT:LRTG=224,LDIENST=ALLE,LWERT=1,BUNR=240,LWR=240,

LBER=16,CARRIER=1,ZONE=LEER,LATTR=DMCEND,VCCYK=4;
```

14.6.4.3 Konfiguration OpenScape Voice

Die Konfiguration der OpenScape Voice erfolgt über den OpenScape Voice Assistant.

In der OpenScape Voice müssen äquivalente Parameter konfiguriert werden. Folgende Daten müssen passend konfiguriert werden:

Konfiguration des Endpunktprofils

Das **Endpunktprofil** muss vor den **Endpunkten** erstellt werden.

Öffnen Sie die Liste der **Endpunktprofile** in OpenScape Voice Assistant mit **OpenScape Voice > Business Group > Available Private Numbering Plan = NP_Gateways > Profiles > Endpoint Profile**.

Wählen Sie in der Liste das entsprechende Endpunktprofil aus (z.B. HP4K), oder erstellen Sie ein neues Profil.

Register **General**:

- Endpoint Profile:
- – Name: HP4K
  – Remark: <optional>
  – Numbering Plan: NP_Gateways
- Management Information
- – Class of Service: international
  – Routing Area: H4K_Netz
  – Calling Location: <optional>
  – Time Zone: LOCAL
  – SIP Privacy Support: FULL
  – Failed Call Intercept Treatment: Enabled

  Register **Endpunkte**:

  In diesem Register finden Sie eine Liste der dem aktuellen Profil zugewiesenen Endpunkte.

  Register **Services**:
- Message Waiting: Yes
- Call Transfer: Yes
- Call forward Invalid Destination: No
- Toll and Call restrictions: No

Die Endpointdaten, welche die Verbindung zur OpenScape 4000 beschreiben

OpenScape Voice > Business Group > Members > Endpoints > Name

Register **General**:

Definition der Verbindungsdaten eines Endpunkts. Definieren Sie hier den **Namen** und das **Profil**.

Das Kontrollkästchen **Registered** ist automatisch aktiviert, wenn das CGW den Status **registered** aufweist.

Register **SIP**:

Konfiguration von IP-Adresse und Port des CGW und allgemeine Konfigurationen für SIP-Q.

- Wählen Sie die Optionsschaltfläche **SIP-Q Signaling**.

- **Geben Sie** (**Static**, **Dynamic**) ein:
- – Wird hier **Static** eingetragen, dann ist keine Registrierung der HG 3500 (SIP) erforderlich.
  – Wird **Dynamic** eingetragen, dann ist die Registrierung durch die HG 3500 (SIP) erforderlich.
- **Signaling Binding Address**: IP-Adresse des CGW (muss mit dem Parameter **IPADR** in AMO CGWB übereinstimmen)
- **Port**: (muss mit dem Parameter **PORTTCP2** in AMO CGWB übereinstimmen)
- **Transport protocol**: TCP

Register **Attributes**:

Setzen Sie **Support of Best Effort SRTP** (Unterstützung für Best-Effort-SRTP) auf **Enabled (Aktiviert – MIKEY, SDES, Automatic)** und aktivieren Sie das Kontrollkästchen neben **Enable Session Timer (Sitzungstimer aktivieren).**

Register **Aliases**:

Bei der Konfiguration des Endpoints, der die OpenScape 4000 darstellt (also HG 3500), müssen folgende Parameter mit den im AMO CGWB konfigurierten Daten korrespondieren:

- **Name**: Dieser Parameter muss mit dem Parameter **GWID1** übereinstimmen.
- **IP Address** of CGW: Dieser Parameter muss mit dem Parameter **IPADR** übereinstimmen.
- **Aliases**:

- Für dynamische Registrierung dient die ID des Gateways. Diese wird im AMO CGWB im Zweig **LEGKDATA** im Parameter **GWRNR** eingetragen.

  Setzen Sie die IP-Adresse für OpenScape 4000 auf „trusted“.

  OpenScape Voice > Administration > Signaling Management > Digest Authentication > Realms > Add

  Aktivieren Sie das Kontrollkästchen **Trusted Entry** , tragen Sie die IP-Adresse des CGW in das Feld **Signaling Primary** ein und wählen Sie **All Ports**.

  Signalisierungs- und Registrierungsparameter, welche die Daten für die Registrierung an der OpenScape Voice beschreiben (IP-Addresse, Port, Login)

  Die hier eingetragenen Daten müssen mit den im AMO CGWB eingetragenen Daten für ERH bzw. SSA übereinstimmen.

  Die Listening IP Address muss in der IP-Addresse des externen Registrars eingetragen werden.

  Der TCP/UDP Port muss im Feld **TCP/UDP Port** eingestellt werden.

  Die für die Authenfizierung eingestellten Daten (**UserID**, **Kennwort**, **Realm**) müssen mit den im AMO CGWB im Zweig Daten für SSA eingetragenen Daten übereinstimmen.

  Aliases:

  Für dynamische Registrierung dient die ID des Gateways. Diese wird im AMO CGWB im Zweig **LEGKDATA** im Parameter **GWRNR** eingetragen.

  Wichtig: Ausführlichere Informationen zur OpenScape Voice-seitigen Konfiguration finden Sie in der entsprechenden OpenScape Voice-Dokumentation.

14.6.5 Nummernmanagement zwischen OpenScape 4000 und OpenScape Voice für Italien

Auf Grund eines anderen Rufnummernformates der italienischen Mobiltelefone werden die Rufnummern in Richtung OpenScape Voice falsch modifiziert, wenn Sie die folgenden Einrichtungshinweise nicht beachten.

Szenario:

1. System A - OpenScape 4000

2. System B - OpenScape Voice

Kommender Amtsanruf zu OpenScape 4000 zu einem Teilnehmer in OpenScape Voice.

Voraussetzungen:

Alle Rufnummern die zur OpenScape Voice gesendet werden, müssen das Format **ISDN/INTERNATIONAL** haben.

Die OpenScape 4000 muss als italienisches System konfiguriert werden.

Generierung (Beispiel)

KZP=QUER in Richtung Amt konfigurieren:

```
EINRICHTEN-WABE:CD=901,DAR=TIE;
```

Eigene Richtung zum Amt für die italienischen Mobilrufnummern einrichten:

```
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=393,LDIENST=ALLE,

NAME=ITALIANMOBILE,BUNUM=XX,ZKNNR=1-1-393,ROUTOPT=NEIN,REROUT=NEIN,ZLN
SWTCH=JA;
EINRICHTEN-LODR:LWR=393,LWREL=ECHOFELD,FELD=3;
EINRICHTEN-LODR:LWR=393,LWREL=NPI,NPI=ISDN,TON=UNKNOWN;
EINRICHTEN-LODR:LWR=393,LWREL=ENDE;
EINRICHTEN-
LDAT:LRTG=393,LDIENST=ALLE,BUNUM=XX,LWR=393,LBER=1;
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=0-
W-3,LRTG=393,

LBER=1;
```

Eigene Richtung zum Amt für die italienischen Mobilrufnummern einrichten (wenn die Rufnummer mit Länderkenzeichen gewählt wird):

```
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=394,LDIENST=ALLE,

NAME=ITALIANMOBILE,BUNUM=XX,ZKNNR=1-1-393,ROUTOPT=NEIN,REROUT=NEIN,ZLN
SWTCH=JA;
EINRICHTEN-LODR:LWR=394,LWREL=ECHOFELD,FELD=4;
EINRICHTEN-LODR:LWR=394,LWREL=NPI,NPI=ISDN,TON=UNKNOWN;
EINRICHTEN-LODR:LWR=394,LWREL=ENDE;
EINR-LDAT:LRTG=394,LDIENST=ALLE,BUNR=xx,LWR=394,LBER=1;
EINR-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM=0-
W-0039-3,LRTG=394,

LBER=1;
```

KNDEF-Eintrag mit **TYP=FREMD** für die italienischen Mobilrufnummern erstellen:

```
EINRICHTEN-KNDEF:KNNR=1-1-393,TYP=FREMD,ISDNCC=39;
```

COT Parameter DCCO hinzufügen, um eine Knotennummer Ableitung zu ermöglichen:

```
AENDERN-COT:COTNU=YY,COTART=COTZU,COTPAR=DCCO;
```

14.7 Konfigurationsanleitung für OpenScape 4000/OpenScape Voice Networking

14.7.1 Allgemein

In diesem Dokument wird beschrieben, wie OpenScape 4000 und OpenScape Voice für die Vernetzung eingerichtet werden.

Eine detaillierte Beschreibung der spezifischen Einstellungen finden Sie in den Installationsschritten bzw. in der Servicedokumentation für OpenScape 4000 und OpenScape Voice.

14.7.2 Einleitung und Übersicht

- Das Modul HG 3500 ist Teil des OpenScape 4000 Systems. Hierbei handelt es sich um ein Peripherie-Gateway-Modul mit einer LAN-Schnittstelle zum OpenScape Voice-System.
- Das OpenScape 4000-System enthält einen Kundendatenspeicher. Diese Datenbank umfasst die Konfiguration für Trunks, Stationen und Funktionen.
- Die HG 3500-Baugruppe kann mit verschiedenen Parametern konfiguriert werden. Die HG 3500-Konfiguration muss mit der Konfiguration auf dem OpenScape Voice-System übereinstimmen.
- Zur Konfiguration im OpenScape 4000 System ist eine Schnittstelle für AMO-Befehle vorhanden.
- Dieses Dokument dient dem OpenScape 4000-Systemtechniker als Hilfe bei der Suche nach einer geeigneten Konfiguration.
- Weitere Einzelheiten hierzu finden Sie in der Servicedokumentation für das OpenScape 4000 System.

14.7.3 Anforderungen und freigegebene Kombinationen

OpenScape 4000

- Unterstützte Versionen
- HiPath 4000/OpenScape 4000 muss SIP-Q V2, d. h., HiPath 4000 V4 oder neuer unterstützen.
- Satzbaugruppen

Satzbaugruppen

Typ	Sachnummer
STMI2	Q2316-X oder Q2316-X10
STMI4[9]	Q2324-X500, Q2324-X510 oder Q2324-X511
vhg3500	Q2300-X
STMIX	Q2343-X

OpenScape Voice

- Unterstützte Versionen
- OpenScape Voice V5.0 und höher.

Erhältliche Kombinationen

Exakte Angaben zu den erhältlichen Kombinationen finden Sie unter „Vertriebsinformationen – Kompatibilitätsmatrix“. Dieses Dokument steht auf dem Unify Partnerportal zur Verfügung.

14.7.4 Konfiguration auf OpenScape 4000

[9] Hinweis: Für STMI4-Baugruppen muss die SENTA-Version 12 oder höher sein

14.7.4.1 Einstellungen für STMI2/STMI4

14.7.4.1.1 Zentrale Einstellungen in OpenScape 4000

- **GATEKPR=YES** von **CHANGE-ZANDE:TYPE=ALLDATA** wird in diesem Dokument verwendet. Wenn **GATEKPR=NO** definiert wird, sieht AMO CGWB geringfügig anders aus. Für diesen Parameter sind beide Konfigurationen in Ordnung.
- In einem HiPath 4000/OpenScape 4000-, HiPath 3000-Netzwerk empfehlen wir die E.164-Nummerierung für das gesamte Netzwerk. Fügen Sie danach bitte den COT-Parameter **NPIS** für jede digitale Leitung hinzu.
- Einstellungen für Modul in OpenScape 4000
- Bei diesem Beispiel ist die Satzbaugruppe an Stelle 1-2-4 installiert (d. h,. LTG=1, LTU=2, SLOT=4).

14.7.4.1.2 AMO-Konfigurationen

AMO BFDAT

```
ABFR-BFDAT:4;
H500:  AMO BFDAT STARTED
------------------------------------------------------------------------
| FCTBLK =  4    BRDBCHL : BCHL120              STATUS=
  OK               |
------------------------------------------------------------------------
|  1. FUNCT : HG3550       4 LINES    UNITS  3  BCHLCNT  30
  TOTAL BCHAN 120   |
------------------------------------------------------------------------
AMO-BFDAT-111       CONFIGURATION OF FUNCTIONAL BLOCKS FOR
 CGW BOARDS
EINRICHTEN-BFDAT:FCTBLK=4,FUNCTION=HG3550,BGBKAN=BKAN120;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=4,FUNCTION=HG3550,ANZSATZ=4,ANZEINH=3;
AENDERN-BFDAT:CONFIG=OK,FCTBLK=4,ANTW=JA;
```

AMO BCSU

```
ABFR-BCSU:TBL,1,2,4;
H500:  AMO BCSU  STARTED
 LTG  1  LTU 2   SRCGRP 1   ALARMNO-LTU 0

-----+----------+--------+---+-+-+---+-+------------
+------------+------------
     |          |        |   |S|H|AL-| |            |
       |
     | ASSIGNED  | MODULE |FCT|E|W|ARM| | INSERTED   |
 HW-     | MODULE
 PEN | MODULE    | TYPE   |ID |C|Y|NO | | MODULE     |STATE
 INFO  | STATUS
-----+----------+--------+---+-+-+---+-+------------
+------------+------------
   4 | Q2324-X510 STMI4      1   A   0| | Q2324-X510 |  1
 -12 -  | READY
     +--------------------------------+-+------------
+------------+------------
     | IP ADDRESS : 172. 29.136.200         B-CHANNELS :
 120    BCHLCNT : 120
     | BLOCK NO   :   4                     PRERESERVED
 LINES ASSIGNED :   NO
```

```
     |  1. FUNCT  : HG3550        4 LINES   B-CHANNELS :
 120    BCHLCNT : 120
     +--------------------------------+-+------------
+------------+------------
+----+----+---------------------------+-+------------
+------------+--------+
| NO SECURITY STATUS AVAILABLE, SINCE FEATURE SPE IS NOT
 ACTIVATED         |
+---------
+-----------------------------------------------------------------
+
AMO-BCSU -111       BOARD CONFIGURATION, SWITCHING UNIT

DISPLAY COMPLETED;
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=2,EBT=4,SACHNR="Q2324-
X510",FCTID=1,LW►
VAR="0",FCTBLK=4,BKAN3550=120,ALARMNR=0;
AMO TDCSU
ABFR-TDCSU:1-02-004-0;
H500:  AMO TDCSU STARTED
  +------------------------ DIGITAL TRUNK (FORMAT=L)
 -------------------------+
  | DEV      = HG3550IP      PEN      =  1-02-004-0   TGRP
    = 281          |

 |-----------------------------------------------------------------
  | PROTVAR  = ECMAV2        INS      = Y
 SRCHMODE = DSC          |
  | COTNO    = 200           COPNO    = 36            DPLN
    = 0            |
  | ITR      = 0             COS      = 1             LCOSV
    = 3            |
  | LCOSD    = 8             CCT      = OSV KN281
 DESTNO   = 81           |
  | SEGMENT  = 8             DEDSCC   =
 DEDSVC   = NONE         |
  | FACILITY =               DITIDX   =
 SRTIDX   =              |
  | TRTBL    = GDTR          SIDANI   = N
 ATNTYP   = TIE          |
  | CBMATTR  = NONE          NWMUXTIM = 10
 TCHARG   = N            |
  | SUPPRESS = 0             DGTPR    =
 CHIMAP   = N            |
  | ISDNIP   =               ISDNNP   =
                   |
  | PNPL2P   =               PNPL1P   =               PNPAC
    =              |
  | TRACOUNT = 10            SATCOUNT = MANY          NNO
    = 281          |
  | ALARMNO  = 0             FIDX     = 1
 CARRIER  = 1            |
  | ZONE     = EMPTY         COTX     = 200           FWDX
    = 10           |
  | DOMTYPE  =               DOMAINNO =
 TPROFNO  =              |
```

```
  | INIGHT    =                                          CCHDL
    =              |
  | UUSCCX    = 16            UUSCCY    = 8            FNIDX
    = 1            |
  | CLASSMRK = EC       & G711     & G729AOPT
 SRCGRP    = 1            |
  | TCCID     =
 SECLEVEL = TRADITIO      |

 |-------------------------------------------------------------------
  | BCNEG     = N           BCGR      = 1            LWPAR
    = 0            |
  | LWPP      = 0           LWLT      = 0            LWPS
    = 0            |
  | LWR1      = 0           LWR2      = 0
                   |
  | DMCALLWD = Y            VNNO      =
                   |
  | SVCDOM    =
                   |
  | BCHAN     =  1 && 30
                   |
  |
                   |

 +-------------------------------------------------------------------
+
  AMOUNT OF B-CHANNELS IN THIS DISPLAY-OUTPUT: 30
AMO-TDCSU-111       DIGITAL TRUNKS

DISPLAY COMPLETED;
EINRICHTEN-TDCSU:ART=NEU,LAGE=1-02-004-0,COTNR=200,CO►
PNR=36,WABE=0,VBZ=0,COS=1,LCOSS=3,LCOSD=8,SATZNR="O KN281
 ",ZLNR=81,PROT►
VAR="ECMAV2",SEGMENT=8,DEDSVC=KEINE,TRTBL=GDTR,SIDANI=N,TREFTYP=QUER,C
NE,TCHARG=N,ANZUNT=0,TRACOUNT=10,SATCOUNT=VIELE,KNNR=281,ALARMNR=0,FID
R=1,ZONE=LEER,COTX=200,AULX=10,CHIMAP=N,UUSCCX=16,UUSCCY=8,FNIDX=1,NWM
RCGRP=1,CLASSMRK=EC&G711&G729AOPT,BUNR=281,SUCHART=AB,INBETR=J,SECLEVE
,GER=HG3550IP,BCHAN=1&&30,BCNEG=N,BCGR=1,LWPP=0,LWLT=0,LWPS=0,LWR1=0,L
CALLWD=Y;
```

Hinweise:

- Stellen Sie sicher, dass **ZLNR** nicht 0 ist (mit dem Wert 0 wird die Schleifenerkennung deaktiviert).
- Bitte setzen Sie den Parameter **TRACOUNT** auf die Anzahl der Hops, die in Ihrem Netzwerk gültig sind. Bitte prüfen Sie auch, ob der COT-Parameter **ATRS** festgelegt ist (siehe auch Abschnitt 7.10, “Schleifenerkennung für OpenScape Voiceâ unten).

AMO BUEND

```
ABFR-BUEND:281;
H500:  AMO BUEND STARTED
+------------------------------ FORMAT = L
 ------------------------------------+
|  TGRP NUMBER :   281   TGRP NAME   : OSV IFS
 MAXIMUM NO.   :  120 |
```

```
|                        CHARCON     : NEUTRAL
                    |
|  SUBGROUP NO.:    10   DEVICE TYPE : HG3550IP
 TRACENO       :    0 |
|  SEARCH MODE : DESCENDING
 ACD THRESHOLD :    * |
|  NUMBER OF ASSOCIATED ROUTES       : 10
 PRIORITY      :    2 |
|  TDDRFLAG     :    ON  TDDRTHRESHOLD: 5
 SOURCEGROUPIDX :    1 |
|  GDTRRULE     :     0      ACDPMGRP : 0
                    |
|  THE FOLLOWING TRUNKS (LTG-LTU-SLOT-CCT) HAVE BEEN
 ALLOCATED:                 |
+-------------------------------------------------------------------
+
|   1- 2-  4-0           1 |  1- 2-  4-0           2 |  1-
 2-  4-0           3 |
|   1- 2-  4-0           4 |  1- 2-  4-0           5 |  1-
 2-  4-0           6 |
|   1- 2-  4-0           7 |  1- 2-  4-0           8 |  1-
 2-  4-0           9 |
|   1- 2-  4-0           10 |  1- 2-  4-0           11 |
 1- 2-  4-0
12 |
|   1- 2-  4-0          13 |  1- 2-  4-0          14 |  1-
 2-  4-0          15 |
|   1- 2-  4-0          16 |  1- 2-  4-0          17 |  1-
 2-  4-0          18 |
|   1- 2-  4-0          19 |  1- 2-  4-0          20 |  1-
 2-  4-0          21 |
|   1- 2-  4-0          22 |  1- 2-  4-0          23 |  1-
 2-  4-0          24 |
|   1- 2-  4-0          25 |  1- 2-  4-0          26 |  1-
 2-  4-0          27 |
|   1- 2-  4-0          28 |  1- 2-  4-0          29 |  1-
 2-  4-0          30 |
|   1- 2-  4-1           1 |  1- 2-  4-1           2 |  1-
 2-  4-1           3 |
|   1- 2-  4-1           4 |  1- 2-  4-1           5 |  1-
 2-  4-1           6 |
|   1- 2-  4-1           7 |  1- 2-  4-1           8 |  1-
 2-  4-1           9 |
|   1- 2-  4-1          10 |  1- 2-  4-1          11 |  1-
 2-  4-1          12 |
|   1- 2-  4-1          13 |  1- 2-  4-1          14 |  1-
 2-  4-1          15 |
|   1- 2-  4-1          16 |  1- 2-  4-1          17 |  1-
 2-  4-1          18 |
|   1- 2-  4-1          19 |  1- 2-  4-1          20 |  1-
 2-  4-1          21 |
|   1- 2-  4-1          22 |  1- 2-  4-1          23 |  1-
 2-  4-1          24 |
|   1- 2-  4-1          25 |  1- 2-  4-1          26 |  1-
 2-  4-1          27 |
```

```
|   1- 2-  4-1          28 |  1- 2-  4-1          29 |  1-
 2-  4-1          30 |
|   1- 2-  4-2           1 |  1- 2-  4-2           2 |  1-
 2-  4-2           3 |
|   1- 2-  4-2           4 |  1- 2-  4-2           5 |  1-
 2-  4-2           6 |
|   1- 2-  4-2           7 |  1- 2-  4-2           8 |  1-
 2-  4-2           9 |
|   1- 2-  4-2          10 |  1- 2-  4-2          11 |  1-
 2-  4-2          12 |
|   1- 2-  4-2          13 |  1- 2-  4-2          14 |  1-
 2-  4-2          15 |
|   1- 2-  4-2          16 |  1- 2-  4-2          17 |  1-
 2-  4-2          18 |
|   1- 2-  4-2          19 |  1- 2-  4-2          20 |  1-
 2-  4-2          21 |
|   1- 2-  4-2          22 |  1- 2-  4-2          23 |  1-
 2-  4-2          24 |
|   1- 2-  4-2          25 |  1- 2-  4-2          26 |  1-
 2-  4-2          27 |
|   1- 2-  4-2          28 |  1- 2-  4-2          29 |  1-
 2-  4-2          30 |
|   1- 2-  4-3           1 |  1- 2-  4-3           2 |  1-
 2-  4-3           3 |
|   1- 2-  4-3           4 |  1- 2-  4-3           5 |  1-
 2-  4-3           6 |
|   1- 2-  4-3           7 |  1- 2-  4-3           8 |  1-
 2-  4-3           9 |
|   1- 2-  4-3          10 |  1- 2-  4-3          11 |  1-
 2-  4-3          12 |
|   1- 2-  4-3          13 |  1- 2-  4-3          14 |  1-
 2-  4-3          15 |
|   1- 2-  4-3          16 |  1- 2-  4-3          17 |  1-
 2-  4-3          18 |
|   1- 2-  4-3          19 |  1- 2-  4-3          20 |  1-
 2-  4-3          21 |
|   1- 2-  4-3          22 |  1- 2-  4-3          23 |  1-
 2-  4-3          24 |
|   1- 2-  4-3          25 |  1- 2-  4-3          26 |  1-
 2-  4-3          27 |
|   1- 2-  4-3          28 |  1- 2-  4-3          29 |  1-
 2-  4-3          30 |
+-------------------------------------------------------------------------
+
AMO-BUEND-111       TRUNK GROUP

DISPLAY COMPLETED;
EINRICHTEN-BUEND:BUNUM=281,NAME="OSV IFS
 ",ANZ=120,ANZFANG=0,AN►
ZACD=*,PRIONUM=2,TDDRFLAG=ON,GDTRRGL=0,ACDPMGRP=0,ZEICHUM=NEUTRAL;
```

AMO COP

```
ABFR-COP:36;
   COP:  36  INFO: 36: S0/2 QUER ECMA2 AB V3.0
   DEVICE: S2CONN       SOURCE: DB
```

```
   PARAMETER:
```

AMTSBERECHTIGUNG:	
AMTSZUGANG	TA
FERNBERECHTIGUNG:	
AMTSZUGANG	TA

```
EINRICHTEN-COP:COPNU=36,BERAMT=FBKW,BERFERN=FBKW;
AENDERN-COP:COPNU=36,COPART=COPZU,GER=S2VERB,INFO="36: S0/2
 QUER ECMA2 AB V3.0";
```

AMO COT

Die folgenden COT-Parameter wurden getestet und werden empfohlen.

```
ABFR-COT:200;
H500:  AMO COT   STARTED
   COT: 200  INFO: OSV STANDARD COT
   DEVICE: INDEP        SOURCE: DB
   PARAMETER:
```

WIEDERANRUF WENN BENUTZER BEIM MAKELN AUFLEGT	RCL
UMLEITEN EXTERNER VERBINDUNG	UMLEITEN
AMTSLEITUNG SIGNALISIERUNG ANTWORT	ANTW
AUFSCHALTEN MÖGLICH	KNOR
CALL EXTEND FOR BUSY, RING OR CALL STATE	CEBC
NETWORKWIDE AUTOMATIC CALLBACK ON BUSY	CBBN
NETWORKWIDE AUTOMATIC CALLBACK ON FREE	CBFN
NETZWEITE ANRUFUMLEITUNG ERLAUBT	FWDN (*1)
NETZWEITE ANRUFUMLEITUNG BEI KEINE ANTWORT	FNAN (*1)
REGENERATED CO DIALTONE ON OUTGOING SEIZURE	COTN
DON'T RELEASE CALL TO BUSY HUNT GROUP	BSHT
CAMP-ON DID CALLS	KNDI (*2)
END-OF-DIAL FOR IS SET	BLOCK
SEND NO NODE NUMBER TO PARTNER	LWNC
ACTIVATE TRANSIT COUNTER ADMINISTRATION FOR S0/ S2 LINE	ATRS
CONNECTION TO ROUTE OPTIMIZATION NODE	ROPT
TSC-SIGNALING FOR NETWORKWIDE FEATURES (MANDATORY)	TSCS
USE DEFAULT NODE NUMBER OF TRUNK	DFNN (*3)
NO LOCAL HOLDTONE, HOLDTONE FROM REMOTE SYSTEM	NLHT
SEND NO BILLINGELEMENTS	SNBE
GEBÜHREN KOMMEND IGNORIEREN	IICB
SIGNALISIERUNG VON CDR-E-SPEZIFISCHEN MELDUNGEN UNTERDRÜCKEN.	NCDR
SATZ GESPERRT FÜR FLAG-TRACE.	NOFT
SENDEN DER VIRTUELLEN RUFNUMMER ZUM EXTERNEN NETZ.	VNCO
KEIN EINFACHER DIALOG VORHANDEN	NOSD
NPI ISDN, ABGEHENDER VERKEHR	NPIS (*4)
SEND DIGITS VIA IN.BAND DTMF BEFORE ANSWER	IBBA
PREVENT NODE INFORMATION	PRNI
OPENSCAPE VOICE INTERWORKING	OSCV
NO TONE	NTON

RECALL IF USER HANGS UP IN CONSULTATION CALL
RCL

```
UMLEITEN EXTERNER VERBINDUNG  &nbspXFER

TRUNK SIGNALING ANSWER
   ANS

KNOCKING OVERRIDE POSSIBLE KNOR

CALL EXTEND FOR BUSY, RING OR CALL STATE CEBC

NETWORKWIDE AUTOMATIC CALLBACK ON BUSY CBBN

NETWORKWIDE AUTOMATIC CALLBACK ON FREE CBFN

NETWORKWIDE CALL FORWARDING PERMITTED FWDN (*1)

NETWORKWIDE FORWARDING NO-ANSWER FNAN (*1)
REGENERATED CO DIALTONE ON OUTGOING SEIZURE COTN
DON'T RELEASE CALL TO BUSY HUNT GROUP  BSHT
CAMP-ON DID CALLS KNDI (*2)
END-OF-DIAL FOR BLOCK IS SET BLOC
SEND NO NODE NUMBER TO PARTNER  LWNC
ACTIVATE TRANSIT COUNTER ADMINISTRATION FOR S0/S2 LINE ATRS
CONNECTION TO ROUTE OPTIMIZATION NODE  ROPT
TSC-SIGNALING FOR NETWORKWIDE FEATURES (MANDATORY) TSCS
USE DEFAULT NODE NUMBER OF TRUNK  DFNN (*3)
NO LOCAL HOLDTONE, HOLDTONE FROM REMOTE SYSTEM NLHT
SEND NO BILLINGELEMENTS SNBE
IGNORE INCOMING BILLING IICB
SUPPRESS SIGNALING OF CDR-E SPECIFIC MESSAGES NCDR
NO FLAG TRACE NOFT
SEND VIRTUAL SUBSCRIBER NUMBER TO CO VNCO
NO SIMPLE DIALOG AVAILABLE NOSD
NPI ISDN, OUTGOING CALL NPIS (*4)
SEND DIGITS VIA IN.BAND DTMF BEFORE ANSWER IBBA
PREVENT NODE INFORMATION PRNI
OPENSCAPE VOICE INTERWORKING OSCV
NO TONE NTON
AMO-COT  -111       CLASS OF TRUNK FOR CALL PROCESSING

DISPLAY COMPLETED;
EINRICHTEN-
COT:COTNU=200,COTPAR=AERF&UASE&MVLT&AMGL&UELM&RRBN&RRFN&AWTE&SAAO
&ROPT&TSCS&VKNN&KLHT&GBNS&GBKI&NCDR&NOFT&VNCO&NOSD&NPIS&IBBA&PRNI
CV&RWSN;
AENDERN-COT:COTNU=200,COTART=COTZU,GER=UNAB,INFO="OSV
 STANDARD COT";
```

Hinweise:

- (* 1) COT-Parameter **FWDN** und **FWAN** können Probleme verursachen, wenn im gesamten Netzwerk kein einheitlicher Nummerierungsplan verwendet wird.
- (* 2) **KNDI**, damit Netzwerkanrufe bei einem Anruf von DDI automatisch an die Station gekoppelt werden können.

- (* 3) **DFNN** wird nicht unbedingt benötigt. Ohne den Parameter werden Knoteninformationen über LCR von der Anrufernummer abgeleitet. Wenn keine Route konfiguriert ist, wird der Knoten (**NNO**) von AMO TDCSU übernommen. **DFNN** wird oft von Technikern festgelegt, sodass immer der AMO TDCSU **NNO** verwendet wird.
- (*4) Wenn das gesamte Netzwerk (HiPath 4000/OpenScape 4000, HiPath 3000, OpenScape Voice) die E.164-Nummerierung verwendet und der COT-Parameter **NPIS** für jede digitale Leitung festgelegt ist. Wird der Nummerierungsplan **UNKNOWN/UNKNOWN** verwendet, ist**NPIS NICHT** festzulegen.
- Der COT-Parameter **NOTO** ist nicht zu setzen. Ab OpenScape Voice V5 gibt OpenScape 4000 Töne auch bei Fortschrittsnachrichten wieder (verzögerte Trennung).
- Setzen Sie den Parameter **TRACOUNT** (mit AMO TDCSU) auf die Anzahl der Hops, die in Ihrem Netzwerk gültig sind (siehe Abschnitt AMO TDCSU).
- **SECO** muss unter Umständen für US-Konfigurationen festgelegt werden, damit E911 einwandfrei funktioniert.
- Weitere Informationen finden Sie unter:

  https://gsikm-productive.unify.com/rkm/viewdoc.jsp?doc=209494

  AMO CGWB

```
ABFR-CGWB:2,4;
H500:  AMO CGWB  STARTED
------------------------------------------------------------------------

|  CGW BOARD DATA
                      |
------------------------------------------------------------------------

|   HG3550
                      |
------------------------------------------------------------------------

|  LTU = 2       SLOT = 4      SMODE = NORMAL
 POOLNO: 0            |
------------------------------------------------------------------------
  GLOBAL DATA AND ETHERNET INTERFACE DATA - CONFIGURABLE
 VALUES:

 ------------------------------------------------------------
  IPADR     = 10.237.88.122       // eigene Adresse
                                  // config OSV ->
 Endpoint-> alias
                                      TCPP   =
 (4060)
  NETMASK   = 255.255.255.192         VLAN   = NO
 (NO)
  DEFRT     = 172.29 .136.193         (0.0.0.0 = NOT
 CONFIGURED)
  BITRATE   =          (CHECK OS)     VLANID = 0      (0)
  PATTERN   = 213 (213)
  TRPRSIP   = 0   (0)
  TRPRSIPQ  = 120 (0)                  // Anzahl
 verfügbarer SIPQ-Trunks
```

```
 TRPRH323  = 0   (0)                // Kanal, abhängig
von DMC-Verfügbarkeit
 TPRH323A = 0   (0)
 TLSP   = 4060  (4061)
 GLOBAL DATA - CONSTANT VALUES:
 ------------------------------
 AMO INTERFACE VERSION: 0      OPMODE: 1   DATA_VALID:
YES
 DNSIPADR  = 10.237.1.3
 DNSIPADR2  = 0.0.0.0
 SERVICE INTERFACE
 -----------------
 LOGINTRM = "TRM" (TRM)
 PASSW    = *****
 ASC DATA - CONFIGURABLE VALUES:
 ------------------------------
 TOSPL    = 184   (184)     TOSSIGNL = 104   (104)
 UDPPRTLO = 29100 (29100)  UDPPRTHI = 30099 (30099)
 T38FAX   = YES   (YES)    REDRFCTN = YES   (YES)
 RFCFMOIP = YES   (YES)    RFCDTMF  = YES   (YES)
 PRIO1 :  CODEC = G711A   VAD = NEIN   RTP-SIZE = 20
 // RTP-SIZE 20
                  // falls die Funktion DECT IP oder
 OSCMC bereits an einem Ort
im Netzwerk vorhanden sind
 PRIO2 :  CODEC = G711U   VAD = NEIN   RTP-SIZE = 20
 PRIO3 :  CODEC = G729A   VAD = NEIN   RTP-SIZE = 20
 PRIO4 :  CODEC = G723    VAD = NEIN   RTP-SIZE = 30
 PRIO5 :  CODEC = NONE    VAD = NEIN   RTP-SIZE = 20
 PRIO6 :  CODEC = NONE    VAD = NEIN   RTP-SIZE = 20
 PRIO7 :  CODEC = G729AB  VAD = JA     RTP-SIZE = 20
 DSP CONFIGURATION DATA
 ----------------------
 JITBUFD  = 60   (60) (PAREMERTER IS NOT USED ANYMORE)
 MANAGEMENT STATION AND BACK-UP SERVER
 -------------------------------------
 MGNTIP = 10.237.80.50 (0.0.0.0) // Adresse von
OpenScape 4000 Assistant
 MGNTPN    = 8000 (8000)
 BUSIP     = 10.237.80.50 (0.0.0.0)    // Adresse von
OpenScape 4000 Assistant
 BUSPN     = 443 (443)
 UIMODE    = CLASSIC (CLASSIC
 DMC DATA
 --------
 DMCCONN = 90 (0) // Höchstwert für DMC
 WBM LOGIN DATA
 --------------
 LOGINWBM  = HP4K-DEVEL   ROLE  = ENGR (ADMIN)
 LOGINWBM  = HP4K-SU      ROLE  = SU (ADMIN)
 LOGINWBM  = HP4K-ADMIN   ROLE  = ADMIN (ADMIN)
 LOGINWBM  = HP4K-READER  ROLE  = READONLY (ADMIN)
 GATEWAY DATA
 ------------
 GWID1     = GW1
 GWID2     =
```

```
  H.235 SECURITY DATA
  -------------------
  GLOBID1   = Gateway2003
              (Gateway2003)
  GLOBID2   =
  TIMEWIN   = 100  (100)
  SECSUBS   = YES   (NO)                // YES für
 SECURE NO für TCP
  SECTRNK   = YES   (NO)                // YES für
 SECURE NO für TCP
  GLOBPW    =
 242-191-30-119-188-83-173-161-43-0-70-36-218-74-169-221-78-102-
174-170
  LEGK DATA
  -----------------
  GWNO      =  (0)
  GWDIRNO   = 166                        //
 Konfiguration OSV-> Endpunkt ->
Alias
  REGEXTGK  = YES (NO)                  // Yes für
 Registration, NO für DNS-SRV
  SIP TRUNKING DATA FOR  ERH
  --------------------------
  GWAUTREQ    = NO (NO)
  GWSECRET    = *****
  GWUSERID    =
  GWREALM     =
  SIP TRUNKING DATA FOR  SSA
  --------------------------
  SIPREG  = YES (NO)                  // Yes für
 Registration, NO für DNS-SRV
  REGIP1      = 10.237.81.104 (0.0.0.0)     // OSV
 Node-1 oder Proxy-Adresse
                                        // sipsm1 OSV
 (wenn TCP)
                                       // sipsm3 OSV-
Cluster (wenn TLS)
  PORTTCP1    = 5060 (5060)
  PORTTLS1    = 5061  (5061)
  REGIP2      = 10.237.84.104 (0.0.0.0)       // OSV
 Node-2, falls geo-getrennt
                                        // OSV
 Node-1, wenn Proxy konfigu►
riert ist
                                        // sipsm2
 OSV (wenn TCP)
                                        // sipsm4
 OSV-Cluster (wenn TLS)
  PORTTCP2    = 5060 (5060)
  PORTTLS2    = 5061 (5061)
  REGTIME     = 300  (120)               // Wert >= 300
  DLS DATA
  ------------------------------------
  DLSIPADR  = 0.0.0.0
  DLSPORT   = 18443
  DLSACPAS  = NO
```

```
  JB DATA - CONFIGURABLE VALUES:
  ------------------------------
  JBMODE    = 2
  AVGDLYV   = 40  (40)
  MAXDLYV = 120 (120) MINDLYV = 20 (20)
  PACKLOSS  = 4   (4)
  AVGDLYD   = 60  (60)  MAXDLYD = 200 (200)
IP CONFIGURATION
  ------------------------------------
  IPMODE    = IPV4 (IPV4)
  DHCPV4    = NO (NO)
  DHCPV6    = NO (NO)
  MANAGEMENT LAN INTERFACE DATA - CONFIGURABLE VALUES:

 ------------------------------------------------------------------
  MIPADR    = 0  .0  .0  .0          MNETMASK   = 0  .0
  .0  .0
  MVLAN     = NO     (NO)            MVLANID    = 0
 (0)
  MDEFRT    = 0  .0  .0  .0          (0.0.0.0 = NOT
 CONFIGURED)
AMO-CGWB -111       CONFIGURATION OF HG3500 BOARD
DISPLAY COMPLETED;
  <
EINRICHTEN-
CGWB:LTU=2,EBT=4,SMODE=NORMAL,IPADR=172.29.136.200,NET►
MASK=255.255.255.192;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=GLOBIF,MUSTER=213,VLAN=NEIN,VLANI
=172.29.136.193,BITRATE="AUTONEG",TRPRSIP=0,TRPRSIPQ=120,TR►
PRH323=0,TPRH323A=0,TLSP=4061,DNSIPADR=0.0.0.0,DNSIPAD2=0.0.0.0
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=SERVIF,LOGINTRM="TRM";
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,UDPPRTLO=29100,UDPPRTHI=30099
="184",TOSSIGNL="104",T38FAX=NEIN,RFCFMOIP=JA,RFC►
DTMF=JA,REDRFCTN=JA,PRIO=PRIO1,CODEC=G711A,VAD=NEIN,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO2,CO►
DEC=G711U,VAD=NEIN,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO3,CO►
DEC=G729A,VAD=NEIN,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO4,CO►
DEC=G723,VAD=NEIN,RTP="30";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO5,CO►
DEC=NONE,VAD=NEIN,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO6,CO►
DEC=NONE,VAD=NEIN,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=ASC,PRIO=PRIO7,CO►
DEC=G729AB,VAD=JA,RTP="20";
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=DSP,JITBUFD="60";
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=GKDATA,PRIGKPN=1719,PRIGKID1="PRI
,SECGKPN=1719,SECGKID1="SECONDARYRASMANAGERID",TIMTLIVE=120;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=MGNTDATA,MGNTIP=172.29.136.242,MG
PN=8000,BUSIP=172.29.136.242,BUSPN=443;
```

```
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=DMCDATA,DMCCONN=90;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=WBMDATA,LOGINWBM="HP4K-
DEVEL",ROLE=ENGR;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=WBMDATA,LOGINWBM="HP4K-
SU",ROLE=SU;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=WBMDATA,LOGINWBM="HP4K-
ADMIN",ROLE=ADMIN;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=WBMDATA,LOGINWBM="HP4K-
READ►
ER",ROLE=READONLY;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=H235DATA,SECSUBS=NEIN,SECTRNK=NEIN,GL
BID1="Gateway2003",TIMEWIN=100,GLOBPW=242-191-30-119-188-83-173-161
218-74-169-221-78-102-174-170;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=LEGKDATA,GWRNR=166,REGEXTGK=JA;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=SIPTRERH,GWAUTREQ=NEIN,GWUSERID="sipq
REALM="mchh";
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=SIPTRSSA,SIPREG=JA,REGIP1=172.29.132.
5060,PORTTLS1=5061,REGTIME=300,REGIP2=0.0.0.0,PORTTCP2=5060,PORTTLS
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=DLSDATA,DLSIPADR=172.29.128.156,DL►
SPORT=18443,DLSACPAS=NEIN;
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=4,TYP=JB,AVGDLYV=40,MAXDLYV=120,MINDLYV=20,
LOSS=4,AVGDLYD=60,MAXDLYD=200,JBMODE=2;
```

14.7.4.1.3 Umleitung an ein OpenScape-Voice-System

Für die Nummerierung zwischen OpenScape 4000 und und OpenScape Voice ist die internationale Nummernwahl zu wählen.

Angaben zur Umleitungskonfiguration für OpenScape 4000 finden Sie in der Servicedokumentation im Abschnitt *OpenScape 4000, Band 3: Anwendungsfälle für Leistungsmerkmale*.

14.7.4.1.4 Hinweis zu nationalen und lokalen Rufnummern

Für OpenScape 4000-Teilnehmer ist die Verwendung von nationalen Rufnummern ebenfalls sinnvoll.

Beispielsweise ist die Station +49(89)722-31256 erreichbar über die Nummer

31256	// Falls die geschlossene Nummerierung konfiguriert ist
000498972231256	// immer
0-722-31256	// lokale Wahl
0-089-722-31256	// nationale Rufnummer

Wenn die lokale oder nationale Wahl von OpenScape 4000-Benutzern angefordert wird, ist eine besondere zusätzliche Konfiguration erforderlich. Diese Konfiguration ist nicht Bestandteil dieser Beschreibung, da diese in Bezug auf OpenScape Voice nicht erforderlich ist. Siehe Servicedokumentation **OpenScape 4000, Band 3, Anwendungsfälle für Leistungsmerkmale**.

Beispiel: Verdeckte Nummerierung

Auch für die geschlossene Nummerierung muss LCR für die internationale Wahl konfiguriert werden (siehe Abschnitt 7.9, “OpenScape Voice-Richtung für die internationale Wahl – Rufnummern auf internationale Nummer erweiternâ).

Hier ist ein Beispiel für die Zielnummer DN=31256. DN=31256 bleibt für +49(89)722-31256

Verwenden Sie das E.164-Nummerierungsschema für die gemeinsame Verwendung von OpenScape 4000 und OpenScape Voice.

Bei internen ISDN-Nachrichten sollte selbst die angerufene Nummer E.164 verwenden mit

1) Nummerierungsplankennung: ISDN

und

1) Nummerntyp: INTERNATIONAL.

Stellen Sie sicher, dass fehlende Stellen mit AMO LODR ausgegeben werden (z. B `EINR-LODR=xxx,CMD=OUTPULSE,DGTS=4989722;`). AMO WABE definiert den Zugangscode.

Beispiel für AMO WABE mit Zielnummer 31256 und **NETZRTG=224**:

```
EINRICHTEN-WABE:RNR=224,KZP=NETZRTG;
ABFRAGEN-WABE:TYP=ALLG,RNR=224;
H500:  AMO WABE  STARTED

 ------------------------------------------------------------------
  | DIGIT INTERPRETATION                    VALID FOR ALL
 DIAL PLANS            |

 ------------------------------------------------------------------
  |                  |    CALL PROGRESS STATE     |NODE/
DIGIT| RESERVED/CONVERT |
  |      CODE        |            1 11111 11112 22| ANALYSIS
 | DNI/ADD-INFO      |
  |                  |0 12345 67890 12345 67890 12|  RESULT
 | *=OWN NODE        |

 ------------------------------------------------------------------
  | 224              |* ..... ..... ..... ..... ..| NETRTE
 |                   |

 ------------------------------------------------------------------
AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES

DISPLAY COMPLETED;
EINRICHTEN-WABE:RNR=31256,KZP=TLN,PRUEF=NEIN;
AENDERN-WABE:RNR=31256,ZLNR=218;
ABFRAGEN-WABE:TYP=ALLG,RNR=31256;
H500:  AMO WABE  STARTED
```

```
 ------------------------------------------------------------------------
  | DIGIT INTERPRETATION                    VALID FOR ALL
 DIAL PLANS            |

 ------------------------------------------------------------------------
  |                   |    CALL PROGRESS STATE     |  DIGIT
 | RESERVED/CONVERT  |
  |      CODE         |            1 11111 11112 22| ANALYSIS
 | DNI/ADD-INFO      |
  |                   |0 12345 67890 12345 67890 12|  RESULT
 | *=OWN NODE        |

 ------------------------------------------------------------------------
  | 31256             |. .**** ***** **... ..... .*| STN
 |                   |
  |                   |                            |
 |DESTNO 218         |
  |                   |                            |
 |DNNO    0-  0-218  |
  |                   |                            |
 |PDNNO   1-  1-218  |

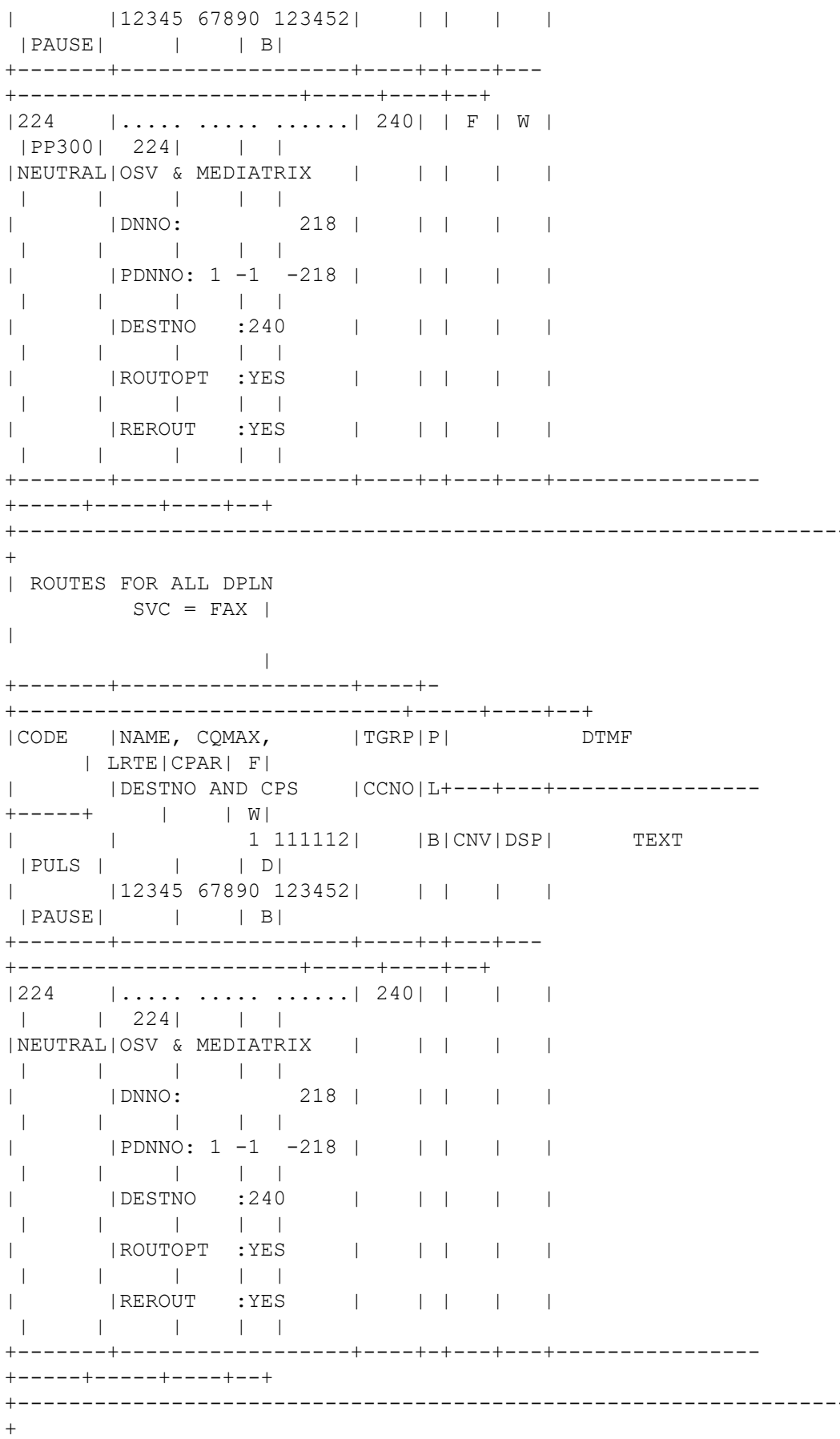
 ------------------------------------------------------------------------
AMO-WABE -111       DIALLING PLANS, FEATURE ACCESS CODES

DISPLAY COMPLETED;
```

AMO RICHT wird zur Vorbereitung von Bündeln verwendet.

Beispiel für AMO RICHT mit **KZ=224** (definiert mit AMO WABE), **LRTG=224** (später verwendet mit AMO LDAT) und **ZLNR=240** (vorkonfiguriert mit AMO BUEND)

```
EINRICHTEN-
RICHT:ART=KZ,LRTG=224,KZ=224,VKS=0,DIENST=ALLE,NAME="OSV &
 MEDIA►
TRIX",BUNU1=240,ZLNR=240,ZKNNR=218,PZKNNR=1-1-218,ZEICHUM=NEUTRAL,KPR►
CAUL=NEIN,CLNAMEDL=NEIN;
AENDERN-
RICHT:ART=KZ,KZ=224,VKS=0,DIENST=SPR,TYP=MFV,MFVUMS=FIX,MFVPULS=PP300;
ABFRAGEN-RICHT:ART=KZ,KZ=224,VKS=0;
H500:  AMO RICHT STARTED
+------------------------------------------------------------------------
+
| ROUTES FOR ALL DPLN
          SVC = VCE |
|
                    |
+-------+-----------------+----+-
+-----------------------------+-----+----+--+
|CODE   |NAME, CQMAX,      |TGRP|P|          DTMF
      | LRTE|CPAR| F|
|       |DESTNO AND CPS    |CCNO|L+---+---+----------------
+-----+     |    | W|
|       |          1 111112|    |B|CNV|DSP|      TEXT
 |PULS |     |    | D|
```


|PAUSE|
|224
|PP300|
|NEUTRAL|
|DNNO:
|PDNNO: 1 -1 -218
|DESTNO :240
|ROUTOPT :YES
|REROUT :YES
ROUTES FOR ALL DPLN
SVC = FAX
|CODE
|NAME, CQMAX,
|DESTNO AND CPS
|TGRP|P|
DTMF
|CCNO|L
|CNV|DSP|
TEXT
|PULS
|12345 67890 123452|
|OSV & MEDIATRIX
218
1 111112
B
D
W

```
| ROUTES FOR ALL DPLN
          SVC = DTE |
|
                    |
+-------+-----------------+----+-
+-------------------------------+-----+----+--+
|CODE   |NAME, CQMAX,      |TGRP|P|          DTMF
      | LRTE|CPAR| F|
|       |DESTNO AND CPS    |CCNO|L+---+---+---------------
+-----+     |    | W|
|       |          1 111112|    |B|CNV|DSP|      TEXT
 |PULS |     |    | D|
|       |12345 67890 123452|    | |   |   |
 |PAUSE|     |    | B|
+-------+-----------------+----+-+---+---
+----------------------+-----+----+--+
|224    |..... ..... ......| 240| |   |   |
 |     |  224|    |  |
|NEUTRAL|OSV & MEDIATRIX   |    | |   |   |
 |     |     |    |  |
|       |DNNO:         218 |    | |   |   |
 |     |     |    |  |
|       |PDNNO: 1 -1  -218 |    | |   |   |
 |     |     |    |  |
|       |DESTNO   :240     |    | |   |   |
 |     |     |    |  |
|       |ROUTOPT  :YES     |    | |   |   |
 |     |     |    |  |
|       |REROUT   :YES     |    | |   |   |
 |     |     |    |  |
+-------+-----------------+----+-+---+---+---------------
+-----+-----+----+--+
AMO-RICHT-111       TRUNK ROUTING

DISPLAY COMPLETED;
```

AMO LODR definiert die Wahlregel.

Beispiel für AMO LODR mit **LWR=240** (Verwendung mit AMO LDAT).

```
EINRICHTEN-LODR:LWR=240,LWREL=ZIFFSEND,ZIFFERN=4989722;
EINRICHTEN-LODR:LWR=240,LWREL=ECHOFELD,FELD=1;
EINRICHTEN-LODR:LWR=240,LWREL=NPI,NPI=ISDN,TON=INTERNAT;
EINRICHTEN-LODR:LWR=240,LWREL=ENDE;
EINRICHTEN-LODR:LWR=240,INFO="OSV";
ABFRAGEN-LODR:LWR=240;
H500:  AMO LODR  STARTED
   +-------------------------------------------------------
+
   |  ODR     POSITION  CMD         PARAMETER
 |
   +--------+-----------------------------------------------
+
   |  240   |      1    OUTPULSE    4989722
 |
   |        |      2    ECHO        1
 |
```

```
   |        |      3    NPI         ISDN
 |
   |        |      4    TON         INTERNAT
 |
   |        |      5    END
 |
   +--------+-------------------------------------------------
+
   |INFO:OSV
 |
   +-------------------------------------------------------
+
H03: THE NEXT FREE ODR IS 2
AMO-LODR -111       ADMINISTRATION OF LCR OUTDIAL RULES

DISPLAY COMPLETED;
```

AMO LDAT definiert die Mindestkosten für Umleitungsdaten.

Beispiel für AMO LDAT mit **BUNUM=240** (definiert mit AMO BUEND), **LWR=240** (definiert mit AMO LODR) und **LRTG=224** (definiert mit AMO RICHT)

```
EINRICHTEN-
LDAT:LRTG=224,LDIENST=ALLE,LWERT=1,BUNUM=240,LWR=240,LBER=16,CARR
ER=1,ZONE=LEER,VCCYK=4;
ABFRAGEN-LDAT:TYP=ALLE,LRTG=224;
H500:  AMO LDAT  STARTED
+-------------------------------------------------------------------
+
| LROUTE = 224                NAME = OSV & MEDIATRIX
     SERVICE =  ALL |
| TYPE = NWLCR                                  DNNO OF
 ROUTE  =        218    |
| SERVICE INFO =
                     |
+------+-----+-----+----+-----+----------+-----------
+----------+------+-------+
|      |     |     |    |     | SCHEDULE | CARRIER   |
     |      |       |
|LRTEL | LVAL|TGRP | ODR|LAUTH| ABCDEFGH |       ZONE|
 LATTR | LDSRT|COTIDX |
+------+-----+-----+----+-----+----------+-----------
+----------+------+-------+
|     1|    1|  240| 240|16   | ******** | 1    EMPTY|
     |      | 0     |
+-------------------------------------------------------------------
+
AMO-LDAT -111       LCR-DIRECTIONS

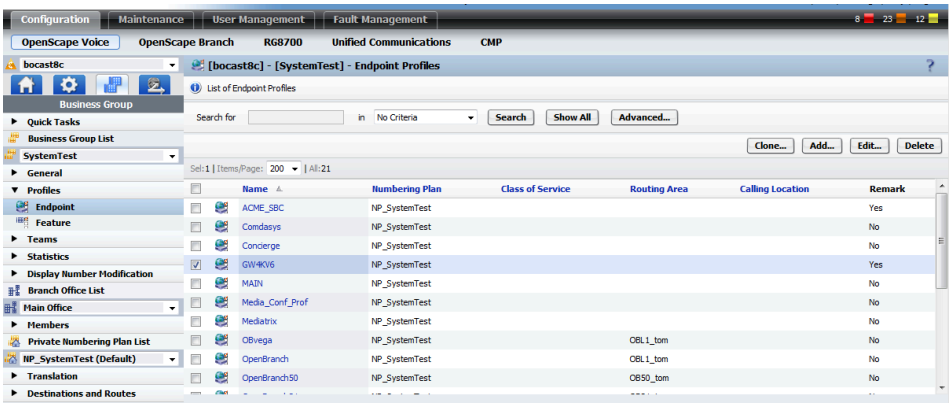
DISPLAY COMPLETED;
```

14.7.5 Konfiguration für OpenScape Voice

Die folgenden Abschnitte beschreiben die Trunking-Konfiguration für OpenScape 4000 auf Seite von OpenScape Voice.

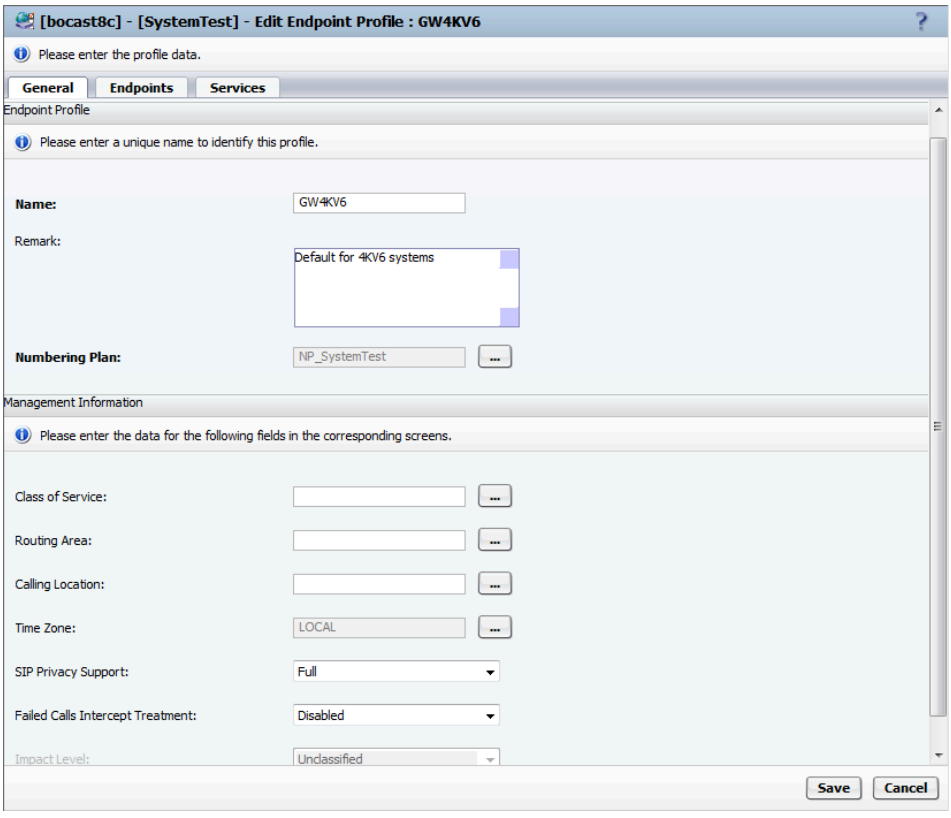
14.7.5.1 OpenScape Voice Endpoint Profile

Common Management Platform > OpenScape Voice > Business Group > Profiles > Endpoint Profile



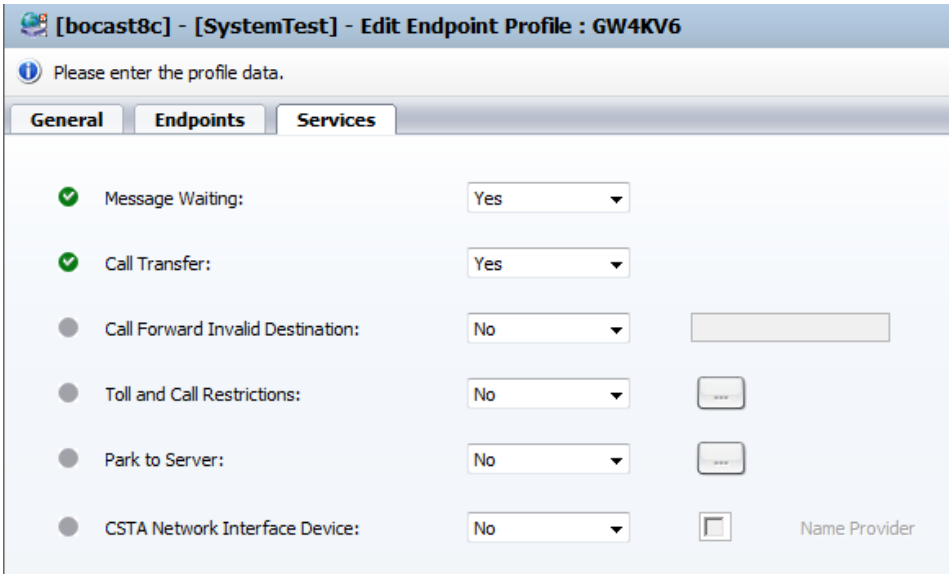
OpenScape Voice: Endpoint Profile-Konfiguration

Endpoint Profile-Ordner **General**:



OpenScape Voice: Endpoint-Ordner „“

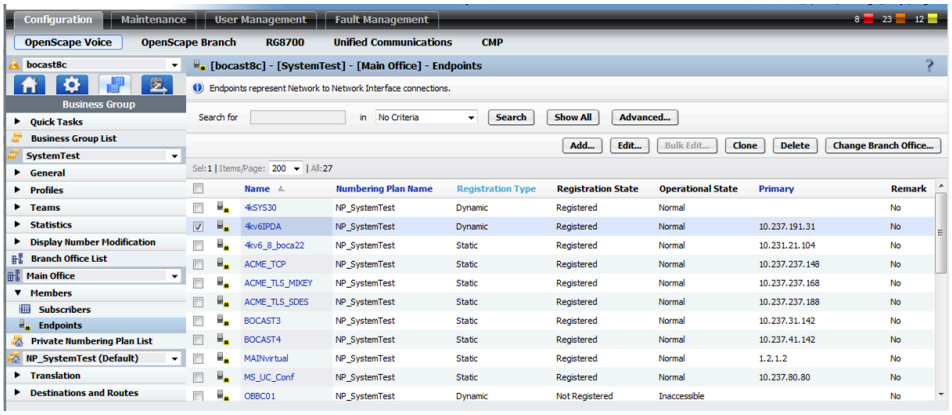
Endpoint Profile-Ordner **Services**:



OpenScape Voice Endpoint-Ordner „Services“

14.7.5.2 OpenScape Voice Endpoint

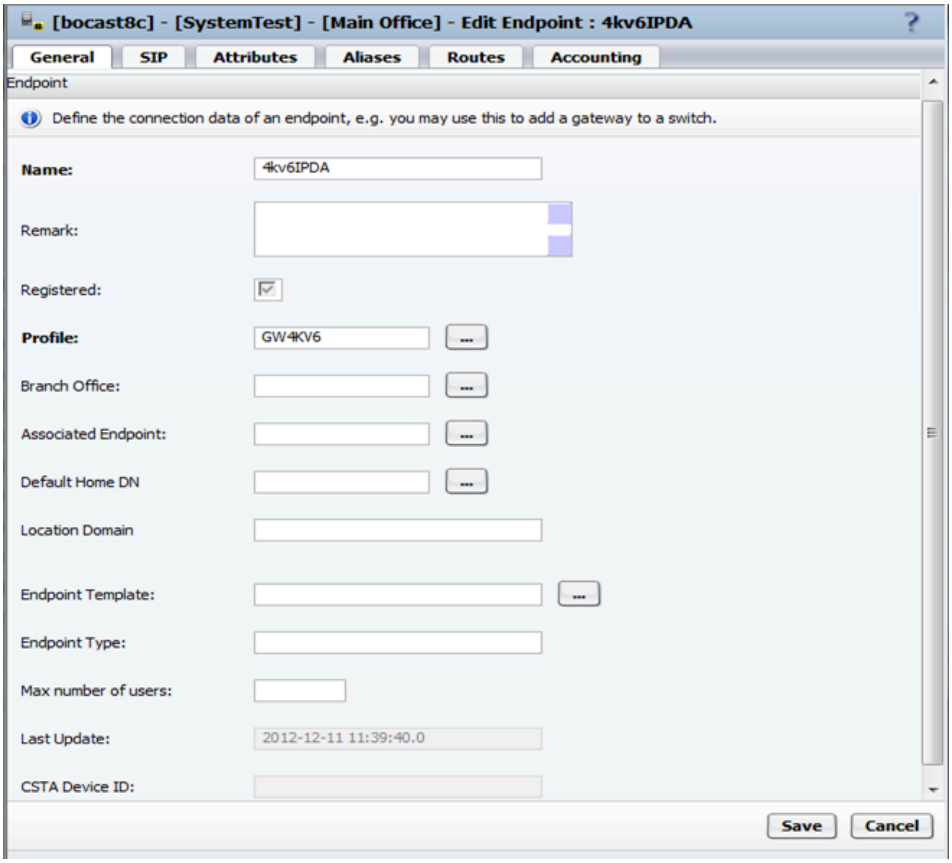
Common Management Portal > OpenScape Voice > Business Group > Main Office > Members > Endpoints > Name (z. B. 4kv6IPDA)



OpenScape Voice: Endpoint-Konfiguration

Endpoint zu OpenScape 4000-Ordner „General“:

Namensdefinition und Profil:

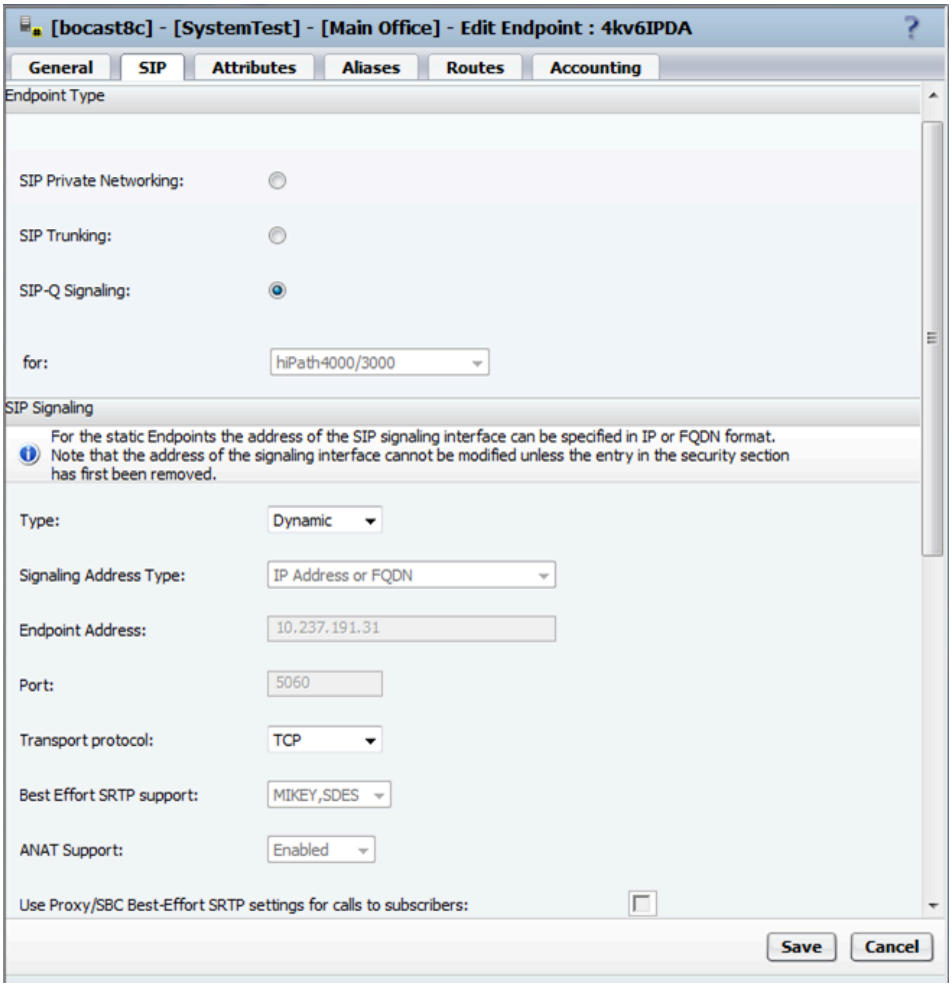


OpenScape Voice Endpoint zu OpenScape 4000-Ordner „General“

Das Kontrollkästchen **Registered** wird automatisch angezeigt, wenn für HG 35xx **Dynamic** definiert ist und der Status **Registered** lautet.

Endpoint-Anforderungen zu OpenScape 4000-Ordner „SIP“:

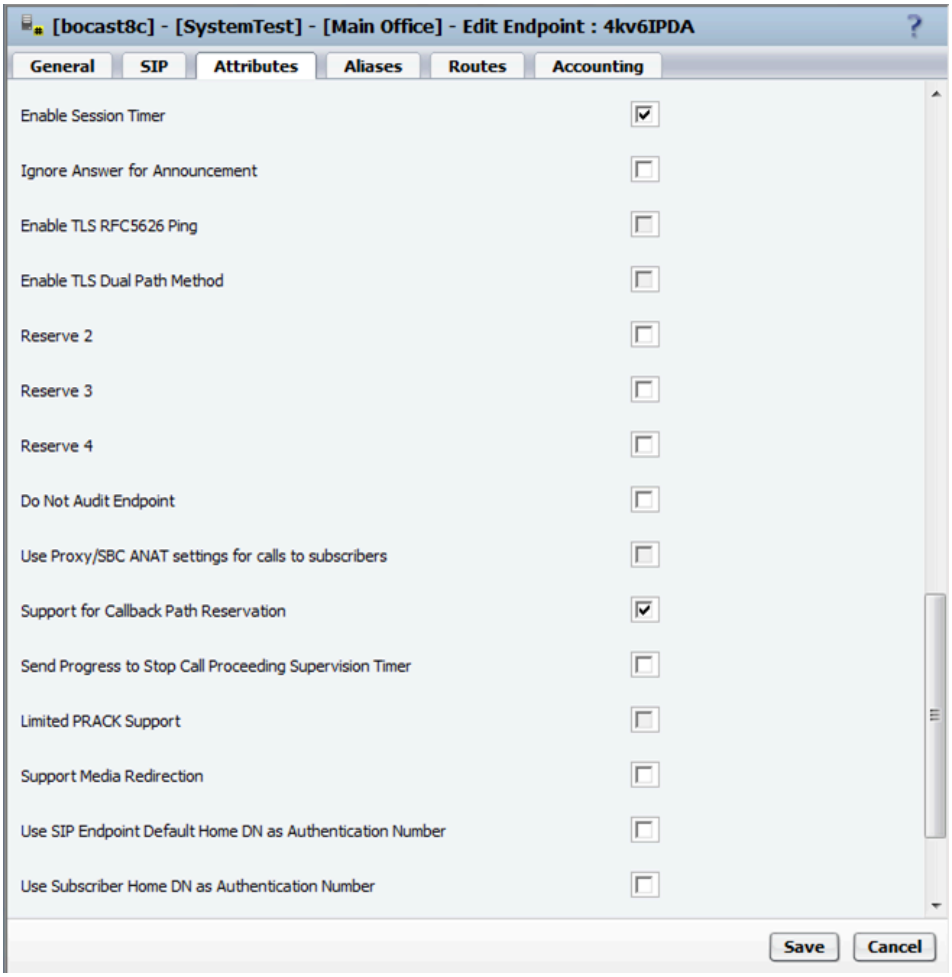
- **SIP-Q Signaling** (über Optionsfeld aktivieren)
- IP-Adresse für HG 35xx (**Endpoint Address**)
- **Transport protocol** (TCP)



OpenScape Voice Endpoint zu OpenScape 4000-Ordner „SIP“

Endpoint zu OpenScape 4000-Ordner „General“:

Es ist nur **Enable Session Timer** erforderlich.



OpenScape Voice Endpoint zu OpenScape 4000-Ordner „Attributes“

Wichtig: Unterstützung für **Callback Path Reservation** ist für Unified Communication besonders wichtig.

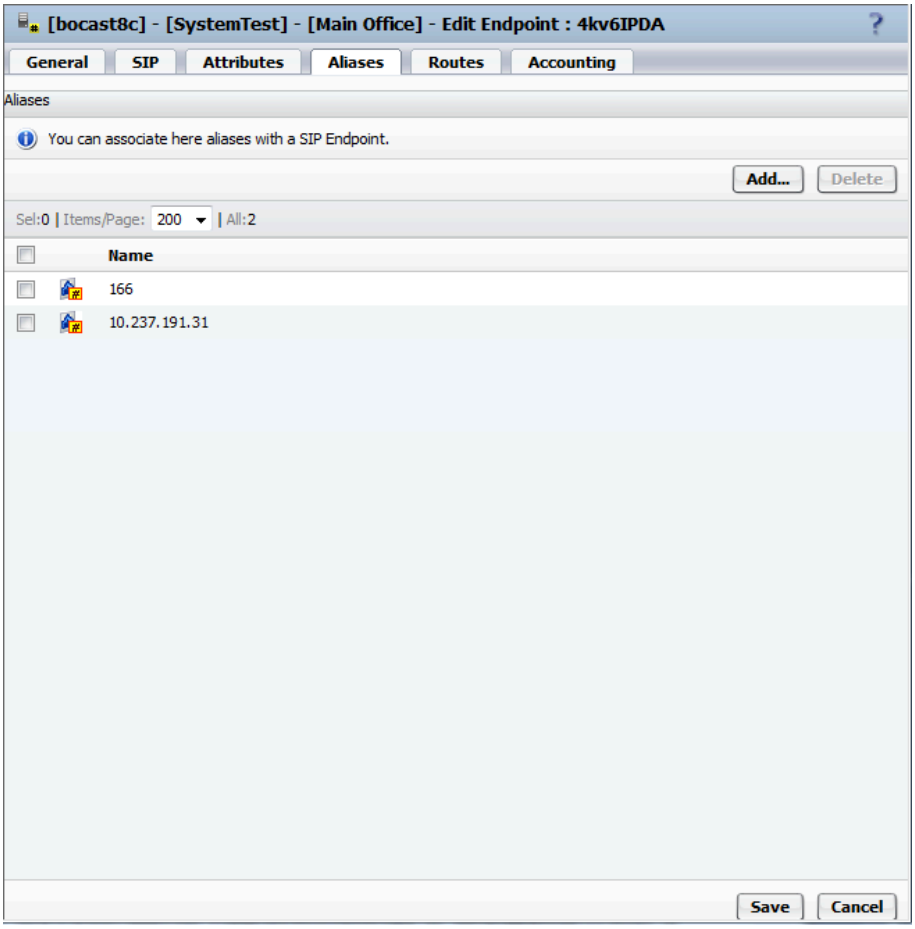
Endpoint zu OpenScape 4000-Ordner „Aliases“:

Fügen Sie die IP-Adresse von HG 35xx aus OpenScape 4000 ein, z. B.:

1) 10.237.191.31 (mit AMO CGWB auf Seiten von OpenScape 4000 prüfen).

Fügen Sie den Parameter **GWRNR** von OpenScape 4000 ein, z. B.

166 (mit AMO CGWB auf Seiten von OpenScape 4000 prüfen).



OpenScape Voice Endpoint zu OpenScape 4000-Ordner „Aliases“

Alle diese Namen sind in OpenScape 4000 mit AMO CGWB definiert.

IP-Adresse für HG 35xx:

```
EINRICHTEN-
CGWB:LTU=22,EBT=2,SMODE=NORMAL,IPADR=10.237.191.31,NET▶
MASK=255.255.255.0;
```

HG 3550 LEGKDATA für **GWRNR** und **REGEXTGK**:

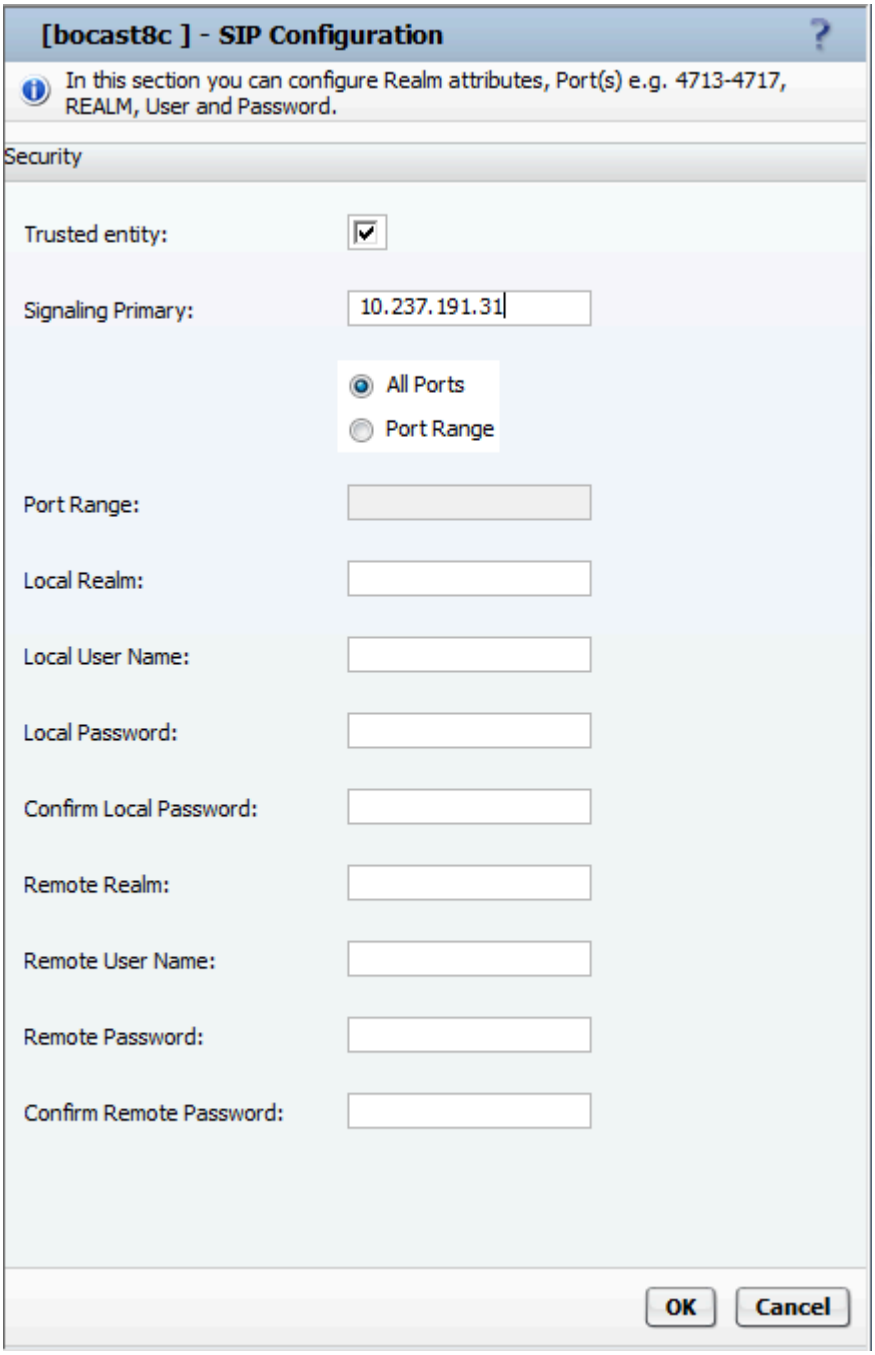
```
AENDERN-
CGWB:MTYP=CGW,LTU=22,EBT=2,TYP=LEGKDATA,GWRNR=166,REGEXTGK=JA;
```

Anmerkung: REGEXTGK kann auch auf NEIN gesetzt werden, jedoch muss dann ein GWNR hinzugefügt werden.

14.7.5.3 IP-Adresse für OpenScape 4000 im Fall der Digest-Authentifizierung als vertrauenswürdig einstufen

Common Management Portal > OpenScape Voice > Administration > Signaling Management > Digest Authentication > Realms > Add

Aktivieren Sie das Kontrollkästchen **Trusted Entity** und geben Sie die IP-Adresse für **Signalling Primary**ein (z. B. 10.237.191.31 (HG 35xx von OpenScape 4000))



OpenScape Voice: IP-Adresse für OpenScape 4000 als vertrauenswürdig einstufen

14.7.6 DNS-SRV für HG 3500

AMO CGWB erfordert die folgenden Elemente:

Konfigurieren Sie die IP-Adresse des DNS-SRV-Servers (**DNSIPADR**) in **TYP=GLOBIF**.

```
AENDERN-
CGWB:MTYP=CGW,LTU=22,EBT=5,TYP=GLOBIF,DNSIPADR=10.237.1.3;
```

Konfigurieren Sie den Parameter **GWDRNR** in **TYP=LEGKDATA**, der auch für **Account Name** im SIP-Amtsleitungsprofil verwendet wird.

```
AENDERN-
CGWB:MTYP=CGW,LTU=22,EBT=5,TYP=LEGKDATA,GWRNR=166,REGEXTGK=NEIN;
```

Anmerkung: REGEXTGK kann auch auf NEIN gesetzt werden, jedoch muss dann ein GWNR hinzugefügt werden.

Konfigurieren Sie **SIPREG=NEIN** in **TYP=SIPTRSSA** für die Verwendung des SIP-Amtsleitungsprofils.

```
AENDERN-
CGWB:MTYP=CGW,LTU=22,EBT=5,TYP=SIPTRSSA,SIPREG=NEIN;
```

Wichtig: Für DNS-SRV muss das SIP-Amtsleitungsprofil **SIPQTrkWithRegistration** aus der Web-Schnittstelle des Gateways verwendet werden.

14.7.6.1 Beispiel einer Web-Schnittstelle für Geo-Separated OpenScape Voice mit TLS-Konfiguration

WBM > Explorers > Voice Gateway > SIP Trunk Profile Parameter

Use Profiles for Trunks via SIP-Q muss aktiviert/auf **Yes** gesetzt werden.



Abbildung 244: OpenScape 4000: Profile für SIP-Leitungen verwenden

DNS-SVR-Einträge:

nd08a.st.lz.com führt zu

sipsm3 auf node1

sipsm4 auf node2.

WBM > Explorers > Voice Gateway > SIP Trunk Profiles

Verwenden Sie DNS-SRV-Hostnamen für Registrar- und Proxy-Adressen, und legen Sie Port=0 fest.

SIP Transport Protocol ist nicht konfigurierbar. Der Abschnitt **Security** befindet sich am unteren Rand des Pulldown-Bereichs und wird verwendet, um die Parameter MIKEY bzw. SDES festzulegen, wenn SPE verwendet werden soll.

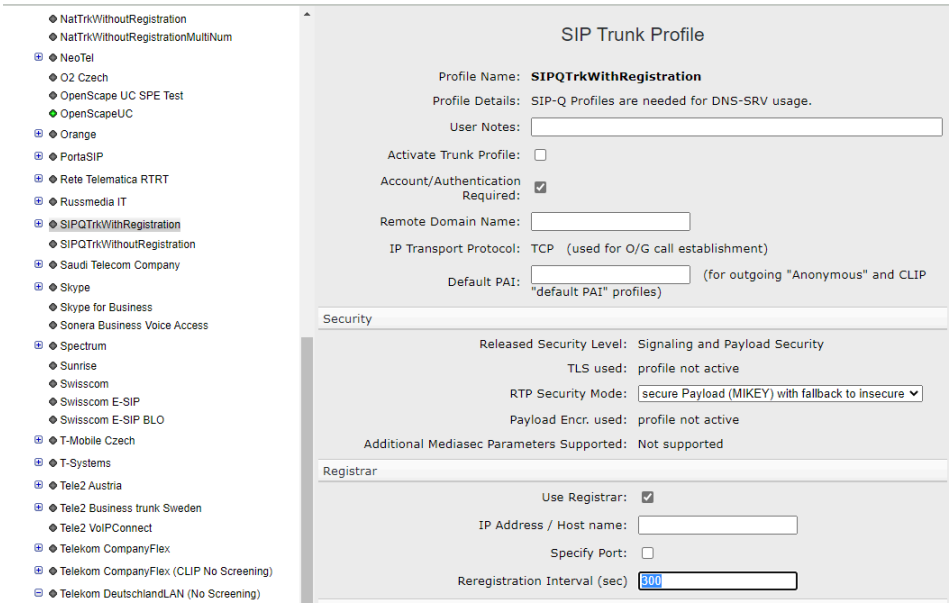


Abbildung 245: OpenScape 4000: Eigenschaften des SIP-Amtsleitungsprofils „SIPQTrkWithRegistration“

WBM > Explorers > Voice Gateway > SIP Trunk Profiles > SIPQTrkWith Registration

Bearbeiten Sie den Parameter **Account Name** (wie AMO CGWB Parameter **GWDIRNO**) und wenden Sie ihn an.

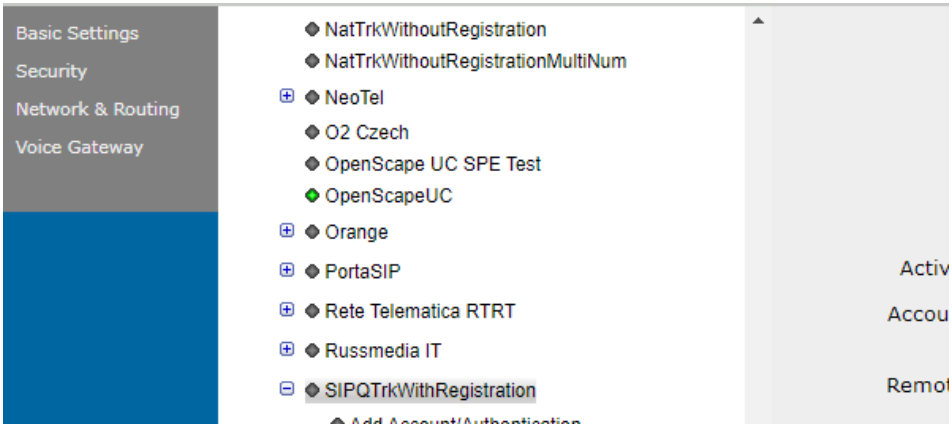


Abbildung 246: OpenScape 4000: Bearbeiten des Kontonamens

Klicken Sie nun mit der rechten Maustaste auf **SIPQTrkWithRegistration**, um das Profil zu aktivieren. Der Ordner wird ROT dargestellt, wenn er nicht für OpenScape Voice oder OpenScape Branch registriert ist. Er wird GRÜN

angezeigt, wenn die Registrierung erfolgreich war.

14.7.6.2 Beispiel für Branch mit Geo-Separated OpenScape Voice und TLS

In Branch-Szenarien (mit Survivability-Proxy, wie OpenScape Branch oder Comdasys) können zwei DNS-Server-Einträge vohanden sein: jeweils einen für den lokalen und den zentralen Branch-Proxy. Geben Sie die DNS-Server

in AMO CGWB unter den Parametern **DNSIPADR** und **DNSIPADR2** an. Beim vorliegenden Bespiel ist für das Netzwerk nur ein DNS-Server vorhanden.

DNS-SVR-Einträge:

br08a2.st.lz.com führt zu:

Branch-Proxy

Sipsm3 auf node1

Sipsm4 auf node2.

nd08a.st.lz.com führt zu:

Sipsm3 auf node1

Sipsm4 auf node2.

WBM > Explorers > Voice Gateway > SIP Trunk Profiles > SIPQTrkWith Registration

Abschnitt **Outbound Proxy**:

Aktivieren Sie das Kontrollkästchen **Use Outbound Proxy** und geben Sie den DNS-SRV-Hostnamen/die IP-Adresse (**IP Address / Host name** (z. B. br08a2.st.lz.com)) für OpenScape Branch ein.

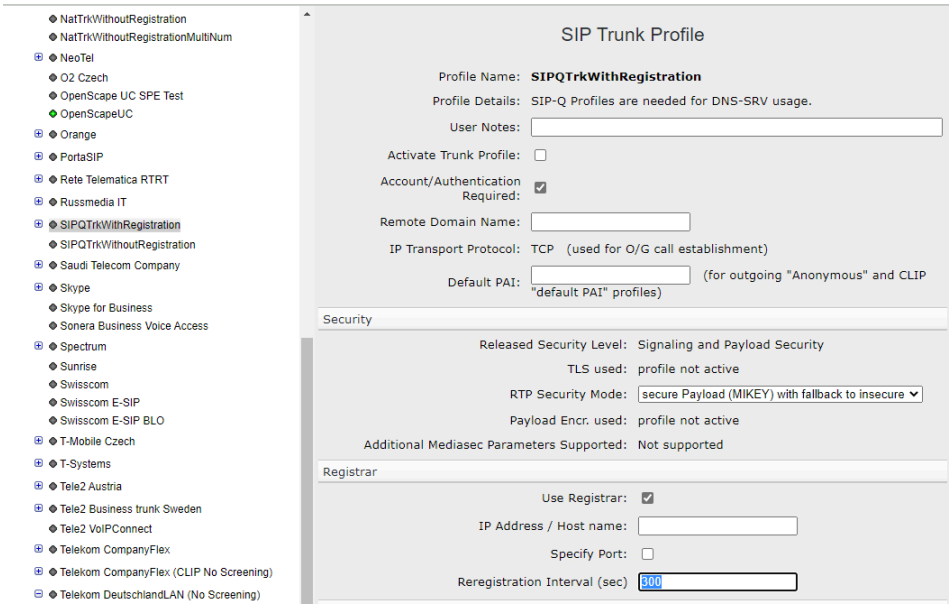


Abbildung 247: OpenScape 4000: IP-Adresse/Hostname für OpenScape Branch

14.7.7 Signaling and Payload Encryption (SPE)

Wichtig: Die virtuellen HG 3500-Gateways können wahlweise für den MIKEY- oder für den SDES-Betrieb, nicht aber für **beide** gleichzeitig konfiguriert werden. Die HG 3500-Gateways lassen sich nur für MIKEY konfigurieren.

Anmerkung: Bei den folgenden Schritten handelt es sich lediglich um die mindestens erforderlichen Einstellungen für sichere Anrufe mithilfe von MIKEY- oder SDES-Verschlüsselung über einen HG 3500-Gateway, der direkt zwischen OpenScape 4000 und und OpenScape Voice-Systemen konfiguriert ist.

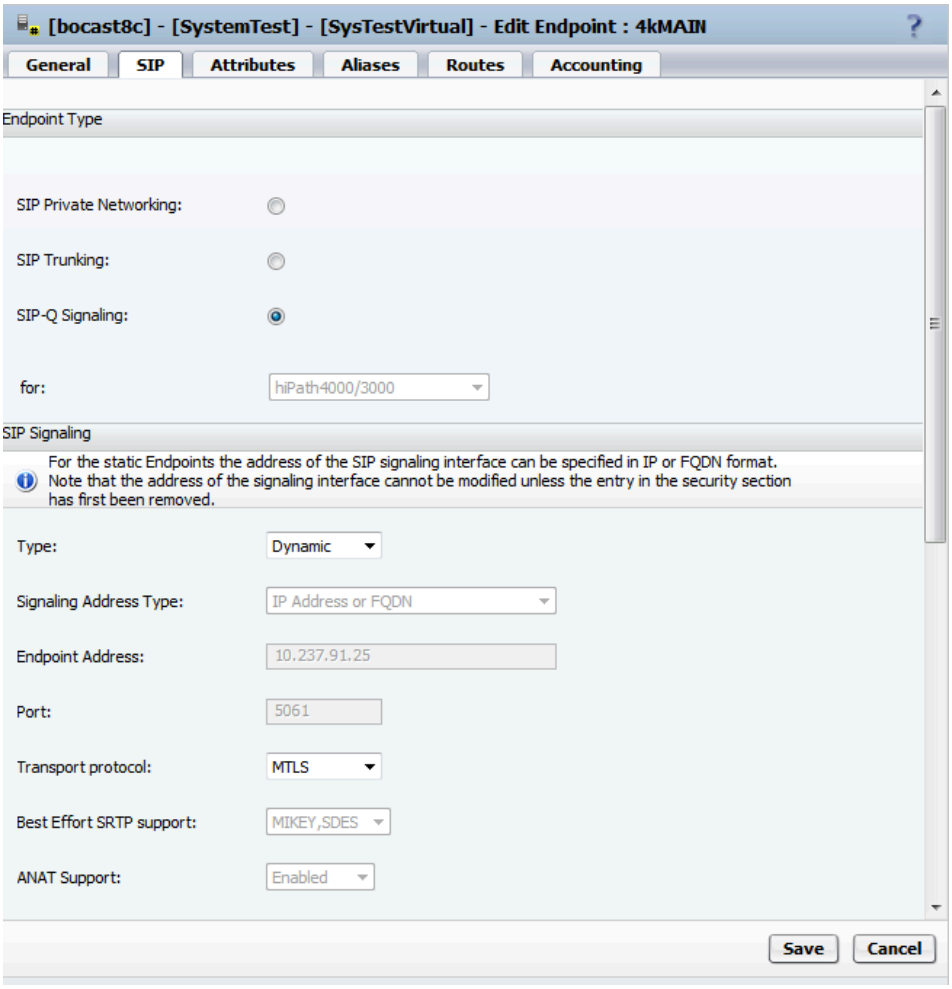
Anmerkung: SDES wird nur von virtuellen HG 3500-Gateways auf OpenScape 4000 SoftGate unterstützt.

Wichtig: Alle OpenScape Voice- und OpenScape 4000-Systeme müssen mithilfe eines NTP Zeit-Servers zeitlich genau abgestimmt werden. Eine Differenz von **mehr als** 60 Sekunden zwischen Registrierung und Sicherheit ist nicht möglich.

1) Kopieren Sie die Standard-Systemsicherheitszertifikate aus OpenScape Voice auf Ihre Arbeitsstation. Diese Zertifikate befinden sich im Ordner `/usr/local/ssl/certs` für `client.pem` bzw. im Ordner `/usr/local/ssl/private` für `root.pem`.
2) Für OpenScape Voice sind dedizierte TLS-Ports vorhanden. Sie können angezeigt werden, indem Sie sich als SRX-Benutzer anmelden und den folgenden Befehl aus dem SRX-Ordner ausführen:
   ```
   $ startup/srxqry <cr/enter>
   ```
   Dies bietet eine lange Ausgabe für jeden Knoten. Suchen Sie jedoch nach dem folgenden Eintrag:
   ```
   SIP TLS Auth         Vip: 10.237.84.104

   Up    ....für IPV4-Adresse
   SIP TLS Auth         Vip: fd00:10:237:84::104

   Up    ....for IPV6-Adresse
   ```
3) OpenScape Voice Konfiguration: Hinzufügen oder Bearbeiten eines Endpunkts. An dieser Stelle muss **SIP-Q Signaling** mit **Port 5061** und **Transport protocol MTLS** festgelegt werden.



OpenScape Voice: Signaling and Payload Encryption: Endpoint-Konfiguration

Für OpenScape 4000

1) AMO ZANDE für **TYP=SECURITY** muss **SPESUPP=JA**, **SECIPSB=SECURE** und **SECIPTR=SECURE** enthalten.
2) AMO TDCSU muss **SECLEVEL=SECURE** enthalten.
3) AMO CGWB für die HFA- und Amtsleitungskonfiguration muss **SECSUBS=JA** und **SECTRNK=JA** lauten. Die Parameter **REGIP1** und **REGIP2** sollten die OpenScape Voice-TLS-Portkennungen verwenden (falls für OpenScape Voice eine Duplex-Konfiguration verwendet wird) gemäß *Schritt 2*.

4) Die Zertifikate werden nun mittels Anmeldung beim WBM auf die HG 35xx-Baugruppe kopiert.

Wählen Sie **Configuration> Security > Signaling and Payload Encryption (SPE) > (rechte Maustaste) SPE-Zertifikat importieren**.

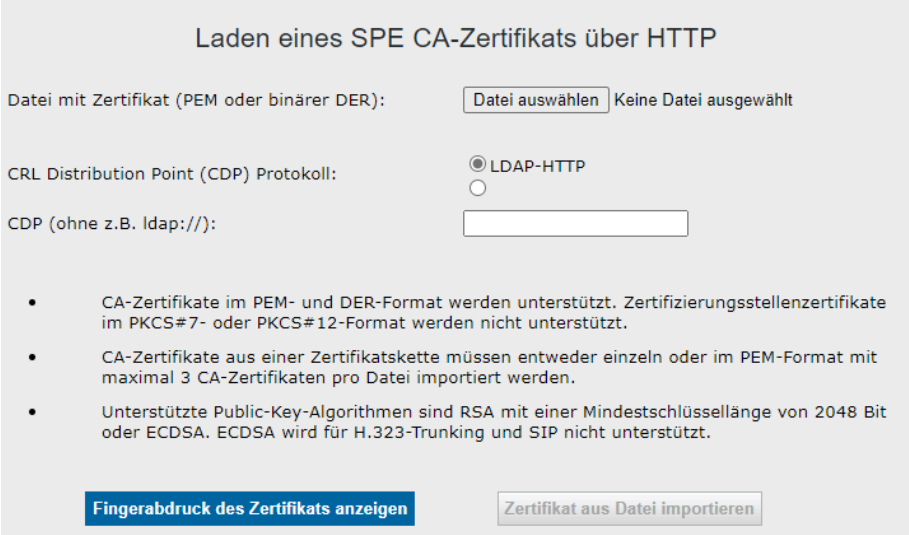


Abbildung 248: OpenScape 4000: Signaling and Payload Encryption: SPE CA-Zertifikate laden

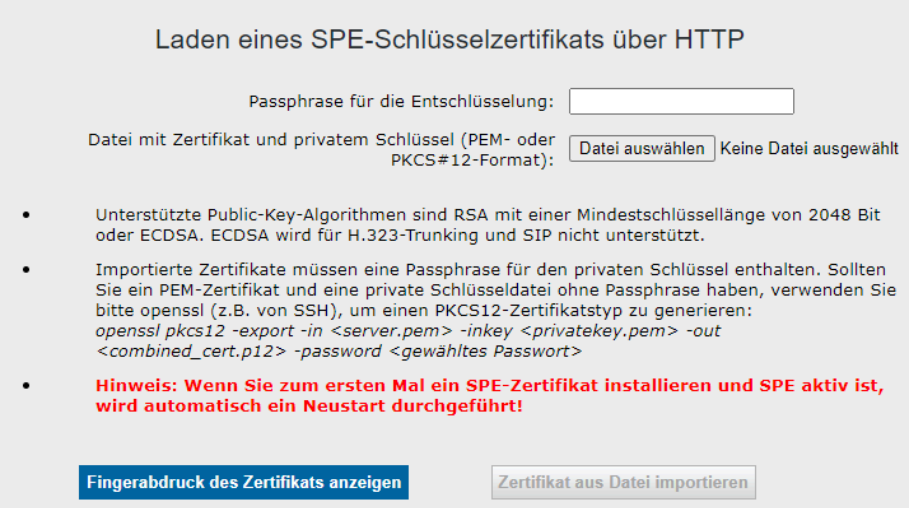
Es wird empfohlen, die Zertifikate in der folgenden Reihenfolge zu installieren:

Laden Sie zunächst das SPE CA-Zertifikat mit der Datei **root.pem**. Klicken Sie mit der rechten Maustaste auf **SPE CA-Zertifikat**, um **vertrauenswürdige CA-Zertifikate zu importieren**. Dies öffnet nun eine neue Browser-Sitzung namens **Load a SPE CA Certificate via HTTP** (SPE CA-Zertifikat per HTTP laden). Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen) und wählen Sie die Datei `root.pem` auf Ihrer Workstation aus. Wählen Sie nun **View Fingerprint of Certificate** (Fingerabdruck des Zertifikats anzeigen). Prüfen Sie den Fingerabdruck und wählen Sie **OK.**

Nun können Sie auf **Import Certificate from File** (Zertifikat aus Datei importieren) klicken.

Führen Sie dieselben Schritte mit dem SPE-Zertifikat und der Datei `client.pem` aus.

Nun registriert sich das Gateway mit dem Transportprotokoll TLS bei OpenScape Voice. Für die Payload wird SRTP mit MIKEY-Verschlüsselung angeboten.



OpenScape 4000: Signaling and Payload Encryption: SPE-Zertifikate laden

SDES-Sicherheit ist nur in Verbindung mit einer SIP-Trunk-Profil-Konfiguration verfügbar. Eine Änderung der OpenScape Voice-Einstellungen ist nicht erforderlich. Änderungen sind nur in OpenScape 4000 erforderlich.

In AMO CGWB muss **SIPREG** auf **NO** gesetzt werden:

```
AENDERN-
CGWB:MTYP=CGW,LTU=22,EBT=2,TYP=SIPTRSSA,SIPREG=NEIN;
```

Dadurch können SIP-Amtsleitungsprofile die Registrierung vom Gateway-WBM verwalten. Diese Profile können mittels Anmeldung beim WBM und Auswahl der Konfiguration **> Voice Gateway > SIP Trunk Profile**

Parameter gefunden und aktiviert werden. Klicken Sie mit der rechten Maustaste und wählen Sie **Edit**.

Use Profiles for Trunks via SIPQ muss aktiviert werden. Bestätigen Sie anschließend mit **Apply**.



OpenScape 4000: Aktivieren der Verwendung von Profilen für SIP-Amtsleitungen

Nun wird ein Ordner mit den verfügbaren SIP-Trunk-Profilen angezeigt. Öffnen Sie diesen Ordner, scrollen Sie nach unten und wählen Sie **SIPQTrkWithRegistration** aus.

Geben Sie die erforderlichen Daten für den Registrar ein. In das Feld **IP Address / Host name** (IP-Adresse/Hostname) sollte ein DNS-SRV eingetragen werden und der Wert im Feld **Registration Interval** (Registrierungsintervall) darf nicht kleiner als **300** Sekunden sein. Der Proxy muss ebenfalls mit denselben Daten konfiguriert werden wie der Registrar. **Outbound Proxy** (Abgehender Proxy) wird für Verbindungen zu OpenScape Branch oder einem anderen Branch/Proxy-Gerät verwendet. Scrollen Sie

zum Ende dieses Bildschirms und wählen Sie **SDES security with Fallback to Insecure (SDES-Sicherheit mit Rückfall in Insecure-Modus).**

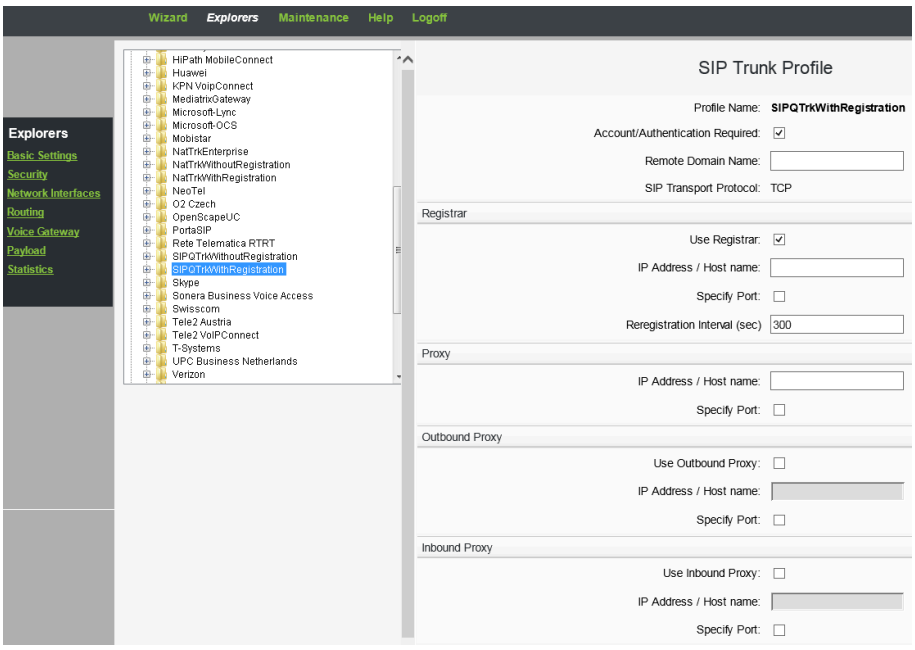


Abbildung 249: OpenScape 4000: Einstellungen für SIP-Amtsleitungsprofile

Hier sehen Sie die Anzeige nach der Konfiguration:

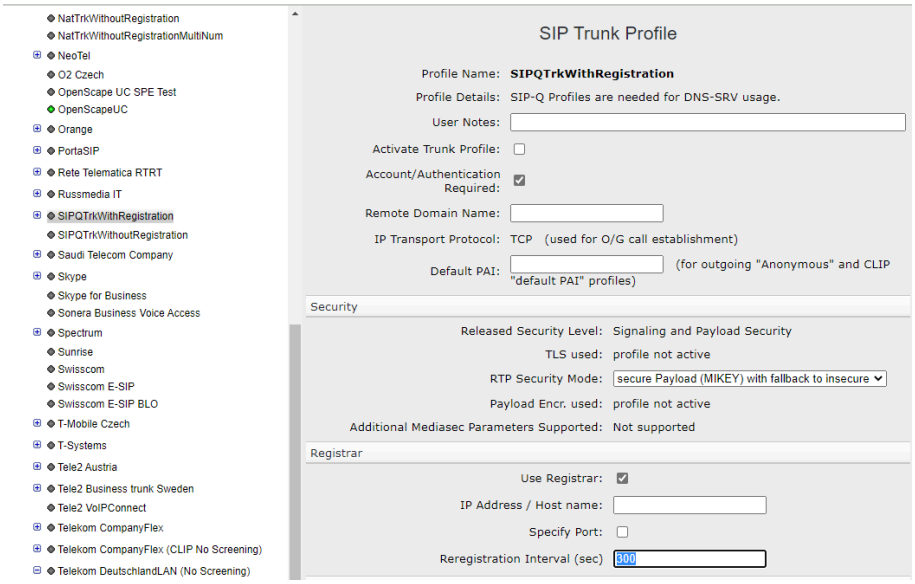


Abbildung 250: OpenScape 4000: SIP-Amtsleitungsprofil – Teil 1

Wählen Sie unter **RTP Security Mode** den RTP-Sicherheitsmodus aus:

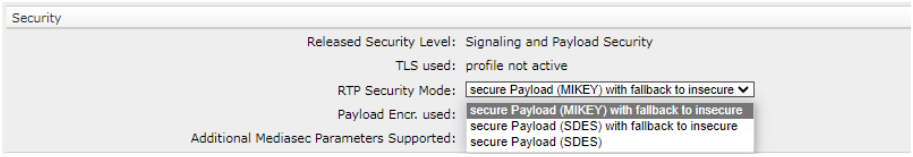
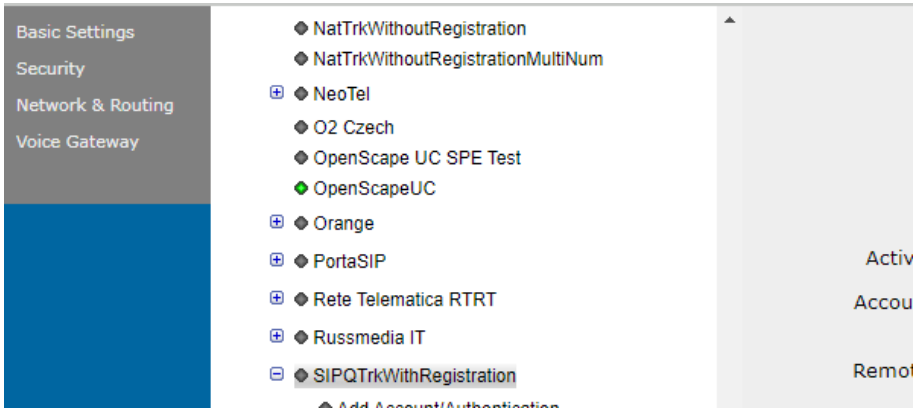


Abbildung 251: OpenScape 4000: SIP-Amtsleitungsprofil – Teil 2

Nun erscheint ein Untermenü zur Konfiguration von **Account Name**. Zum Bearbeiten der Benutzerkennung drücken Sie die rechte Maustaste. Der Eintrag im Feld **Account Name** (Benutzerkennung) muss mit dem Wert **GWDIRNO** in AMO CGWB, **TYPE=LEGKDATA** übereinstimmen.
`AENDERN-CGWB:MTYP=CGW,LTU=22,EBT=2,`**`TYP=LEGKDATA,`**
`GWRNR=166,``REGEXTGK=NEIN;`



OpenScape 4000: Account Name

Jetzt müssen Sie das Profil per Rechtsklick auf SIPQTrkWithRegistration aktivieren.

Speichern Sie die Konfiguration.



Abbildung 252: OpenScape 4000: Konfiguration speichern

Der Ordner wird ROT dargestellt, solange das Gateway nicht ordnungsgemäß bei OpenScape Voice und OpenScape Branch registriert ist. Nach erfolgreicher Registrierung wechselt er die Farbe und wird

GRÜN angezeigt.

5) End-to-end secure calling

Damit sind OpenScape 4000 und das SIP-Gateway für die Unterstützung der Signal- und Payload-Sicherheit (SPE) auf dem SIP-Q-Trunk zu OpenScape Voice konfiguriert. Für durchgängig sichere Verbindungen, die auf den Telefonen angezeigt werden, müssen diese ebenfalls als sichere Geräte konfiguriert werden. Konfigurieren Sie die SIP-Telefone in derselben Weise wie das Gateway, indem Sie die entsprechenden OpenScape Voice-

Sicherheitszertifikate importieren. Nach dem Installieren der Zertifikate wird auf den Telefonen ein Symbol für „sichere Verbindung“ angezeigt.

Wichtig: Für OpenScape Voice können sowohl optiPoint- und OpenStage-Geräte MIKEY verwenden, wobei nur OpenStage-Geräte SDES unterstützen.

Prüfen Sie das **SIP transport**-Protokoll (sollte TLS sein) für OpenStage-Geräte und vergewissern Sie sich, dass für **Connectivity check timer** ein größerer Wert als **0** (in diesem Beispiel 100) festgelegt ist.

OpenStage IP Admin > System > SIP Interface

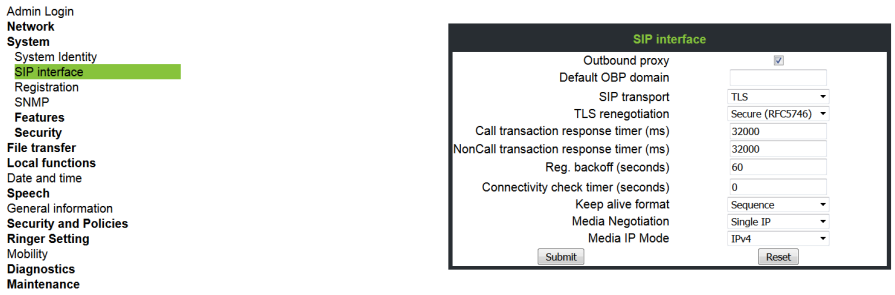


Abbildung 253: OpenStage: SIP-Interface-Einstellungen

Gehen Sie danach weiter zum Abschnitt **Security**. Wählen Sie **System**, aktivieren Sie **Use secure calls** und wählen Sie einen **SRTP type**. Bei OpenStage können Sie zwischen **Mikey** und **SDES**wählen.

OpenStage IP Admin > Security > System

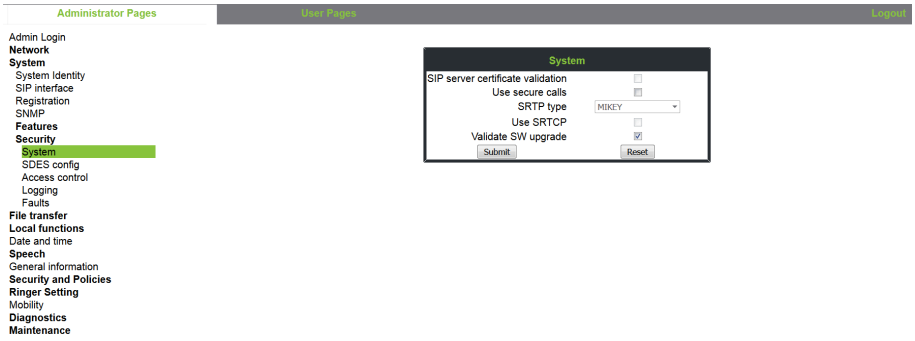


Abbildung 254: OpenStage: Sicherheitseinstellungen

In der SDES-Konfigurationsauswahl können Sie zu SDP-Sitzung (standardmäßig is SRTP und RTP) wechseln und die Priorität für die SDES

SHA1-80- oder SHA1-32-Methoden festlegen. Diese können auch auf den Standardwerten belassen werden, wobei SHA1-80 die höchste Priorität hat.

Für Abonnenten auf OpenScape Voice müssen die Konfiguration **Transport Protocol** auf **TLS** und **Port** auf **5061** gesetzt werden.

Common Management Portal > OpenScape Voice > Business Group > Main Office > Members > Subscribers

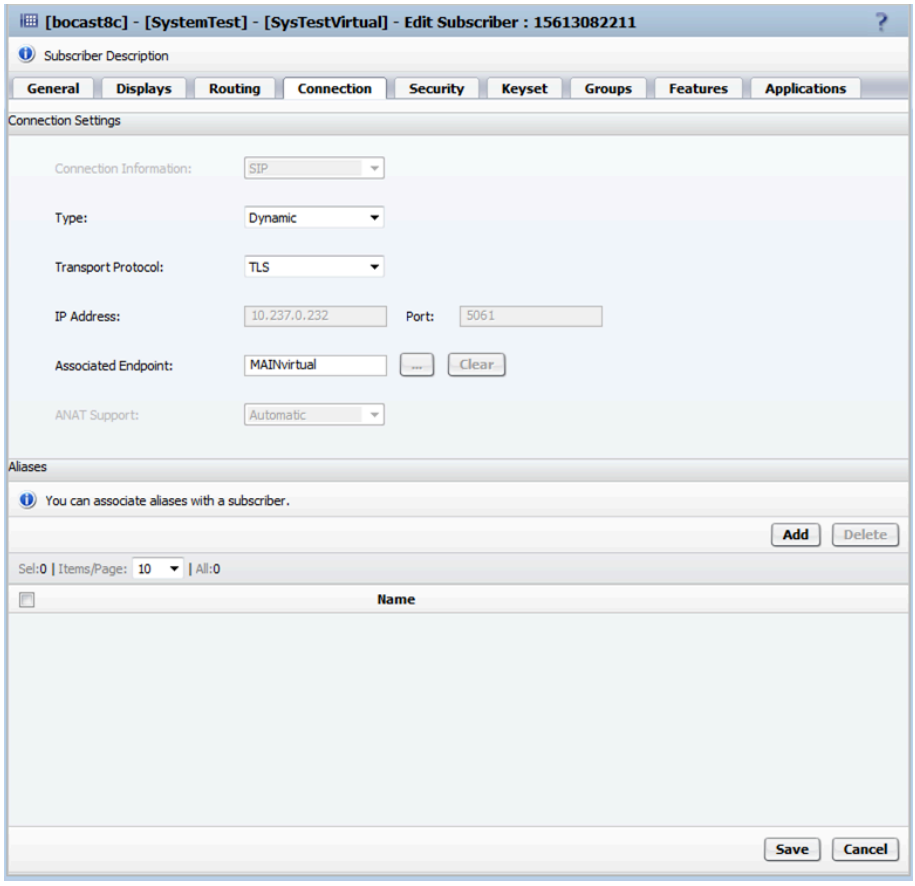


Abbildung 255: OpenScape Voice: Subscriber configuration > Registerkarte „Connection“

Auf der Registerkarte **Security** kann **Secure RTP** auf der Standardeinstellung **MIKEY, SDES** belassen werden.

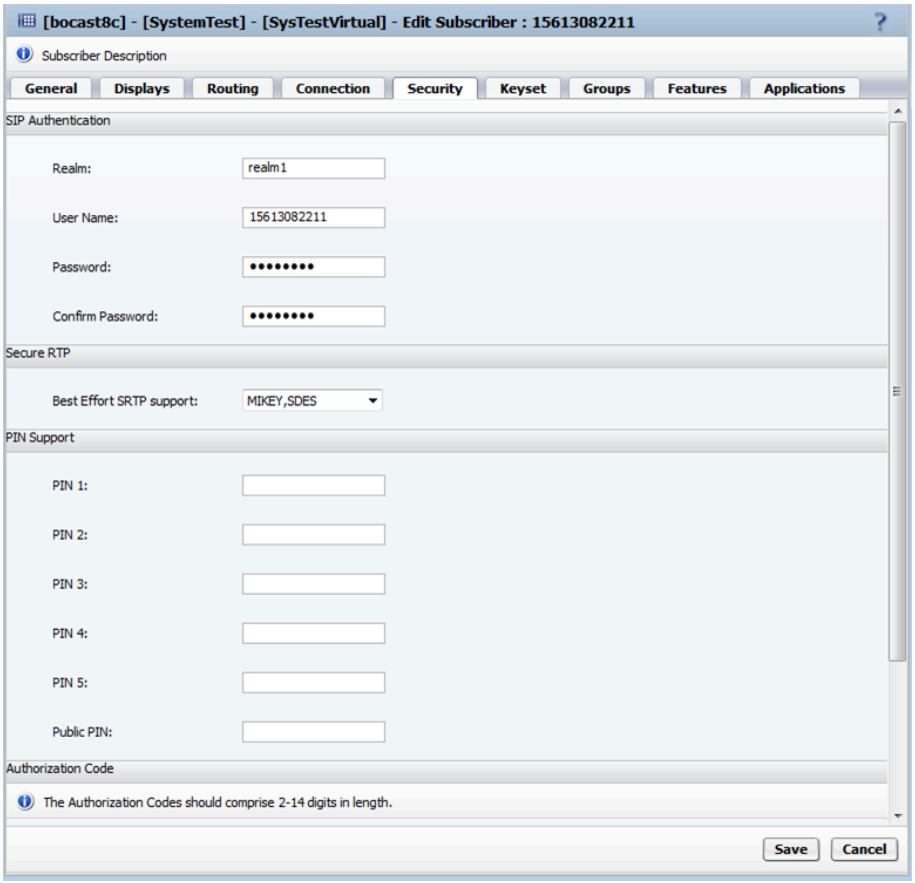


Abbildung 256: OpenScape Voice: Subscriber configuration > Registerkarte „Security“

Anmerkung: Die SIP-Authentifizierungsfelder dienen der Digestautorisierung und sind für die SPE-Operation nicht erforderlich.

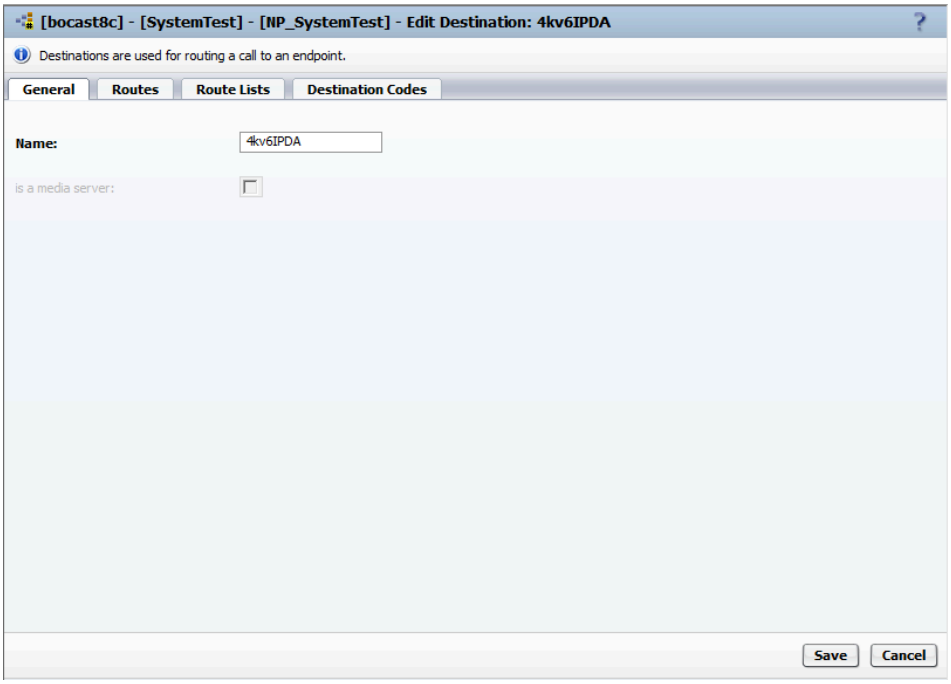
14.7.8 Richtung von OpenScape Voice zu OpenScape 4000

Um auf den Endpunkt zuzugreifen, müssen ein Ziel und eine Richtung konfiguriert werden.

Common Management Platform > OpenScape Voice > Business Group > Destinations and Routes > Destinations > Add

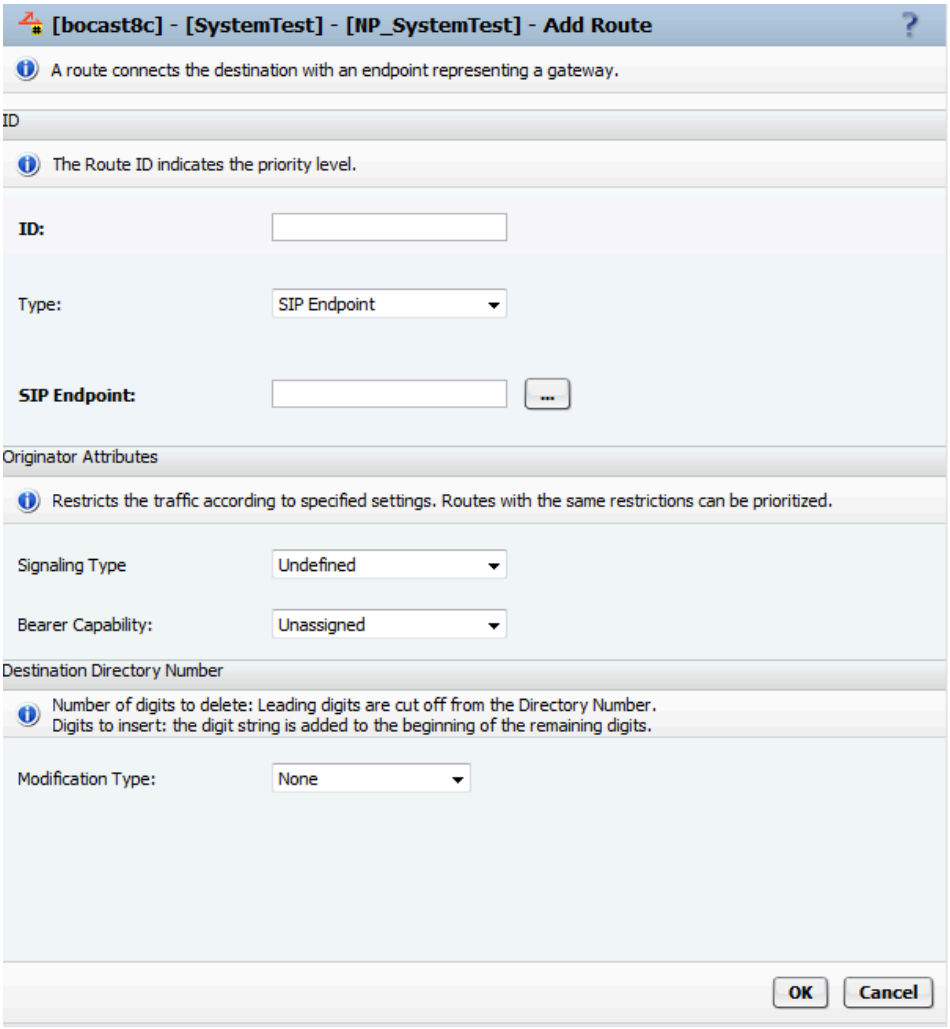
Öffnen Sie den Ordner **Destinations** und wählen Sie **Add**. Ein neuer Ordner wird auf der Registerkarte **Allgemein** geöffnet.

Erstellen Sie einen Namen für die Zieltabelle (z. B. 4kv6IPDA). Aktivieren Sie jedoch nicht das Kontrollkästchen **is a media server**. Bestätigen Sie mit **Save**.



OpenScape Voice: Ziel- und Richtungskonfiguration

Kehren Sie zum Ordner **Destinations** zurück, öffnen Sie den Ordner **4KV6IPDA** und klicken Sie auf der Registerkarte **Routes** auf **Add**.



OpenScape Voice: Ziel- und Richtungskonfiguration

ID: Es kann eine beliebige Nummer verwendet werden. Wenn es sich jedoch wie in den meisten Fällen um die erste Richtung handelt, verwenden Sie „1“. Die Nummer der Richtungs-ID zeigt auch die Prioritätsstufe an, wenn mehr als 1 Richtung konfiguriert ist.

Type: Standardmäßig ist **SIP Endpoint** festgelegt. Ändern Sie den Parameter nicht.

SIP Endpoint: Verwenden Sie das Menü zur Auswahl Ihres Endpunkts (z. B. 4KV6IPDA)

Signaling Type: Standardeinstellung beibehalten

Bearer Capability: Standardeinstellung beibehalten

Modification Type: Standardeinstellung beibehalten

Klicken Sie nun unten auf der Registerkarte auf **OK**.

14.7.9 OpenScape Voice-Richtung für die internationale Wahl – Rufnummern auf internationale Nummer erweitern

In dieser Konfiguration verwenden wir 5 und 6 Ziffern für interne und externe Zielnummern für OpenScape Voice.

Außerdem verwenden wir die E.164-Nummerierung.

Die Zielnummern für die geschlossene Nummerierung liegen im Bereich von 31000 bis 31249.

Für alle gewählten **Präfix-Zugangscodes** wie die Nummer in eine internationale E.164-Nummer umgewandelt.

Nach der Nummernumwandlung existieren alle gültigen gewählten Nummern nur noch als E.164-Nummern.

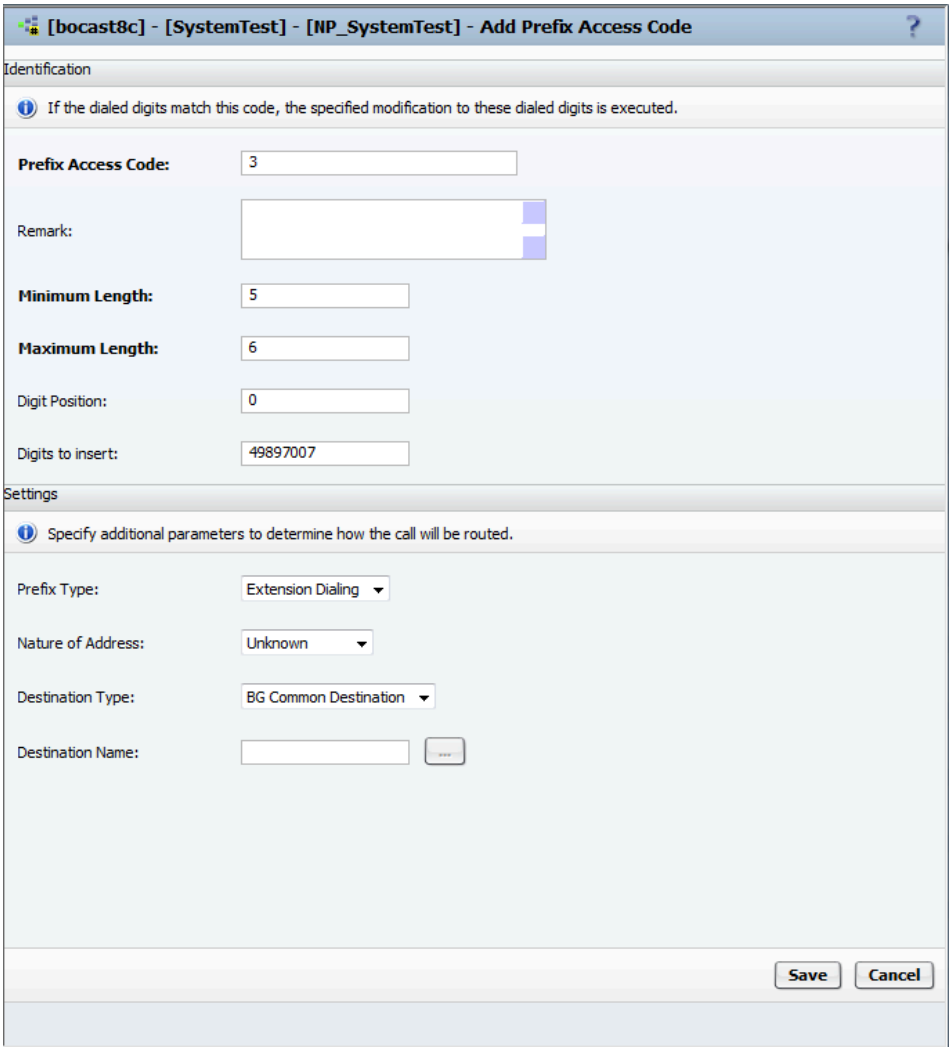
Dieser Eintrag wird an **BG Common Destination** gesendet, wo die Analyse für internationale E.164-Nummern durchgeführt wird.

Common Management Platform > OpenScape Voice > Business Group > Available Private Numbering Plan = „NP_FT_7007“ **> Translation > Prefix Access Codes**

14.7.9.1 Für 5- oder 6-stellige Nebenstellenwahl

Common Management Platform > OpenScape Voice > Business Group > BG_Common > Translation > Prefix Access Codes > Add

- **Prefix Access Code**: 3
- **Minimum Length**: 5
- **Maximum Length**: 6
- **Digits to insert**: 49897007
- **Destination Type**: BG Common Destination
- **Destination Name**: NP_COMMON



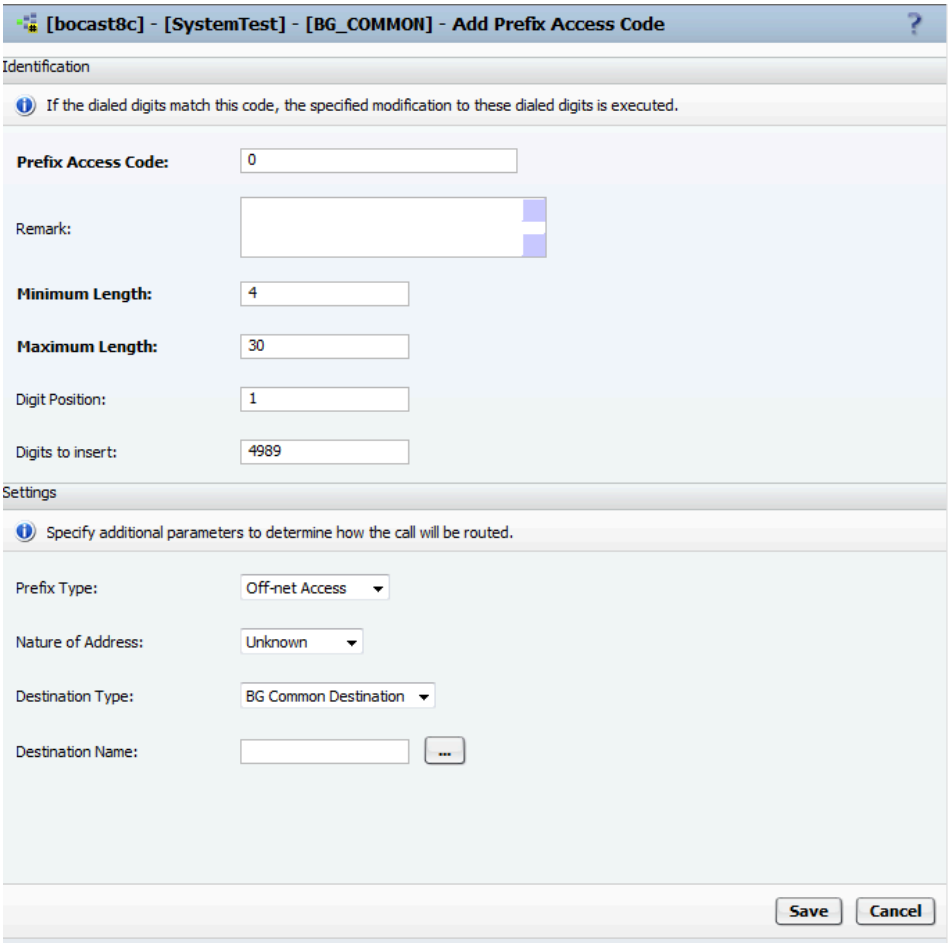
OpenScape Voice: Rufnummern auf internationale Nummer erweitern

14.7.9.2 Wählen mit Ortsvorwahl

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

Beispiel: 0-7007-3xxxx

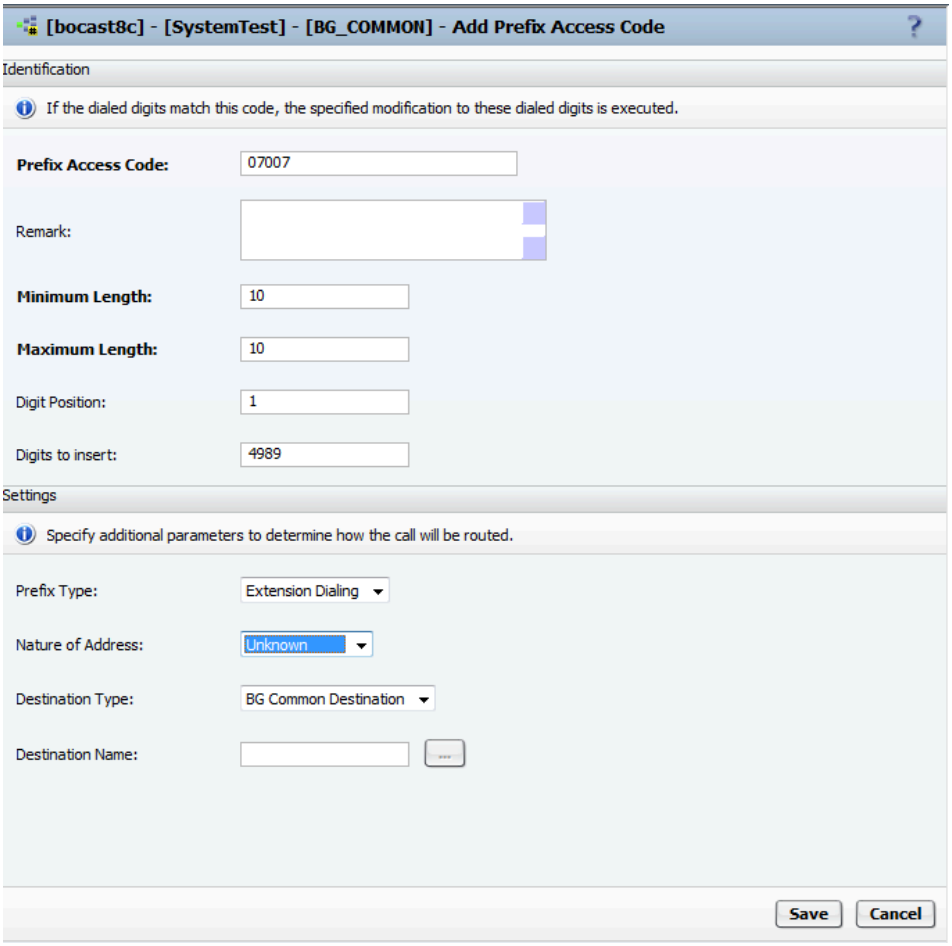
- **Prefix Access Code**: 0
- **Minimum Length**: 4
- **Maximum Length**: 30
- **Digit Position**: 1
- **Digits to insert**: 4989 (fügt 4989 zur gewählten Nummer hinzu)
- **Destination Name**: NP_COMMON (das Anrufziel wird durch die Nummer bestimmt)



OpenScape Voice: Wählen mit Ortsvorwahl

14.7.9.3 Wählen mit Ortsvorwahl (geschlossene Nummerierung)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add



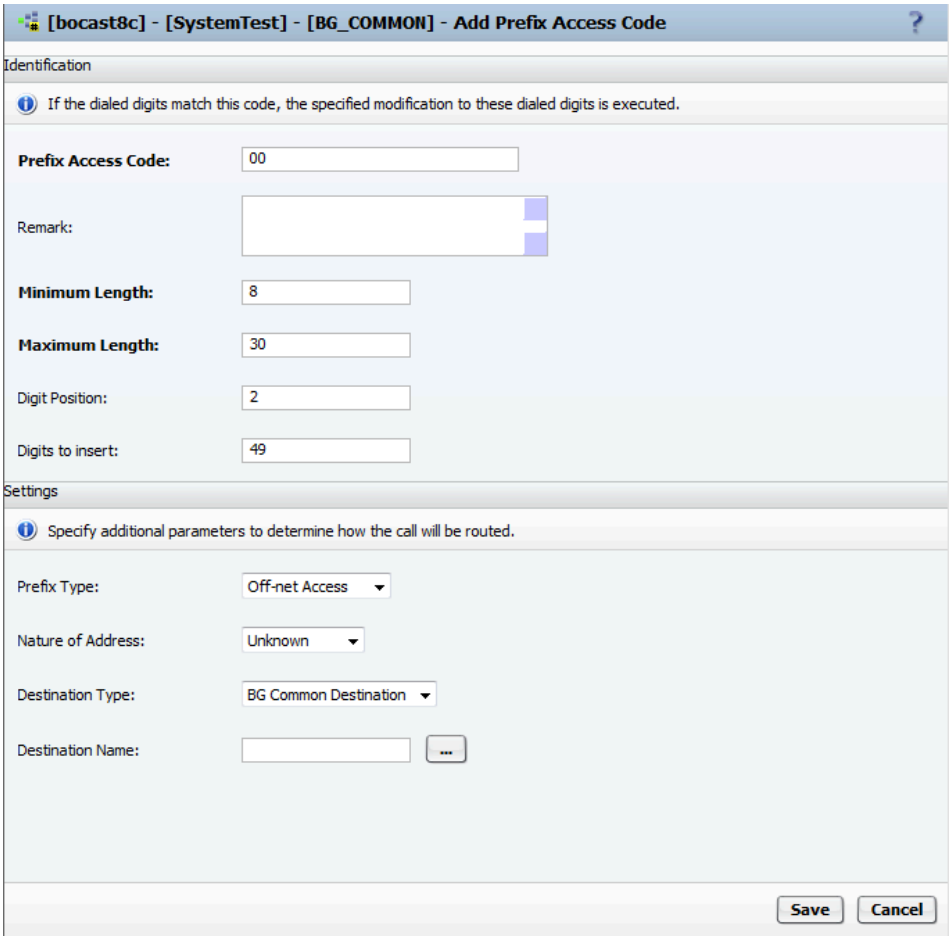
OpenScape Voice: Geschlossene Nummerierung

14.7.9.4 Wählen mit Landesvorwahl

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

Beispiel: 0-0897007-3xxxx

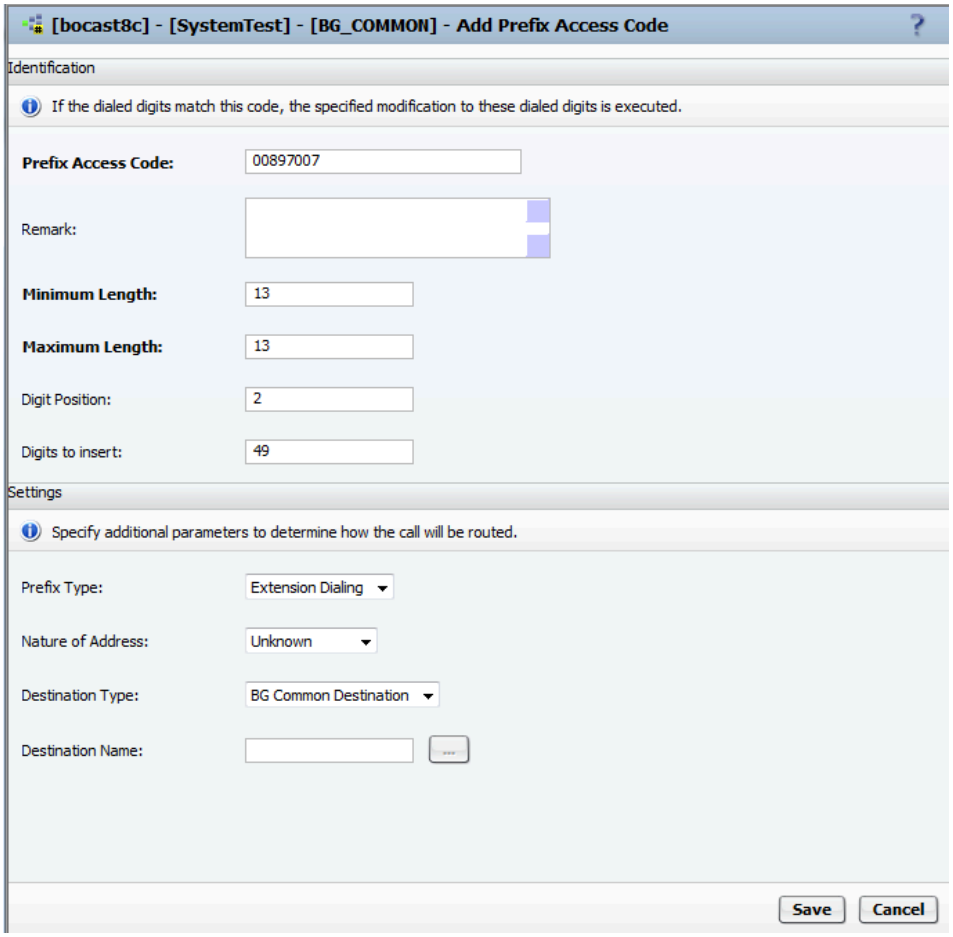
- **Prefix Access Code**: 00
- **Minimum Length**: 8
- **Maximum Length**: 30
- **Digit Position**: 2 (00 am Anfang der Nummer löschen)
- **Digits to insert**: 49 (fügt 49 zur gewählten Nummer hinzu)
- **Destination Name**: NP_COMMON (das Anrufziel wird durch die Nummer bestimmt)



OpenScape Voice: Wählen mit Landesvorwahl

14.7.9.5 Wählen mit Landesvorwahl (geschlossene Nummerierung)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add



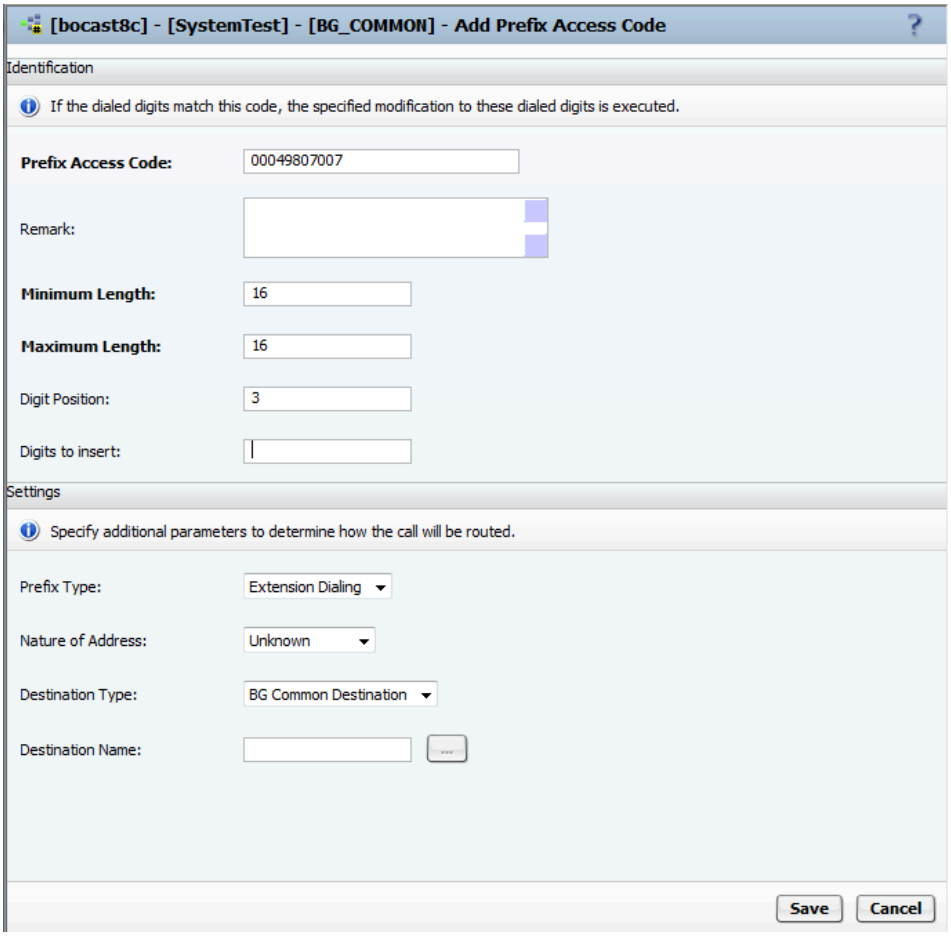
OpenScape Voice: Wählen mit Landesvorwahl (geschlossene Nummerierung)

14.7.9.6 Wählen mit Landesvorwahl

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

Beispiel: 0-0049897007-3xxxx

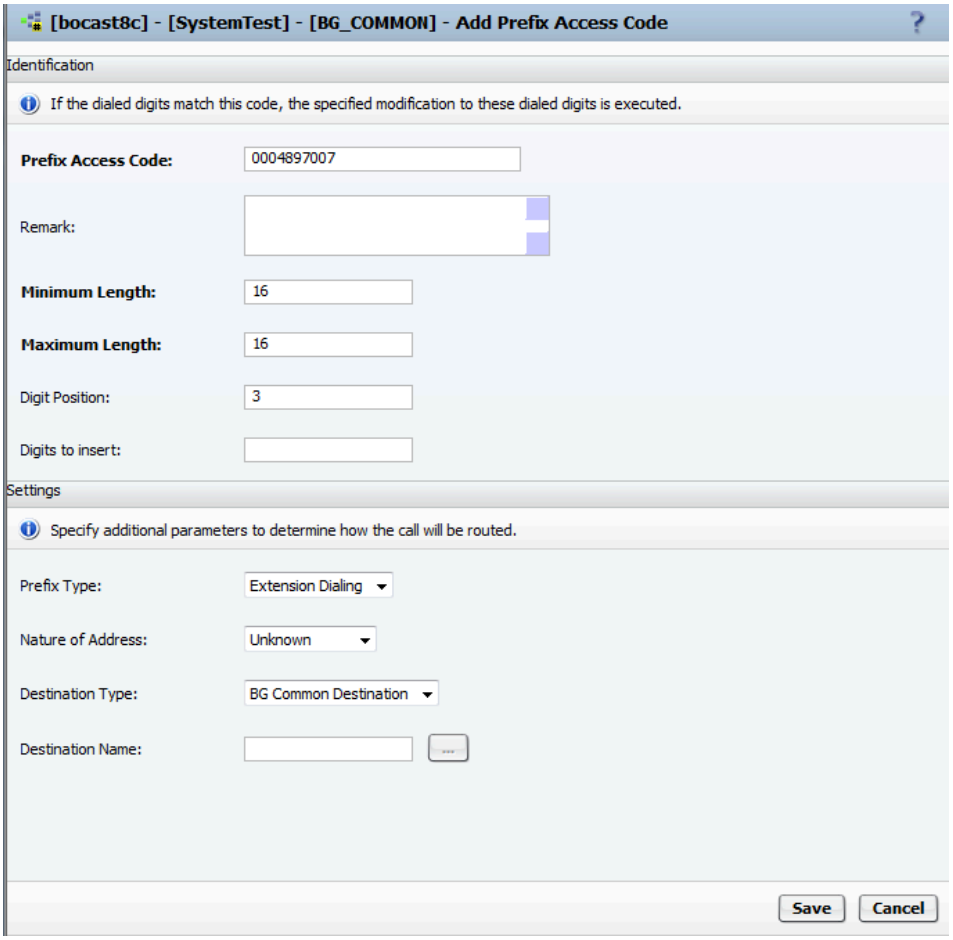
- Prefix Access Code: 000
- Minimum Length: 16
- Maximum Length: 16
- **Digit Position**: 3 (000 am Anfang der Nummer löschen)
- **Destination Name**: NP_COMMON (das Anrufziel wird durch die Nummer bestimmt)



OpenScape Voice: Wählen mit Landesvorwahl

14.7.9.7 Wählen mit Landesvorwahl (geschlossene Nummerierung)

Common Management Platform > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes > Add

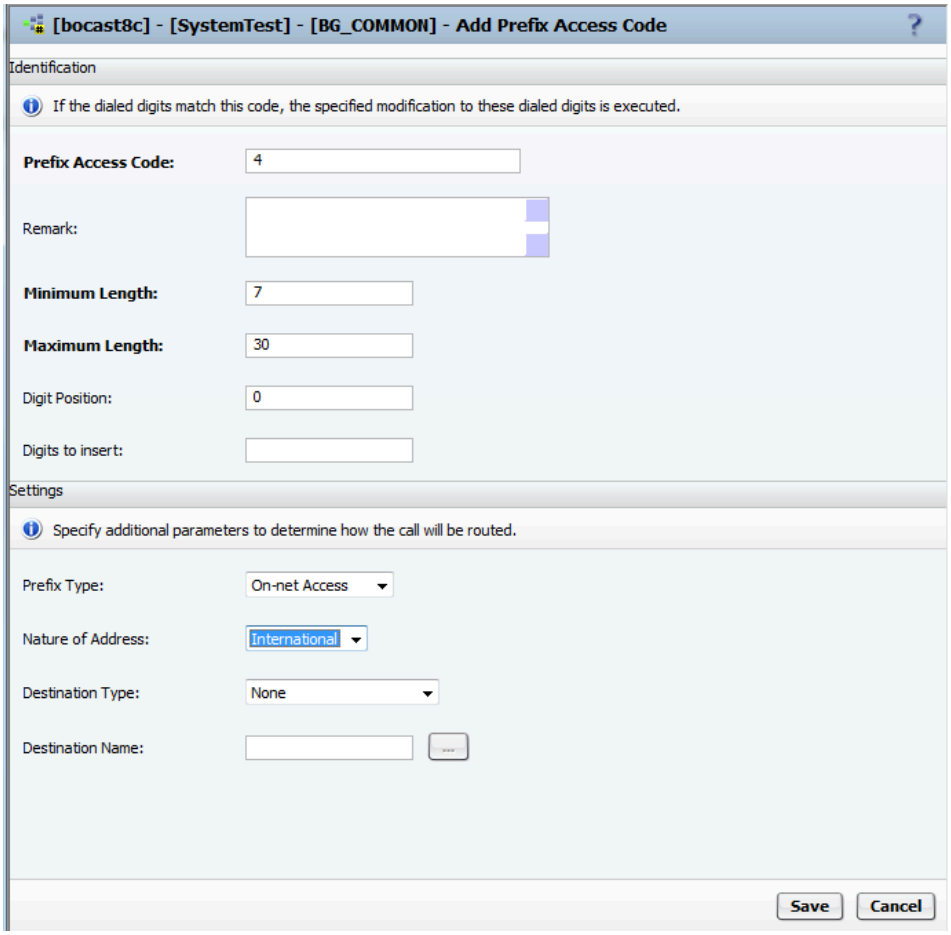


OpenScape Voice: Wählen mit Landesvorwahl (geschlossene Nummerierung)

14.7.9.8 Nummerntyp auf „International“ ändern

Common Management Portal > OpenScape Voice > Business Group > BG_COMMON > Translation > Prefix Access Codes

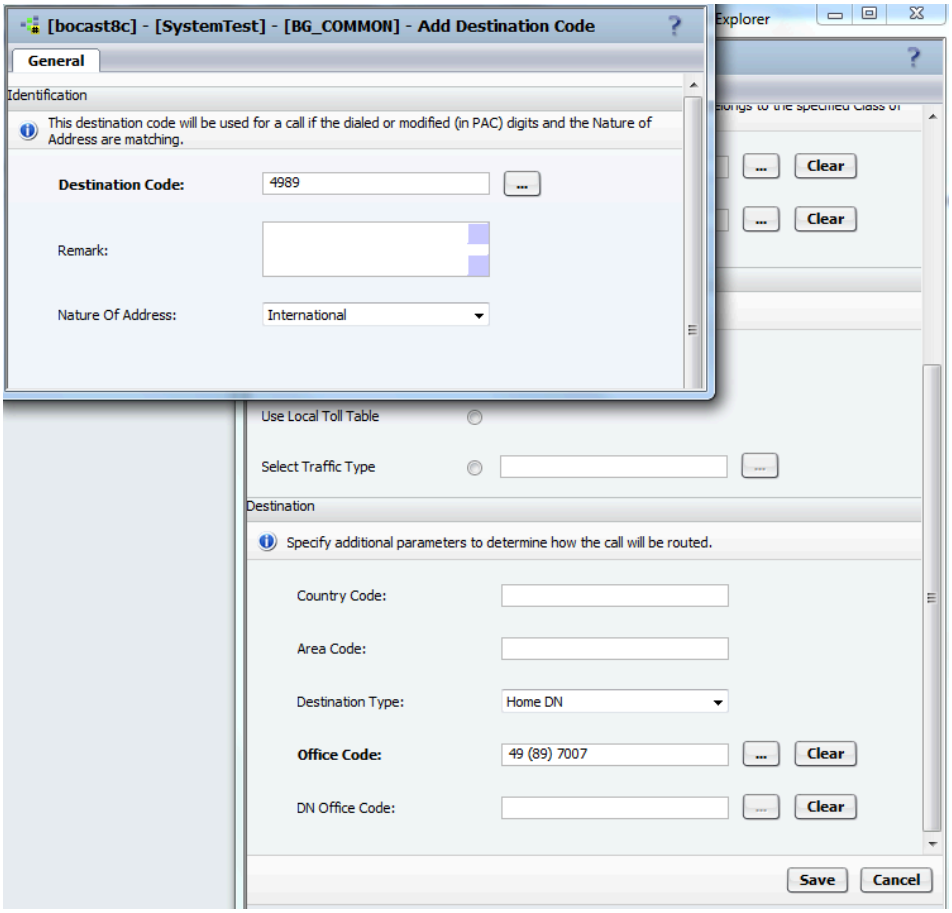
Setzen Sie **Nature of Address** auf **International**.



OpenScape Voice: Nummerntyp auf „International“ ändern

14.7.9.9 Internationale Nummer für „HOME DN“ anpassen

Common Management > OpenScape Voice > Business Group > BG_COMMON > Translation > Destination Code > Add

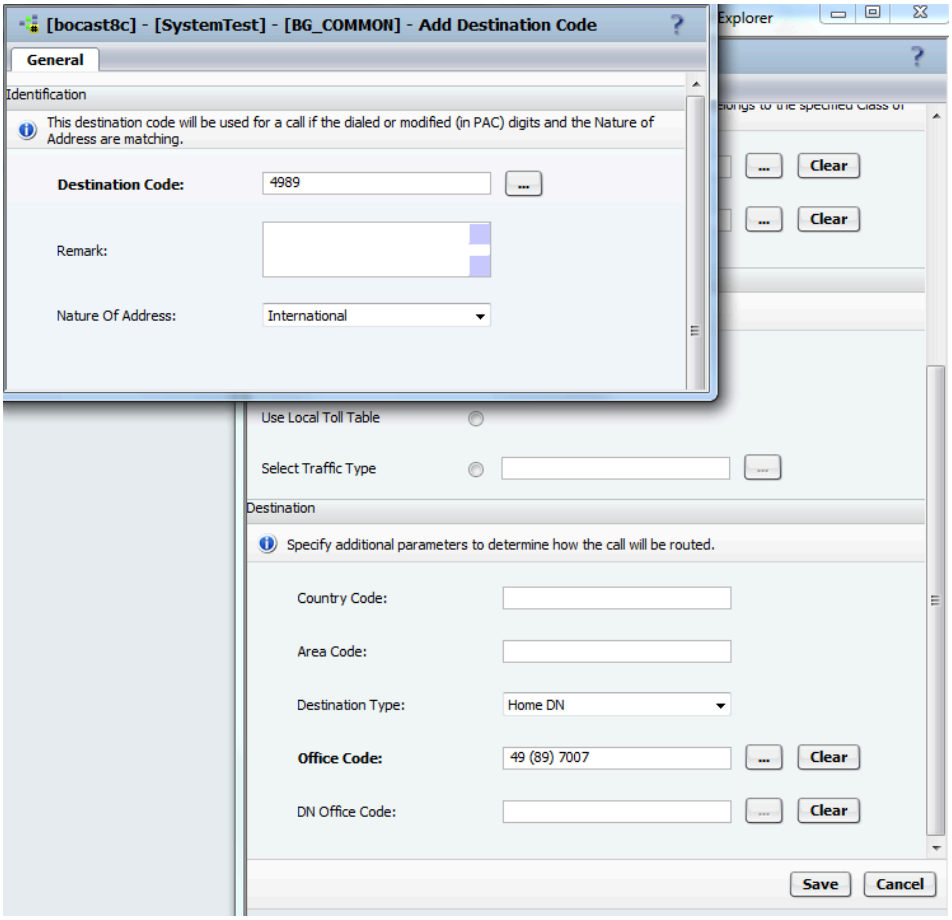


OpenScape Voice: Internationale Nummer für „HOME DN“ anpassen

14.7.9.10 Konfiguration der Standartrichtung, wenn die Nummer in „HOME DN“ nicht übereinstimmt

In Bild 107 oben wurde die Nummer 49897007-xxxxx zur Prüfung gesendet, um festzustellen, ob ein Eintrag im OpenScape Voice-System vorhanden ist. Wenn keine Übereinstimmung besteht, werden gewählte Nummern mit diesem Eintrag verglichen.

Standardmäßig sollten Sie das Partner-OpenScape 4000-System konfigurieren. In diesem Beispiel haben wir als Standard ein anderes OpenScape Voice-System verwendet.

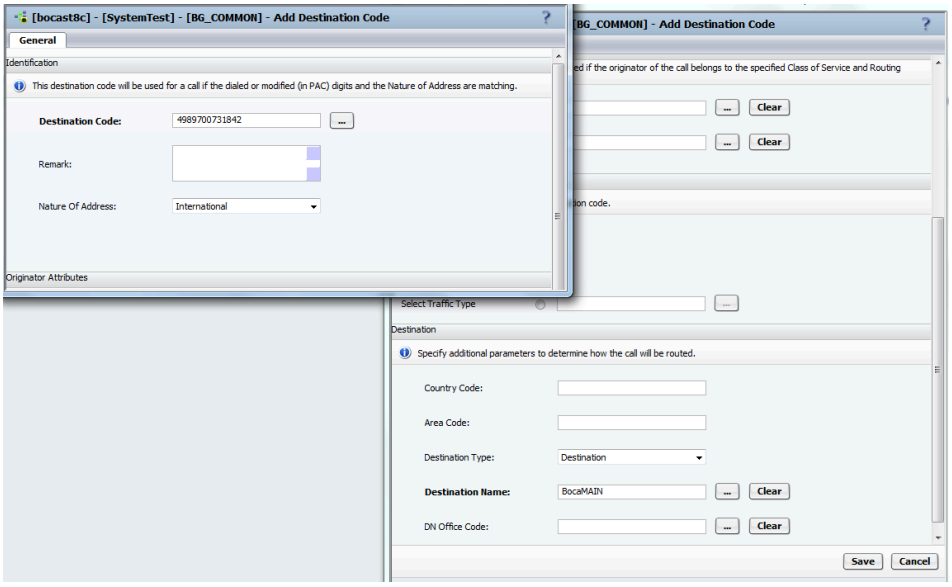


OpenScape Voice: Konfiguration für Standardrichtung

14.7.9.11 Komplette internationale Nummernwahl für einzelne externe Zielnummer

In diesem Beispiel ist mehr als ein Partnersystem vorhanden.

Daher müssen wir jede internationale Nummer, die nicht in unserem eigenen System und im Standard-Partnersystem vorhanden ist, direkt an den Zielort senden.



OpenScape Voice: Komplette internationale Nummernwahl

14.7.10 Schleifenerkennung für OpenScape Voice

OpenScape Voice unterstützt:

- Festlegen und Erhöhen von Q.931 Transit Counter. Dieser Mechanismus bietet nur Schutz bei Anrufen mit einer Schleife innerhalb des Unternehmensnetzwerks (z. B. für OpenScape 4000).
- Bei OpenScape 4000 werden der COT-Parameter **ATRS** und der AMO TDCSU-Parameter **TRACOUNT** für die Konfiguration verwendet.
- OpenScape Voice bietet einen Schleifenerkennungsdienst, der auch Schutz bei Anrufen mit einer Schleife innerhalb des öffentlichen Netzes ermöglicht. Der Dienst kann über die folgenden Parameter aktiviert werden:
- `Srx/Service/CFLoopPrevention`
  `Srx/Service/CFLoopMaxCount`

  Dieser Dienst beschränkt die Anzahl der gleichzeitigen unbeantworteten Anrufe zwischen Amtsleitungen, bei denen die Nummern des anrufenden und des angerufenen Teilnehmers identisch sind. Der Dienst gilt für Tandem-Anrufe (z. Direktanrufe zwischen Amtsleitungen) und Umleitungsszenarien (z. B. wenn ein Amtsleitungsgespräch von einem Teilnehmer an eine Amtsleitung umgeleitet wird). Im Falle der Umleitung wird die „diverted to“-Nummer verwendet.
- Der SIP Max-Forwads-Hop-Zähler gemäß RFC 3261.
- Das Szenario kann mit dem auf OpenScape 4000 konfigurierten Q.931 Transit Counter oder dem Schleifenerkennungsdienst in OpenScape Voice verwaltet werden.

14.7.11 Einschränkungen

- Die HG 3500-Baugruppe sendet nur Digest-Kennungen für Registrierungs- und Einladungsanfragen, wenn eine Anfrage gestellt wird. Diese Benutzernamens- und Kennwortkonfigurationen werden im SIP-Q-

Leitungsprofil vorgenommen. OpenScape 4000 fordert die Digest-Authentifizierung nur für Registrierungsanfragen für SIP-Teilnehmer an.

- In einem HiPath 4000/OpenScape 4000-Netzwerk können die Payload-Partner mit DMC festgelegt werden. Ein HiPath 4000/OpenScape 4000-Telefon kann jedoch keine direkten Payloads für OpenScape Voice-Partner empfangen. Beim HG 3500-Modul ist immer ein Hop vorhanden.
- Wenn für das HG 3500-Modul nicht mehr als zwei Partner konfiguriert sind (z. B. proxy) und **REGIP1** fehlschlägt, bleibt **REGIP2** registriert, bis **REGIP2** nicht mehr verfügbar ist.

Wichtig: Es wird nicht automatisch auf **REGIP1** zurückgeschaltet.

1)

Anmerkung: Ab HiPath 4000 V6 kann DNS-SRV mit SIPQ-Amtsleitungsprofilen verwendet werden.

- Bitte beachten Sie, dass die Anzahl der verwendbaren B-Kanäle, die für SIP-Q-Anrufe zugewiesen werden können, davon abhängt, welche Funktionen (DMC/SPE/QOS-Erfassung) aktiviert sind und welcher Gerätetyp (STMI2/ STMI4) auf OpenScape 4000 verwendet wird. AMOs nehmen einige automatische Anpassungen vor. Weitere Informationen hierzu finden Sie jedoch in der Servicedokumentation unter *OpenScape 4000, Band 4: IP-Lösung*.

14.8 Interworking mit Microsoft Lync Communication Server 2010/2013

14.8.1 Wichtige Hinweise

Wichtig: Dieses Leistungsmerkmal wird nur auf projektspezifischer Basis für Konnektivität mit vHG 35000 (OpenScape 4000 SoftGate) bereitgestellt!

14.8.2 Leistungsmerkmalbeschreibung

Interworking wird zwischen OpenScape 4000 und Microsoft Lync Communication Server 2010/2013, dem Nachfolger von Microsoft Office Communications Server 2007 unterstützt. Das Interworking ermöglicht die Verbindung des Microsoft Lync Communication Server 2010/2013 mit dem OpenScape 4000-Unternehmensnetzwerk über den Mediation Server. Dadurch sind Anrufe zum/vom Lync Communication Server 2010/2013 über HiPath 4000 SoftGate auf nativen SIP-Amtsleitungen möglich.

Die Microsoft Lync Communication Server 2010/2013-Konnektivität funktioniert in Verbindung mit nativen SIP-Amtsleitungen auf dem HiPath 4000 SoftGate (direct SIP).

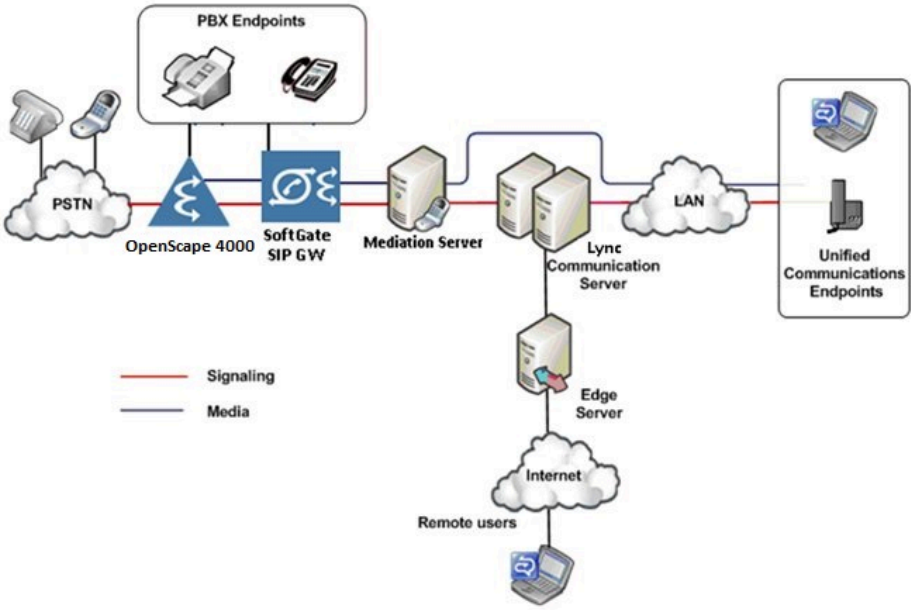


Abbildung 257: Interworking mit Microsoft Lync Communications Server 2010/2013 über Mediation Server

14.8.3 Realisierung

Für die Konnektivität mit Microsoft Lync Communication Server 2010/2013 kommen nur native SIP-Amtsleitungen auf dem 4000 SoftGate infrage (Direct SIP).

14.8.4 Serviceinformationen

14.8.4.1 Einschränkungen

Allgemeine Einschränkungen

- Refer wird nicht unterstützt.
- => Deaktivieren Sie REFER auf dem Lync Mediation-Server.
- OpenScape 4000 SoftGate bietet keine Unterstützung für Comfort Noise.

Leistungsmerkmaleinschränkungen

- Dual Forking
- Media Bypass
- E911
- DNS-Lastausgleich wird von OpenScape 4000 nicht unterstützt.
- Keine Töne auf dem Lync Communications Server-Client nach Übergabe im Rufzustand durch den OpenScape 4000-Anschluss.
- Informationen zu den Einschränkungen der Leistungsmerkmale finden Sie in Abschnitt 8.4.2, „Verfügbare Leistungsmerkmale“ (ausführliche Beschreibungen zu den einzelnen Leistungsmerkmalen in jedem Abschnitt).

14.8.4.2 Verfügbare Leistungsmerkmale

14.8.4.2.1 Basisanruf

Namens- und Nummernanzeige

- Bei HiPath 4000 ankommende Anrufe:
  - Auf dem Display des Anrufers (Lync Communications Server) wird bei einem Basisanruf die gewählte Rufnummer angezeigt.
  - Auf dem Display des gerufenen Teilnehmers (HiPath 4000) werden bei einem Basisanruf in der ersten Zeile die Rufnummer und der Name des Anrufers angezeigt.
  - Auf dem Display des mit HiPath 4000 verbundenen Teilnehmers werden bei einem Basisanruf die Rufnummer und der Name des Anrufers angezeigt.
  - Auf dem Display des mit dem Lync Communications Server verbundenen Teilnehmers wird bei einem Basisanruf die gewählte Rufnummer, aber kein Name angezeigt.
- An Lync Communications Server abgehende Anrufe:
  - Auf dem Display des Anrufers (HiPath 4000) werden bei einem Basisanruf die gewählte Rufnummer und der Name der SIP-Amtsleitung angezeigt.
  - Auf dem Display des gerufenen Teilnehmers (Lync Communications Server) werden bei einem Basisanruf die Rufnummer und der Name des Anrufers angezeigt. Ausnahme: Wenn die Rufnummer des Anrufers/verbundenen Teilnehmers im Global Catalog (Active Directory) aufgeführt sind, wird der im AD angegebene Name des Anrufers/verbundenen Teilnehmers angezeigt.[10]
  - Auf dem Display des mit HiPath 4000 verbundenen Teilnehmers werden bei einem Basisanruf die gewählte Rufnummer und der Name der SIP-Amtsleitung angezeigt.
  - Auf dem Display des mit Lync Communications Server verbundenen Teilnehmers werden bei einem Basisanruf die Rufnummer und der Name des Anrufers angezeigt. Ausnahme: Wenn die Rufnummer des Anrufers/verbundenen Teilnehmers im Global Catalog (Active Directory) aufgeführt sind, wird der im AD angegebene Name des Anrufers/verbundenen Teilnehmers angezeigt.[11]
- CLIP/CLIR-Leistungsmerkmale - Übermittlung von Name und Rufnummer des Anrufers (Erlaubt und Eingeschränkt).
- **Einschränkung (Namens- und Nummernanzeige)**: Die Benachrichtigung über entgangene Anrufe enthält keine Informationen zum Namen des Anrufers.
- Besonderer Hinweis: Der verwendete Rufnummernplan ist E.164 (ISDN/International).

Codecs

- G.711a-Law, ptime=20msec bevorzugter Codec G.711 u-Law
- G.729 wird von Lync Communications Server nicht unterstützt.

10 Exception: If calling/connected number is found in Global Catalog (Active Directory) then the name from AD is shown for calling/connected party.

11 Exception: If calling/connected number is found in Global Catalog (Active Directory) then the name from AD is shown for calling/connected party.

- G.723 wird von HiPath 4000 SoftGate und Lync Communications Server nicht unterstützt
- Sprechpausenunterdrückung für G711 ist nicht möglich, während eine andere Signalisierung verwendet wird.
  - Lync Communications Server verwendet Comfort Noise PT (13)
  - vHG 35xx / HiPath 4000 verwendet Attribute: silenceSupp:on - von Lync Communications Server nicht unterstützt.
- Einschränkungen:
  - G.729, G.723 wird nicht unterstützt
  - Sprechpausenunterdrückung wird nicht unterstützt

14.8.4.2.2 Anrufübergabe (ohne Rückfrage, vor Melden, nach Melden)

Der HiPath 4000-Benutzer kann Anrufe an einen Lync Communications Server-Teilnehmer übergeben. Übergabe nach Melden und vor Melden[12] und ohne Rückfrage[13] ist möglich.

- Übergabe im Gesprächszustand (Beaufsichtigte Übergabe)

  Anzeige - keine Aktualisierung der Displayanzeige auf irgendeinem Gerät - AMT-Verhalten:

  Nach der Übergabe werden auf dem Display des Anrufers der Name und die Rufnummer des gerufenen Teilnehmers und auf dem Display des Übergabeziels in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt
- Übergabe im Rufzustand (Übergabe vor Melden)

  Wichtig: Aufseiten der HiPath 4000 angeboten, nicht aufseiten des Lync Communications Servers.

- Anzeige - keine Aktualisierung der Displayanzeige auf irgendeinem Gerät - AMT-Verhalten:

  Nach der Übergabe werden auf dem Display des Anrufers der Name und die Rufnummer des gerufenen Teilnehmers und auf dem Display des Übergabeziels in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt
- Übergabe ohne Rückfrage

  Wichtig: Aufseiten des Lync Communications Servers angeboten, nicht aufseiten der OpenScape 4000.

- Anzeige - Anzeige des übergebenen Teilnehmers wird nicht aktualisiert:

  Nach der Übergabe werden auf dem Display des Anrufers der Name und die Rufnummer des gerufenen Teilnehmers und auf dem Display des Übergabeziels in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt

14.8.4.2.3 Anrufumleitung

Der OpenScape 4000-Benutzer kann Anrufe an einen Lync Communications Server-Teilnehmer umleiten.

[12] nur aufseiten der HiPath 4000

[13] nur aufseiten des Lync Communications Servers

CFA (Alle Anrufe umleiten), CFA (Anrufumleitung bei besetzt) und CFNA (Anrufumleitung bei Nichtmelden) sind möglich.

- Displayanzeige für Anrufumleitung unbedingt/bei besetzt - unabhängig vom Umleitungsziel
  - Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des gerufenen Teilnehmers angezeigt.
  - Auf dem Display des Umleitungsziels werden in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt.
  - Auf keinem Display wird ein Hinweis auf die erfolgte Anrufumleitung angezeigt.
- Displayanzeige für Anrufumleitung bei Nichtmelden - unabhängig vom Umleitungsziel
  - Auf dem Display des Anrufers werden in der ersten Zeile der Name und die Rufnummer des gerufenen Teilnehmers angezeigt.
  - Auf dem Display des Umleitungsziels werden in der ersten Zeile der Name und die Rufnummer des Anrufers angezeigt.
  - Auf keinem Display wird ein Hinweis auf die erfolgte Anrufumleitung angezeigt.

Besonderer Hinweis

- Die Anrufumleitung erfolgt auf beiden Seiten nach der „Forward-Switching“-Methode.

Einschränkungen

- Teilnehmer A erhält keinen Hinweis auf die Anrufumleitung.
- Anrufumleitung bei besetzt wird aufseiten des Lync Communications Servers nicht unterstützt.
- PBX bemerkt die Anrufumleitung nicht.
- Voicemail-Szenarien aufseiten der HiPath 4000 sind nicht möglich.

14.8.4.2.4 Halten und Wiederaufnehmen

Dieses Szenario ist sowohl aufseiten der HiPath 4000 als auch aufseiten des Lync Communications Servers möglich. Verwendet das Attribut „inactive in both directions“ (inaktiv in beiden Richtungen). Lokale Wartemusik (MOH) wird auf beiden Seiten verwendet.

14.8.4.2.5 Dreierkonferenz

Konferenzszenarien sind möglich - AMT-Verhalten.

Anzeige - Auf dem Display aller Konferenzteilnehmer an der OpenScape 4000 werden die korrekten Informationen zu allen OpenScape 4000-Konferenzteilnehmern angezeigt. Lync Communications Server-Teilnehmer werden als externe Teilnehmer angezeigt.

Das Display der OpenScape 4000-Konferenzteilnehmer wird nicht aktualisiert, wenn der Konferenz aufseiten des Office Communications Servers neue Teilnehmer hinzugefügt werden.

Besonderer Hinweis:

Lync Communications Server-Seite: Teilnehmer C / OpenScape 4000 wird der Konferenz hinzugefügt, bevor Teilnehmer C verbunden wird, und „invite/from“ unterscheidet sich vom Basisanruf.

Auf dem Display von Teilnehmer C / OpenScape 4000 wird der konfigurierte Bündelname (OpenScape 4000-System) angezeigt.

OpenScape 4000-Seite: An den Lync Communications Server wird keine Nachricht zur Aktualisierung der Displayanzeige mit „Konferenz“ gesendet.

14.8.4.2.6 MFV

Funktioniert mit 0-15.

14.8.4.2.7 SDES Unterstützung

Sicheres SIP-Trunking wird über SDES zu Microsoft Lync Communication Server unterstützt. Um das Leistungsmerkmal nutzen zu können, wählen Sie das entsprechende SIP Trunk Profil aus und wählen dann den gewünschten **SIP-Trunk Security-Modus**.

14.8.5 Konfigurationsbeispiel

14.8.5.1 OpenScape 4000

OpenScape 4000 Routing-Konfiguration

Trunk- und Routenkonfiguration wie in SIP-Konnektivität > Kapitel 5, „SIP-Carrier / SIP Service Provider konfigurieren“ oder in diesem Konfigurationsbeispiel beschrieben:

- Trunk-Konfiguration

  AMO TDCSU - DEV=HG3550IP

  Außer AMO BFDAT, AMO BCSU, AMO BUEND, AMOTDCSU (ECMAV2-Protokoll) sind noch AMO COT und AMO COP von Interesse:

```
EINRICHTEN-COT:COTNU=80,COTPAR=MVLT&UELM&SAAO&BLOC&LOKN&OLCR&TSCS&VKNN&OL▶
RD&NOFT&KTON;
EINRICHTEN-COP:COPNU=80,BERAMT=FBKW,BERFERN=FBKW;
```

  Routing- und Rufnummernplan-spezifische Informationen siehe unten (AMO TDCSU, AMO COT, AMO COP).

- Konfiguration der Common Gateway Baugruppe

  AMO CGWB (im folgenden Beispiel mit **IPADR=192.168.125.44**) wird zur Konfiguration des verwendeten Trunk-Protokolls (Native SIP), des DNS/SRV-Servers (verwendet von Profil) sowie der Codec-Liste (im Beispiel mit **VAD=NO**) genutzt.

  Das Gateway ist als lokales Gateway mit AMO GKREG konfiguriert. **RFCFMOIP** ist auf **NO** eingestellt.

```
EINRICHTEN-CGWB:LTU=77,EBT=10,SMODE=NORMAL,IPADR=192.168.125.44,NET▶
MASK=255.255.255.0;
AEND-
CGWB:MTYP=CGW,LTU=77,EBT=10,TYP=GLOBIF,MUSTER=213,VLAN=NEIN,VLANID=0,DEFRT=192.1
68.125.234,BITRATE=AUTONEG,TRPRSIP=4,TRPRSIPQ=0,TRPRH323=0,TPRH323A=0,TL▶
SP=4061,DNSIPADR=0.0.0.0;
AEND-CGWB:MTYP=CGW,LTU=77,EBT=10,TYP=SERVIF,LOGINTRM="TRM";
AEND-
CGWB:MTYP=CGW,LTU=77,EBT=10,TYP=ASC,UDPPRTLO=29100,TOSPL="184",TOSSIGNL="104",T3
8FAX=JA,RFCFMOIP=NEIN,RFCDTMF=JA,REDRFC▶
TN=JA,PRIO=PRIO1,CODEC=G711A,VAD=YES,RTP="20";
```

```
AEND-CG►
WB:MTYP=CGW,LTU=77,EBT=10,TYP=ASC,PRIO=PRIO2,CODEC=G729A,VAD=NEIN,RTP="20";
AEND-CG►
WB:MTYP=CGW,LTU=77,EBT=10,TYP=ASC,PRIO=PRIO3,CODEC=G729A,VAD=NEIN,RTP="20";
AEND-CGWB:MTYP=CGW,LTU=77,EBT=10,TYP=DMCDATA,DMCCONN=0;
EINRICHTEN-GKREG:GWNR=11,GWATTR=INTGW&HG3550V2&SIP,WAPLNUM=0,WABE=0,LBER=1,IN►
FO="Direkt SIP nach OCS";
EINR-LDAT:LRTG=300,LDIENST=ALLE,LWERT=1,TGRP=1,ODR=300,LBER=1;
```

- Routing- und Rufnummernplan-Konfigurierung

  Für abgehende Anrufe muss für native SIP-Trunks Blockwahl konfiguriert werden; das Wählmuster muss beispielsweise mit â-Zâ enden.

```
EINRICHTEN-LDPLN:LCRCONF=LCRPATT,WAPLNUM=0,LDP="0"-
"Z",LRTG=1,LBER=1;
```

  Die Regeln für die LCR-Konfiguration hängen von dem zwischen HiPath 4000 und dem Mediation Server verwendeten Rufnummernplan ab.

  Der empfohlene Rufnummernplan ist **NPI= ISDN**, **TON= INTERNATIONAL** (explizites Format).

vHG 3500-Konfiguration

Vergewissern Sie sich, dass die **SIP-Protokollvariante für IP-Networking** auf **Native SIP** (AMO CGWB) eingestellt und das Flag **Profile für Amtsleitungen via Native SIP verwenden** gesetzt ist:

WBM > Explorer > Sprachgateways > Parameter „SIP-Amtsleitungsprofil“

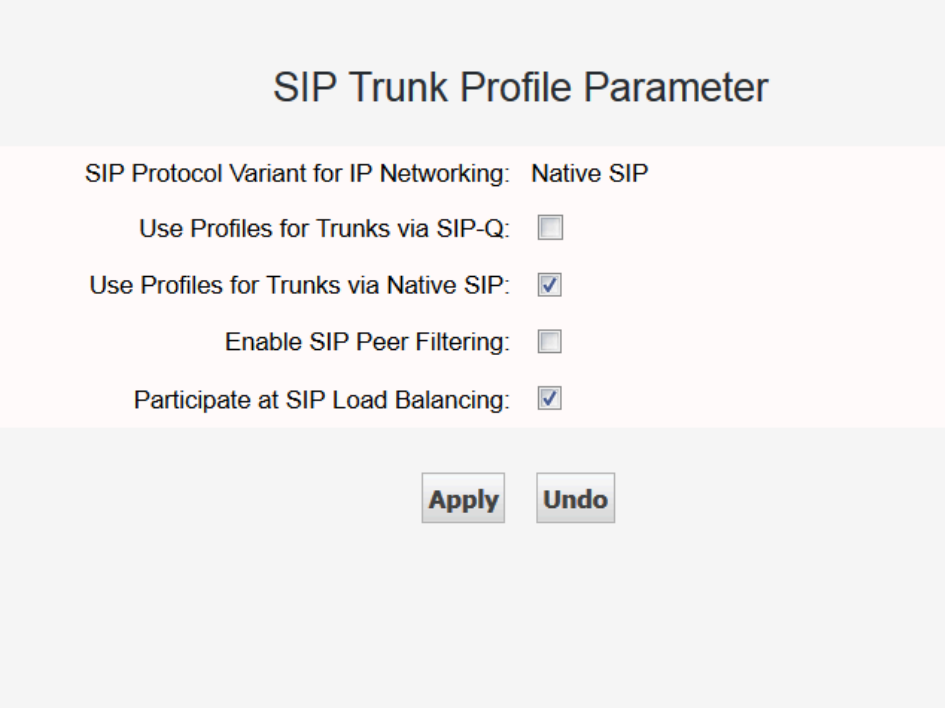


Abbildung 258: Microsoft-Lync - Parameter „SIP-Amtsleitungsprofil“ für vHG 3500

Das SIP-Amtsleitungsprofil Microsoft-*Lync* muss auf dem HiPath 4000 SoftGate auf der Seite „SIP-Amtsleitungsprofil“ aktiviert und die IP-Adresse des Mediation Servers im Feld **IP-Adresse / Hostname** der Registerkarte **Proxy** konfiguriert werden.

Wenn Sie sichere SIP-Trunk-Verbindungen nutzen wollen, wählen Sie den entsprechenden Modus im **SIP-Trunk Security-Modus** Menü. Eine Konfiguration im WBM ist nicht mehr erforderlich.

WBM > Explorer > Sprachgateways > SIP-Amtsleitungsprofil > Microsoft Lync

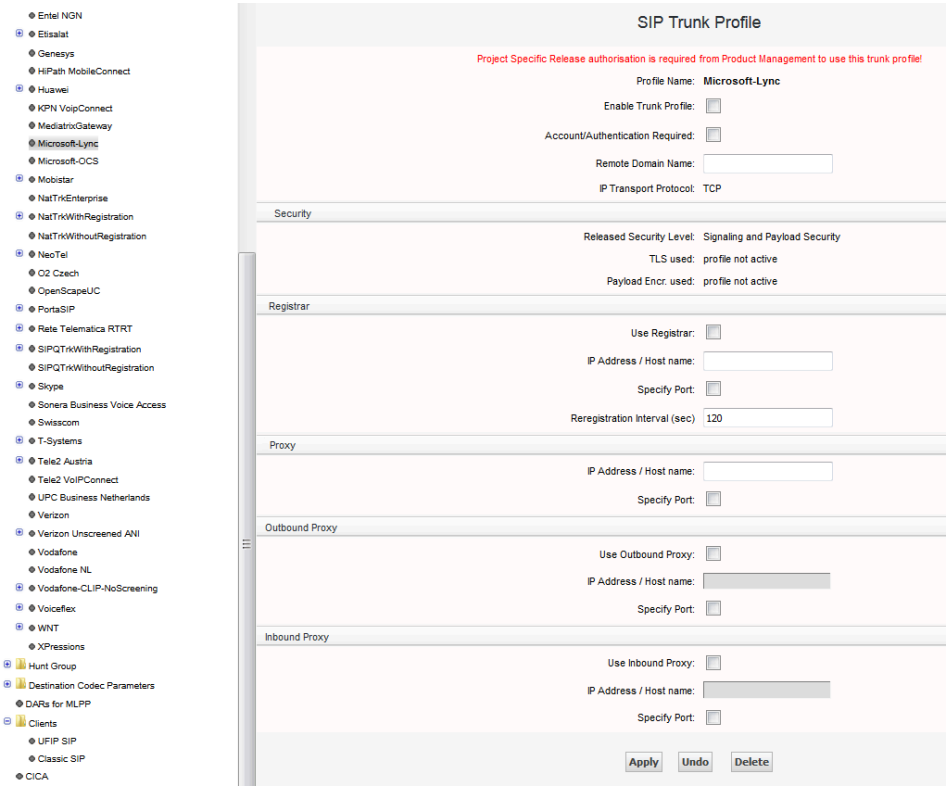


Abbildung 259: Microsoft-Lync - SIP-Amtsleitungsprofilkonfiguration für vHG 3500

Das DMC-Ende muss mit AMO LDAT konfiguriert werden (z. B. `AENDERN-LDAT:LRTG=x,LRTGEL=1,LATTR=DMCEND;`).

14.8.5.2 Microsoft Lync Server/Mediation Server

Führen Sie die folgenden Schritte aus, um die Direct SIP-Konfiguration mit OpenScape 4000 vorzunehmen:

1) Hinzufügen von OpenScape 4000 vSTMI als Gateway zur Lync Server-Topologie
2) Definieren Sie den Wählplan, indem Sie Normalisierungsregeln konfigurieren.
3) Erstellen Sie eine Sprachrichtlinie.
4) Definieren Sie eine Satzkonfiguration.
5) Weisen Sie den Lync-Benutzern Ihre neue Sprachrichtlinie zu.

14.8.5.2.1 Hinzufügen von OpenScape 4000 vSTMI als Gateway zur Lync Server-Topologie

1) Starten Sie den Topology Builder: **Start > Programme > Microsoft Lync Server 2010/2013 > Lync Server Topology Builder**

2) Wählen Sie **PSTN Gateway** und definieren Sie ein neues Gateway:

   Klicken Sie mit der rechten Taste auf **PSTN Gateways** und wählen Sie **New IP/PSTN Gateway**.

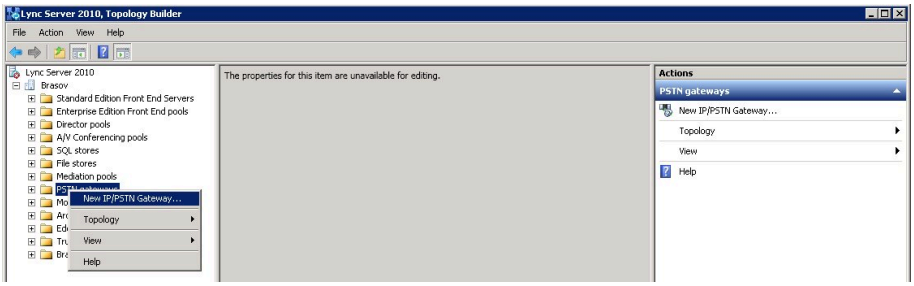


Abbildung 260: Microsoft Lync Server - Neues IP/PSTN-Gateway definieren

3) Dialog **Define New IP/PSTN Gateway**:

   - **Gateway FQDN or IP Address**: Geben Sie die IP-Adresse der OpenScape 4000 an.
   - **Listening port for IP/PSTN gateway**: Geben Sie 5060 ein.
   - Wählen Sie im Feld **Sip Transport Protocol** das **TCP**-Protokoll aus.

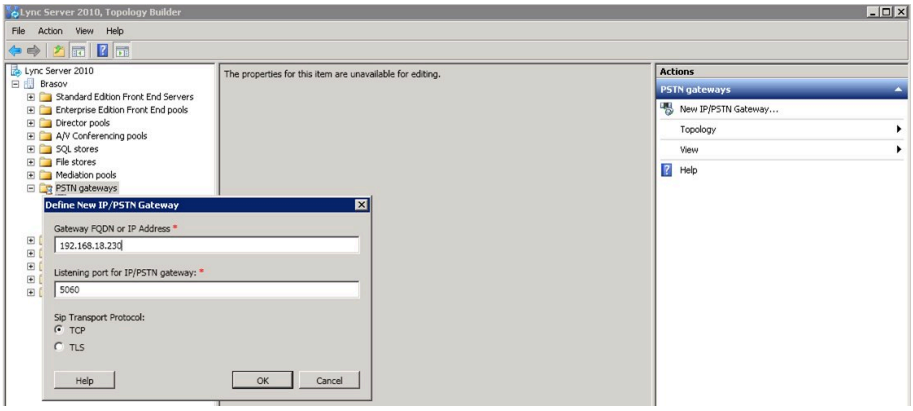


Abbildung 261: Microsoft Lync Server - Eigenschaften für neues IP/PSTN-Gateway

4) Wählen Sie **Mediation-Pools** aus.

   Klicken Sie mit der rechten Maustaste auf **Mediation-Pool**, wählen Sie **Edit Properties** und klicken Sie auf **OK**. Klicken Sie anschließend erneut auf **OK**.

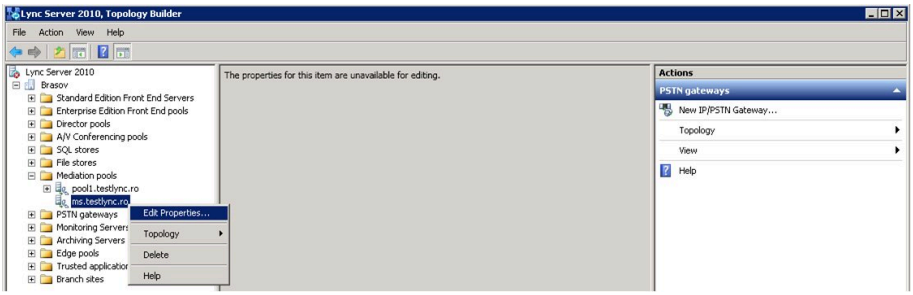


Abbildung 262: Microsoft Lync Server - Eigenschaften für Mediation-Pool

5) Wechseln Sie zur Registerkarte **Gateway on PSTN gateway** und klicken Sie auf **Add**.

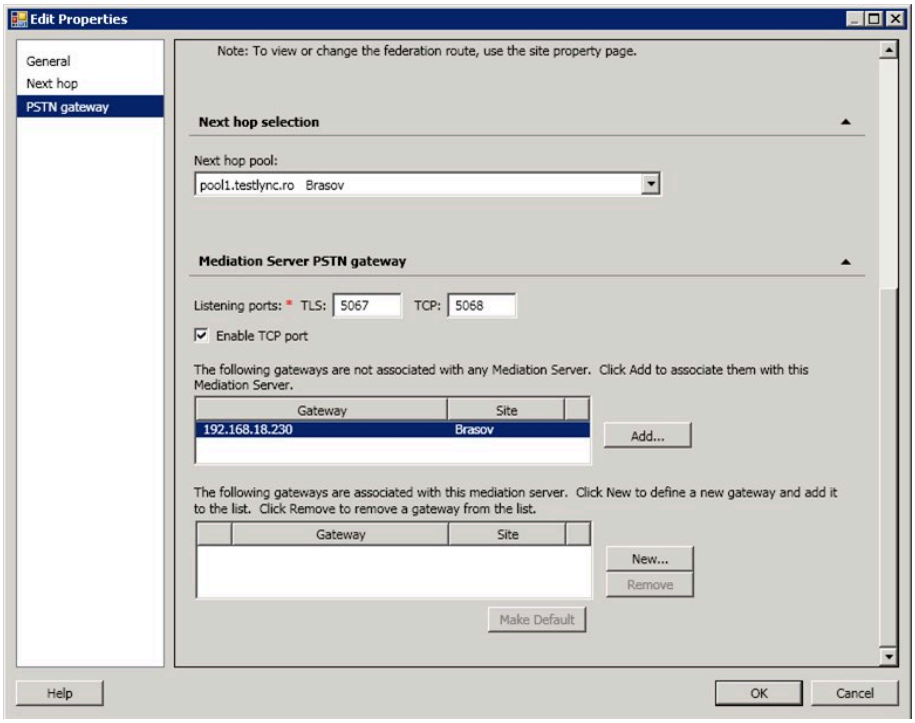


Abbildung 263: Microsoft Lync Server - Eigenschaften für PSTN-Gateway

6) Das Gateway wurde dem Mediation Server zugeordnet. Klicken Sie auf **OK**.

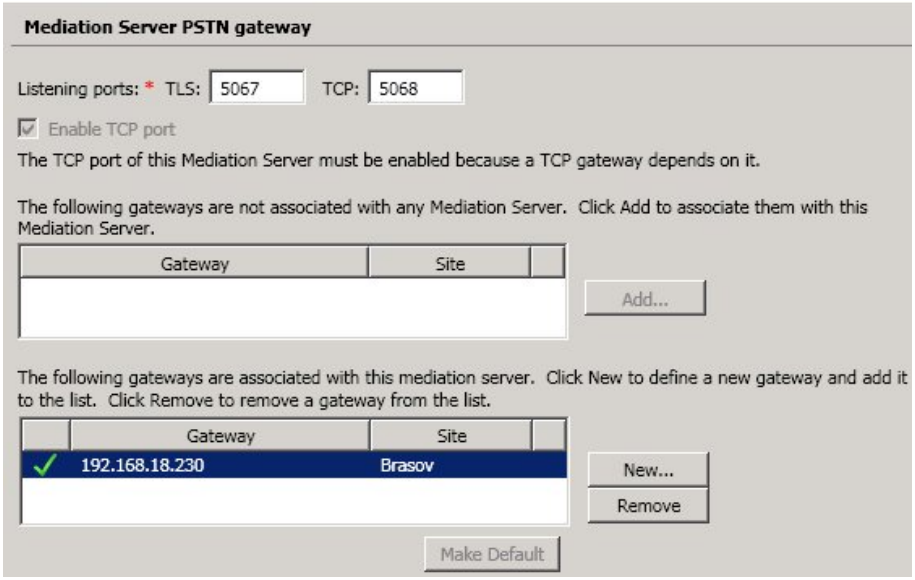


Abbildung 264: Microsoft Lync Server - Gateway zu Mediation Server zuordnen

7) Veröffentlichen Sie Ihre Änderungen der Lync Server-Topologie:

Wählen Sie im Bereich „Actions“ des Topology Builder > Topology > Publish.

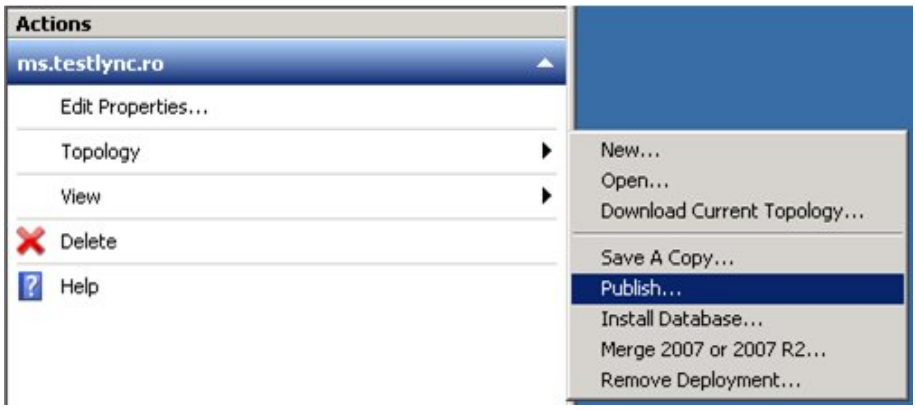


Abbildung 265: Microsoft Lync Server - Änderungen der Lync Server-Topologie veröffentlichen

14.8.5.2.2 Definieren von Wählplanregeln

Definieren Sie im Lync Server Control Panel die Wählplanregeln.

1) Starten Sie das Lync Server Control Panel.

2) **Voice Routing > Registerkarte „Dial Plan“**

3) Erstellen Sie Normalisierungsregeln, die Lync-Benutzern erlauben, OpenScape 4000-Rufnummern und das PSTN anzuwählen.

4) Klicken Sie zum Speichern Ihrer Änderungen auf **Commit** und wählen Sie **Commit all**.

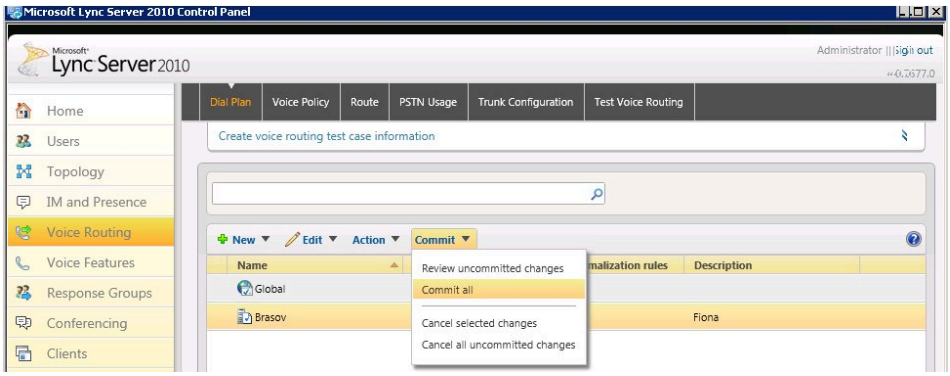


Abbildung 266: Microsoft Lync Server - Wählplanregeln definieren

14.8.5.2.3 Erstellen der Sprachrichtlinie

Benutzer, die einer bestimmten Sprachrichtlinie zugeordnet sind, können über die direkte SIP-Verbindung zum OpenScape 4000-System abgehende Verbindungen herstellen.

1) **Voice Routing > Registerkarte „Voice Policy“**

2) Klicken Sie auf **New**. Klicken Sie je nach dem gewünschten Geltungsbereich der Richtlinie, die Sie erstellen möchten, auf **Site Policy** oder **User Policy**.

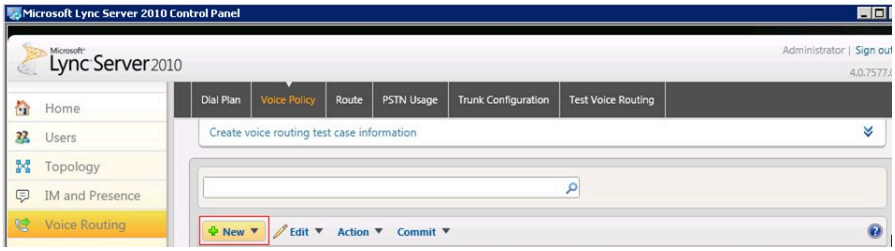


Abbildung 267: Microsoft Lync Server - Sprachrichtlinie erstellen

3) Geben Sie einen eindeutigen Namen und eine Beschreibung für diese Sprachrichtlinie ein.

4) Klicken Sie auf **New**, um eine neue PSTN-Nutzung für diese Richtlinie zu erstellen.

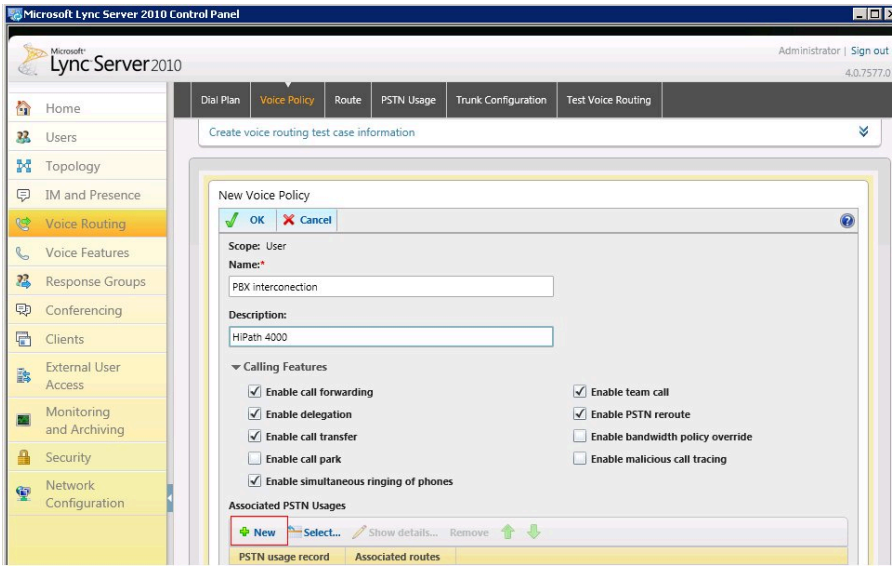


Abbildung 268: Microsoft Lync Server - Neue PSTN-Nutzung erstellen

5) Geben Sie einen Namen für den neuen PSTN-Nutzungsdatensatz ein. Der Name muss in Bezug auf diese spezielle Sprachrichtlinie eindeutig sein. Geben Sie außerdem eine ausführliche Beschreibung des PSTN-Nutzungsdatensatzes ein.

6) Klicken Sie auf **New**, um dieser PSTN-Nutzung eine Route zuzuweisen.

7) Geben Sie einen Namen und eine aussagekräftige Beschreibung für diese Route ein.

8) Klicken Sie auf **Add**, um dieser neuen Route das OpenScape 4000-Gateway zuzuweisen.

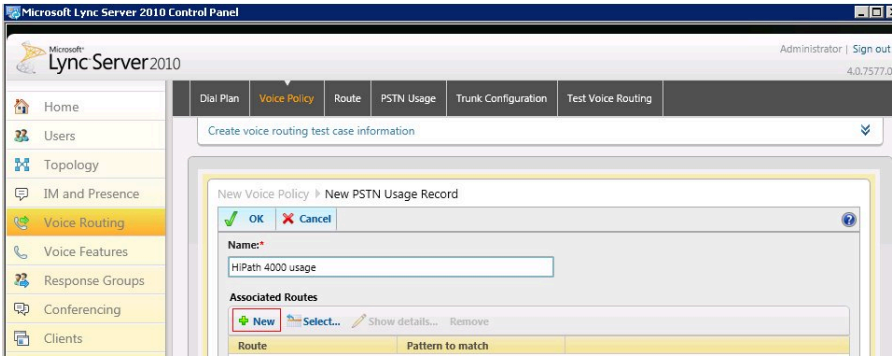


Abbildung 269: Microsoft Lync Server - PSTN-Nutzung eine Route zuweisen

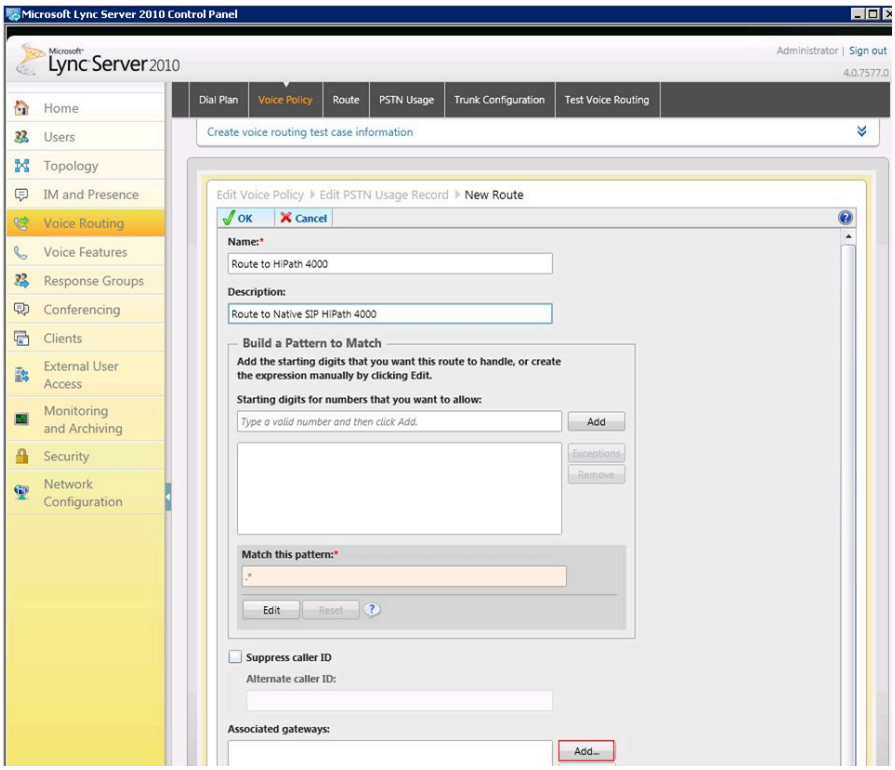


Abbildung 270: Microsoft Lync Server - Route das OpenScape 4000-Gateway zuweisen

9) Wählen Sie das OpenScape 4000-Gateway aus, das Sie zuvor erstellt haben.

10) Klicken Sie in allen eingeblendeten Dialogen auf **OK**, um die Einrichtung der Sprachrichtlinie abzuschließen.

11) Klicken Sie zum Speichern Ihrer Änderungen auf **Commit** und wählen Sie **Commit all**.

14.8.5.2.4 Definieren der Satzkonfiguration

Gehen Sie anschließend wie folgt vor, um das OpenScape 4000 Gateway einer Amtsleitung zuzuweisen, die einem Pool oder einer Site zugeordnet ist:

1) **Lync Server Control Panel > Voice Routing > Registerkarte „Trunk Configuration“**

2) Klicken Sie auf **New**. Klicken Sie je nach dem gewünschten Geltungsbereich der Richtlinie, die Sie erstellen möchten, auf **Site Configuration** oder **Pool Configuration**.

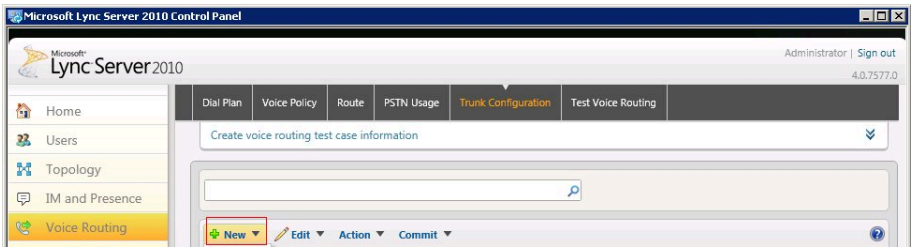


Abbildung 271: Microsoft Lync Server - Satzkonfiguration definieren

3) Wählen Sie einen Pool oder eine Site für diese Satzkonfiguration aus.
4) Klicken Sie im Dialog **New Trunk Configuration** auf **OK**.
5) Klicken Sie zum Speichern Ihrer Änderungen auf **Commit** und wählen Sie **Commit all**.

Wichtig: Achten Sie darauf, dass die Kontrollkästchen **Enable Media bypass** und **Enable refer support** deaktiviert sind.

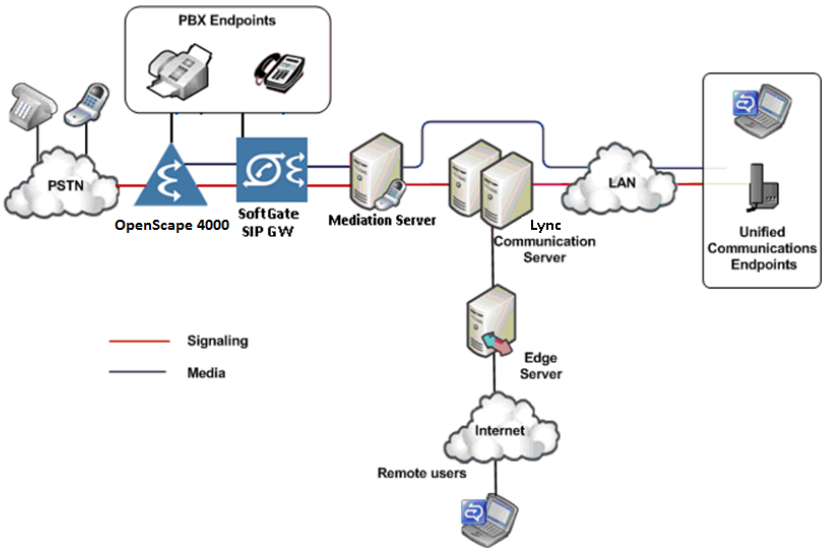
14.9 Skype for Business

14.9.1 Funktionsüberblick

Wichtig: Dieses Leistungsmerkmal wird nur auf projektspezifischer Basis für Konnektivität mit vHG 3500 (OpenScape 4000 SoftGate) bereitgestellt!

Auf SoftGate/STMIX befindliche native SIP-Trunks werden berücksichtigt für die Interoperabilität zwischen OpenScape 4000 und Microsoft Skype for Business über Vermittlungsserver.

Die TLS- und SRTP-Verbindung zwischen OpenScape 4000 und Microsoft Skype for Business über Vermittlungsserver ist optional und kann verwendet werden.



14.9.1.1 Verfügbare Funktionen (Überblick):

- Basic Call
- CLIP/CLIR-Funktionen – Übermittlung von Anrufer-Name und -Rufnummer (Zugelassen und Eingeschränkt)
- Anrufübergabe (Blind, Noch nicht angenommen, Angenommen)
- Anrufweiterleitung (CFA („Call Forward All“) – Anrufweiterleitung für alle Anrufe, CFB („Call Forward Busy“) – Anrufweiterleitung wenn besetzt, CFNA („Call Forward No Answer“) – Anrufweiterleitung wenn nicht angenommen)
- Anruf halten und Anruf wiederaufnehmen
- Dreierkonferenz
- Mehrfrequenzwahlverfahren („Dual-Tone Multi-Frequency“) – DTMF
- Sicherheit

14.9.1.2 Funktionsbeschreibung im Detail

14.9.1.2.1 Basic Call

Funktionalität

- Eingehende Anrufe in OpenScape 4000

– Einem über Skype for Business anrufenden Teilnehmer wird die für einen einfachen Anruf gewählte Nummer angezeigt – Einem über OS4K angerufenen Teilnehmer wird die für einen einfachen Anruf verwendete Nummer und der Name des Anrufers in der ersten Display-Zeile angezeigt – Einem über OS4K verbundenen Teilnehmer wird die für einen einfachen Anruf verwendete Nummer und der Name des Anrufers angezeigt. – Einem über Skype for Business verbundenen Teilnehmer wird die für einen einfachen Anruf gewählte Nummer des Anrufers, aber nicht der Name des Anrufers, angezeigt.

Ausgehende Anrufe zu Skype for Business

– Einem über OS4K anrufenden Teilnehmer wird die für einen einfachen Anruf gewählte Nummer und der Name des SIP-Trunks angezeigt. – Einem über

Skype for Business angerufenen Teilnehmer wird die für einen einfachen Anruf gewählte Nummer und der Name des Anrufers* angezeigt. – Einem über OS4K verbundenen Teilnehmer wird die für einen einfachen Anruf gewählte Nummer und der Name des SIP-Trunks angezeigt. – Einem über Skype for Business verbundenen Teilnehmer wird die für einen einfachen Anruf gewählte Nummer und der Name des Anrufers* angezeigt

---

Wichtig: Wenn die angerufene/verbundene Nummer im globalen Katalog (Active Directory) enthalten ist, dann wird der Name aus dem Active Directory für den angerufenen/ verbundenen Teilnehmer angezeigt.

CLIP/CLIR-Funktionen – Übermittlung von Anrufer-Name und -Rufnummer (Zugelassen und Eingeschränkt)

Einschränkungen

– Benachrichtigungen zu verpassten Anrufen enthalten keine Informationen zu Anzeigenamen, die mit dem anrufenden Teilnehmer verknüpft sind – Die Meldung „Anruf nicht verschlüsselt“ wird auf dem Display angezeigt für den Fall, dass die Sicherheitsfunktionalität aktiviert ist

Besonderer Hinweis:

– Der verwendete Nummernplan ist E.164 (ISDN/International)

14.9.1.2.2 Anrufübergabe

– Gesprächsübergabe (Übergabe von angenommenen Anrufen): keine Display-Aktualisierung für irgendein Gerät;

– Klingeln-Übergabe (Übergabe von noch nicht angenommenen Anrufen): verfügbar auf OS4K-Seite; nicht auf „Skype for Business“-Seite und keine Display-Aktualisierung für irgendein Gerät;

– Blindübertragung: verfügbar auf „Skype for Business“-Seite; nicht auf OS4K-Seite Der ursprüngliche „Skype for Business“-Anrufteilnehmer erhält keine Display-Aktualisierung. Dem Teilnehmer, an den der Anruf übergeben wurde, wird der Name und die Nummer des ursprünglichen „Skype for Business“-Teilnehmers aus Skype for Business beim ersten Aufbauen der Anrufverbindung angezeigt.

Funktionalität

Der OS4K-Benutzer kann Anrufe an einen „Skype for Business“-Teilnehmer, an einen angenommenen Konferenzanruf, an einen noch nicht angenommenen Konferenzanruf (nur auf OS4K-Seite) und blind (nur auf „Skype for Business“-Seite) übergeben.

Anzeige der Übergabe von angenommenen Anrufen – Keine Display-Aktualisierung für irgendein Gerät – CO-Verhalten; Dem anrufenden Teilnehmer wird nach der Übergabe der Name und die Nummer des angerufenen Teilnehmers angezeigt, und dem Teilnehmer, an den der Anruf übergeben wurde, wird der Name und die Nummer des anrufenden Teilnehmers in der ersten Display-Zeile angezeigt.

Anzeige der Übergabe von noch nicht angenommenen Anrufen (nur auf OS4K-Seite) – Keine Display-Aktualisierung für irgendein Gerät – CO-Verhalten; Dem anrufenden Teilnehmer wird nach der Übergabe der Name und die Nummer des angerufenen Teilnehmers angezeigt, und dem Teilnehmer, an den der Anruf

übergeben wurde, wird der Name und die Nummer des anrufenden Teilnehmers in der ersten Display-Zeile angezeigt.

Anzeige der Blindübertragung (nur auf „Skype for Business“-Seite) – Display des übergebenen Teilnehmers wird nicht aktualisiert; Dem anrufenden Teilnehmer wird nach der Übergabe der Name und die Nummer des angerufenen Teilnehmers angezeigt, und dem Teilnehmer, an den der Anruf übergeben wurde, wird der Name und die Nummer des anrufenden Teilnehmers in der ersten Display-Zeile angezeigt.

14.9.1.2.3 Anrufweiterleitung

Funktionalität

Der OS4K-Benutzer kann Anrufe an einen Skype for Business GESCHÄFTSTEILNEHMER weiterleiten. CFA („Call Forward All“) – Anrufweiterleitung für alle Anrufe, CFB („Call Forward Busy“) – Anrufweiterleitung, wenn besetzt (nur auf OS4K-Seite), CFNA („Call Forward No Answer“) – Anrufweiterleitung, wenn nicht angenommen – Möglich, CO-Verhalten;

- Anzeige von Anrufweiterleitung Immer/Wenn besetzt – Unabhängig vom Weiterleitungsziel
  - Dem anrufenden Teilnehmer wird der Name und die Nummer des angerufenen Teilnehmers in der ersten Display-Zeile angezeigt. – Dem Teilnehmer, an den der Anruf weitergeleitet wurde, wird der Name und die Nummer des anrufenden Teilnehmers in der ersten Display-Zeile angezeigt. – Keine sichtbare Anzeige, dass eine Anrufweiterleitung auf irgend einem Display stattgefunden hätte.
- Anzeige von Anrufweiterleitung, wenn Anruf nicht angenommen – Unabhängig vom Weiterleitungsziel
  - Dem anrufenden Teilnehmer wird der Name und die Nummer des angerufenen Teilnehmers in der ersten Display-Zeile angezeigt. – Dem Teilnehmer, an den der Anruf weitergeleitet wurde, wird der Name und die Nummer des anrufenden Teilnehmers in der ersten Display-Zeile angezeigt. – Keine sichtbare Anzeige, dass eine Anrufweiterleitung auf irgend einem Display stattgefunden hätte.

Die Weiterleitungs-Umschaltung erfolgt auf beiden Seiten.

Einschränkungen

Teilnehmer A erhält keine Informationen zur Anrufweiterleitung. Anrufweiterleitung – wenn besetzt – wird von „Skype for Business“ nicht unterstützt. Die Telefonanlage registriert die Anrufweiterleitung nicht. Szenarien mit Sprachnachrichten auf „OpenScape 4000“-Seite sind nicht möglich. Die Anrufweiterleitung per Umleitung ist nicht möglich, beispielsweise werden durch eine Anrufweiterleitung von OS4K zu Skype for Business für einen über Skype for Business eingehenden Anruf keine Ressourcen freigegeben.

14.9.1.2.4 Anruf halten und Anruf wiederaufnehmen

Szenario auf beiden Seiten möglich, OS4K und Skype for Business funktioniert mit Attribut = inaktiv in beide Richtungen -> lokales MoH („Modem on Hold“) wird auf beiden Seiten verwendet

14.9.1.2.5 Dreierkonferenz

Funktionalität

Mögliche Konferenz-Szenarien – CO-Verhalten Anzeige – Bei Konferenzanrufen werden für alle über OS4K zugeschalteten Teilnehmer die

korrekten Anzeige-Informationen für OS4K-Konferenzteilnehmer angezeigt, „Skype for Business“-Teilnehmer werden als externe Teilnehmer angezeigt. Die Anzeige wird auf OS4K nicht aktualisiert, wenn neue Mitglieder auf „Skype for Business“-Seite hinzugefügt werden.

Besonderer Hinweis:

„Skype for Business“-Seite: „Dritter Teilnehmer/OS4K“ wird der Konferenz hinzugefügt, bevor der dritte Teilnehmer verbunden wird, und „Einladung/Von“ unterscheidet sich von „BC“. Die Anzeige für „Dritter Teilnehmer/OS4K“ zeigt den (im OS4K-System) konfigurierten Trunk-Namen an.

OS4K-Seite: Es wird keine Nachricht an OSC mit „Konferenz“ als Display-Aktualisierung gesendet

Einschränkungen

Es wird kein Name und keine Nummer für den OS4K-Benutzer angezeigt, wenn die Einladung zur Konferenz an OS4K versandt wurde. Die Verbindung der OS4K-Teilnehmer an einer „Skype for Business“-Konferenz wird nach Beendigung der Konferenz nicht getrennt. OS4K-Benutzer müssen den Konferenz-Anruf manuell beenden.

14.9.2 Einschränkungen

- Allgemeine Einschränkungen

Zuweisung („Refer“-Funktion) wird nicht unterstützt – Deaktivieren Sie REFER auf „Skype for Business“-Vermittlungsservern – „OS4K REFER“ ist im Profil deaktiviert und keine manuellen Aktionen sind erforderlich Komfortrauschen wird von SoftGate nicht unterstützt.

- Funktionseinschränkungen

– Dual Forking – Gleichzeitiges Klingeln – Videoanrufe – Media Bypass – E911 – DNS Load Balancing wird von OpenScape 4000 nicht unterstützt – Keine Tonsignale auf dem „Skype for Business“-Client nach dem Übergabe-Klingeln von OpenScape 4000 STN – Die Meldung „Anruf nicht verschlüsselt“ wird auf dem Display angezeigt für den Fall, dass die Sicherheitsfunktionalität aktiviert ist – OS4K initiiert die Anrufweiterleitung an Skype for Business, wenn der Anruf von Skype for Business ausgeht, falls die Sicherheitsfunktionalität aktiviert ist – Die Anrufweiterleitung per Umleitung ist nicht möglich

- Der SIP-Trunk, der mit Skype for Business verbunden ist, kann nur auf vSTMI oder STMIX konfiguriert werden.

Siehe oben genannte Einschränkungen auf Funktionsbasis.

- Anrufweiterleitung ist nur verfügbar für Skype for Business, vollständiger Client-Vergleich weiter unten

https://technet.microsoft.com/en-us/library/dn933896.aspx?f=255&MSPPError=-2147217396

Codecs:

– G.711 A-Law, Ping-Zeit = 20 Millisekunden, bevorzugter Codec ist G.711 A-Law – G.729 wird von Skype for Business nicht unterstützt – G.723 wird von SoftGate und Skype for Business nicht unterstützt – Sprechpausenunterdrückung für G.711 ist nicht möglich, wenn eine andere Art von Signalübertragung verwendet wird – Skype for Business verwendet

Comfort Noise PT (13); von SoftGate nicht unterstützt – vHG/OS4K verwendet das Attribut „silenceSupp:on“; von Skype for Business nicht unterstützt – DTMF für RFC2833 wird unterstützt für die Wahltöne 0-15

14.9.3 Spezifische Konfiguration

Siehe Servicehandbuch-Kapitel „SIP-Trunk-Provider“ für Informationen zur allgemeinen Konfiguration

Die folgenden spezifischen Konfigurationsschritte sollten zusätzlich zur Konfiguration des SIP-Trunks zwischen OpenScape 4000 und Skype for Business ausgeführt werden:

1) Konfigurieren Sie das OpenScape-4000-Routing – Siehe Servicehandbuch-Kapitel „SIP-Trunk-Provider“

2) Konfigurieren Sie vHG 3500 – Siehe Servicehandbuch-Kapitel „SIP-Trunk-Provider“

3) Konfigurieren Sie Skype for Business Server 2015.

14.9.3.1 OpenScape-4000-Routing

- DMC-Endpunkt muss konfiguriert werden auf LDAT, z. CHANGE-LDAT:LROUTE=x,LRTEL=1,LATTR=DMCEND;
- Konfiguration von Routing und Nummernplan

Bei ausgehenden Anrufen muss die Blockwahl für den nativen SIP-Trunk konfiguriert werden, das Wählmuster muss also beispielsweise enden auf „-Z“.

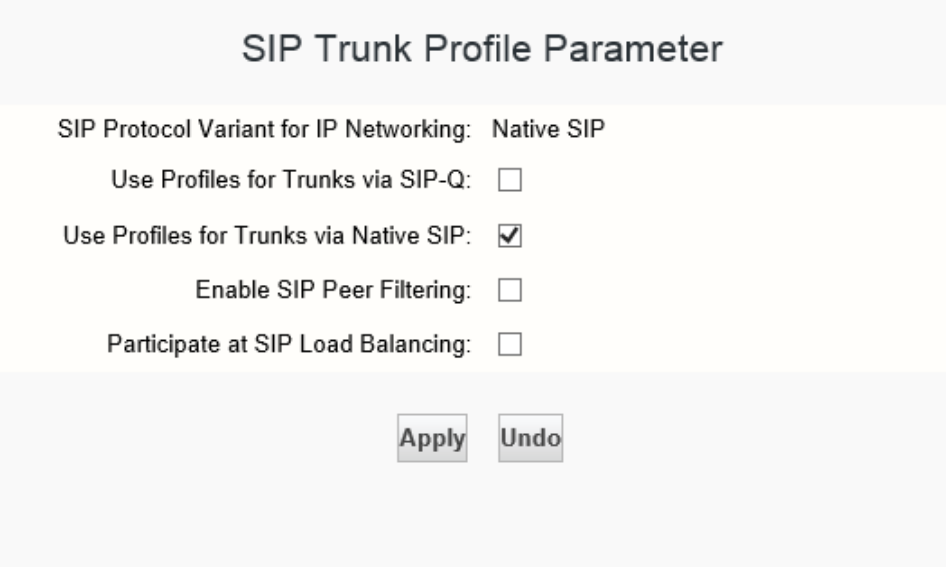
```
ADD-LDPLN:LCRCONF=LCRPATT,DIPLNUM=0,LDP="0"-
"Z",LROUTE=1,LAUTH=1;
```

Der Anrufbegrenzungsmesser kann geändert werden über den Parameter LCREOD in AMO CTIME unter Branch CP1, falls gewünscht;

Die LCR-Konfigurationsregeln sind abhängig davon, welcher Nummernplan zwischen OpenScape 4000 und dem Vermittlungsserver verwendet wird. Der empfohlene Nummernplan ist NPI = ISDN, TON = INTERNATIONAL (explizites Format).

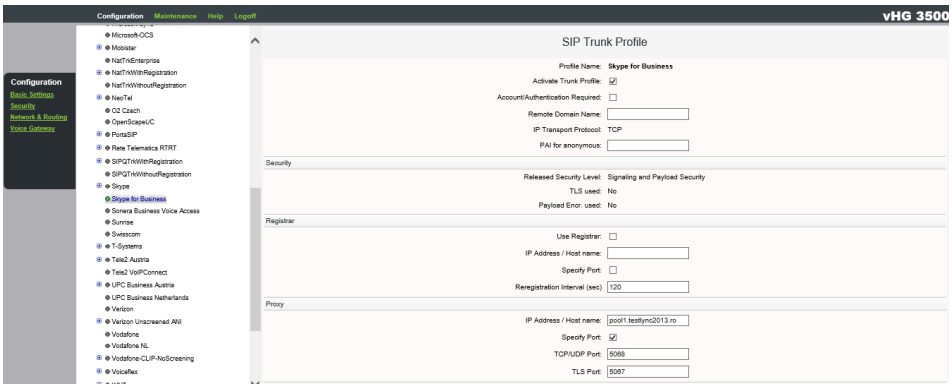
14.9.3.2 Konfiguration von vHG 3500 WBM

Stellen Sie sicher, dass die SIP-Protokollvariante für IP-Netzwerkverbindung eingestellt ist auf Natives SIP-Protokoll (AMO CGWB) und das Flag Profile für Trunks über natives SIP-Protokoll aktiviert ist: WBM > Konfiguration > VoIP-Gateway > SIP-Trunk-Profil-Parameter



14.9.3.2.1 Konfiguration von vHG 3500

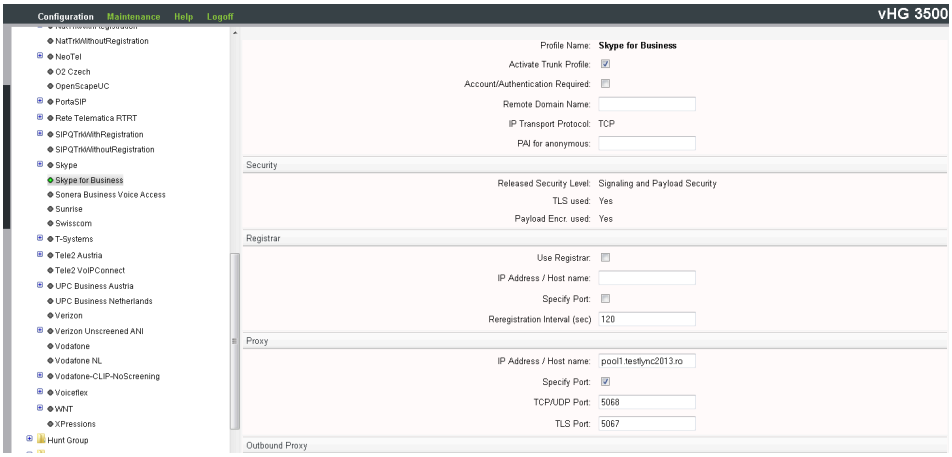
Das „Skype for Business“-Profil muss aktiviert sein, und die IP-Adresse oder der DNS-Name des Vermittlungsservers muss im Feld „IP-Adresse/Host-Name“ auf der Registerkarte „Proxy“ konfiguriert werden.



14.9.3.2.2 Konfiguration von vHG 3500 mit aktivierter Sicherheitsfunktionalität (spezifische Konfiguration)

Das „Skype for Business“-Profil muss aktiviert sein, und die IP-Adresse oder der DNS-Name des Vermittlungsservers muss im Feld „IP-Adresse/Host-Name“ auf der Registerkarte „Proxy“ konfiguriert werden. Zum Aktivieren der Sicherheitsfunktionalität für das Gateway muss das Feld SECLEVEL aus AMO TDCSU auf SECURE eingestellt sein, damit auf der Registerkarte für Gateway-Sicherheitseinstellungen Signal-Übertragung und Nutzlast-Sicherheit die Anzeige für TLS auf YES lautet.

Anmerkung: „Signal-Übertragung und Nutzlast-Sicherheit“ ist optional.



14.9.3.3 Konfiguration von Skype for Business Server 2015

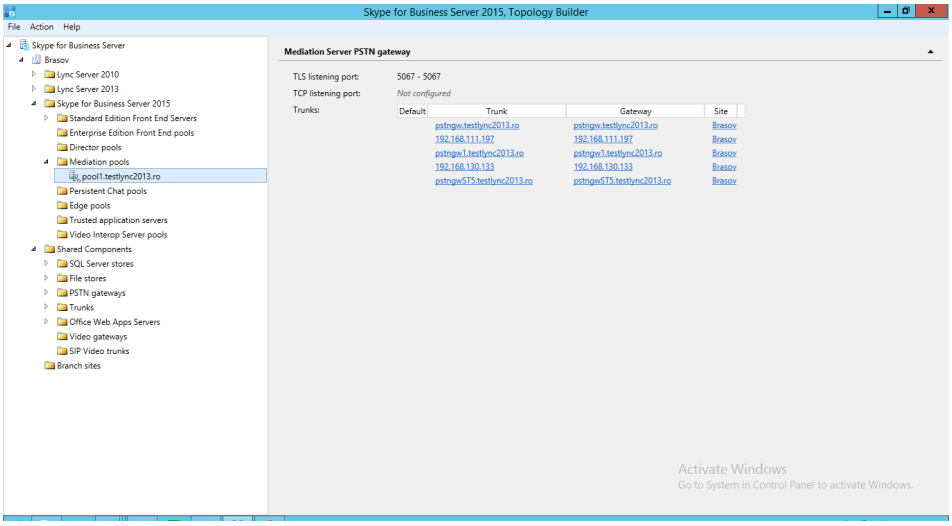
Führen Sie zum Abschließen der direkten SIP-Konfiguration mit OpenScape 4000 die folgenden Schritte aus:

1) Fügen Sie OpenScape 4000 vSTMI (vHG 3500) als Gateway zur Topologie von Skype for Business Server 2015 hinzu.
2) Definieren Sie einen Wählplan, indem Sie Normalisierungsregeln konfigurieren.
3) Erstellen Sie eine VoIP-Richtlinie.
4) Definieren Sie eine Trunk-Konfiguration.
5) Weisen Sie die VoIP-Richtlinie, die Sie erstellt haben, „Skype for Business“-Benutzern zu.

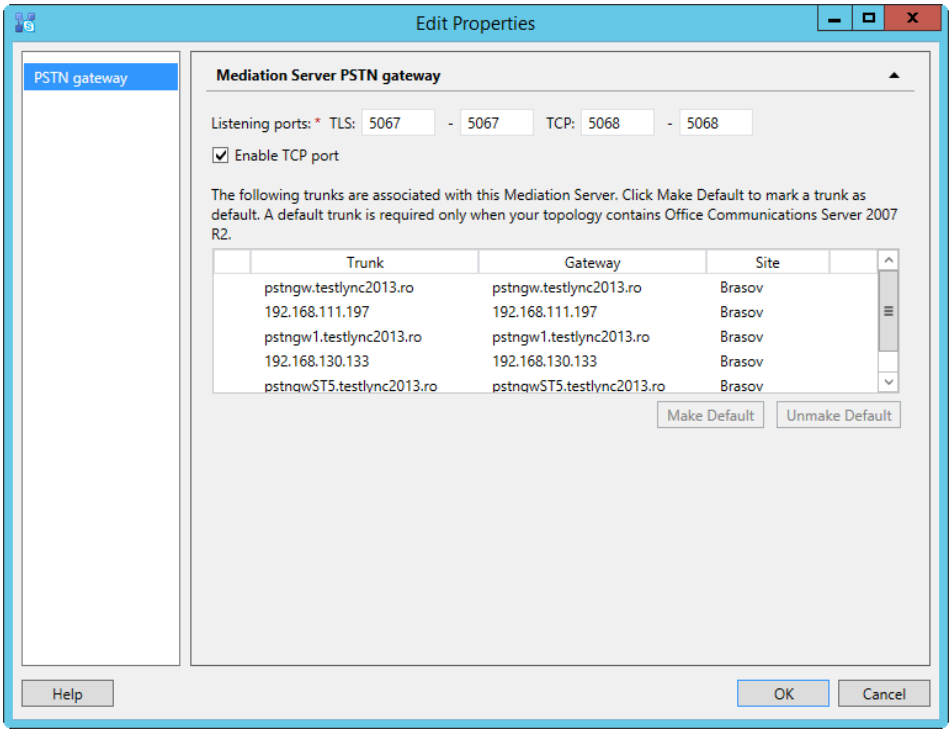
Anmerkung: Auf OpenScape 4000 V8 kann DIRECT STP konfiguriert werden auf vSTMI oder STMIX

14.9.3.4 Hinzufügen von OpenScape 4000 vSTMI als Gateway zur Topologie von Skype for Business Server 2015

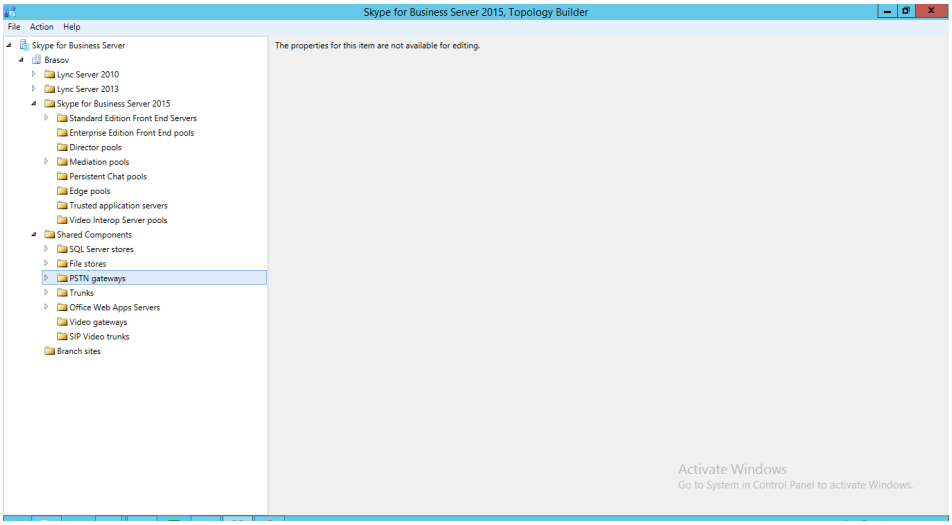
1) Starten Sie Topology Builder: Klicken Sie zuerst auf Start, dann auf Alle Programme, anschließend auf Microsoft Skype for Business Server 2015 und schließlich auf Skype for Business Server 2015 Topology Builder.
2) Erweitern Sie die Anzeige für den Knoten Vermittlungspools.
3) Klicken Sie mit der rechten Maustaste auf den Vermittlungspool, und klicken Sie dann auf Eigenschaften bearbeiten.



1) Aktivieren Sie auf dem PSTN-Gateway für Vermittlungsserver das Kontrollkästchen für die Option TCP-Port aktivieren und legen Sie die Eingangs-Ports 5067 – 5067 für TLS und 5068 – 5068 für TCP fest. Sobald ein neues Gateway definiert ist, wird es hier angezeigt.



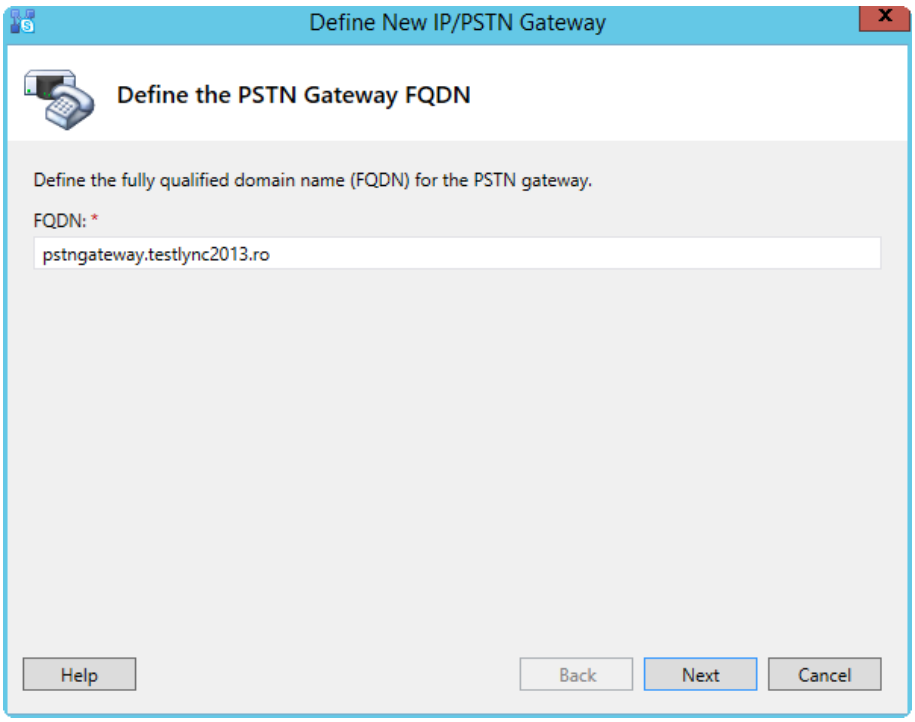
1) Gehen Sie im Feld PSTN-Gateway wie folgt vor: Klicken Sie mit der rechten Maustaste auf PSTN-Gateways und wählen Sie die Option Neues IP-/PSTN-Gateway

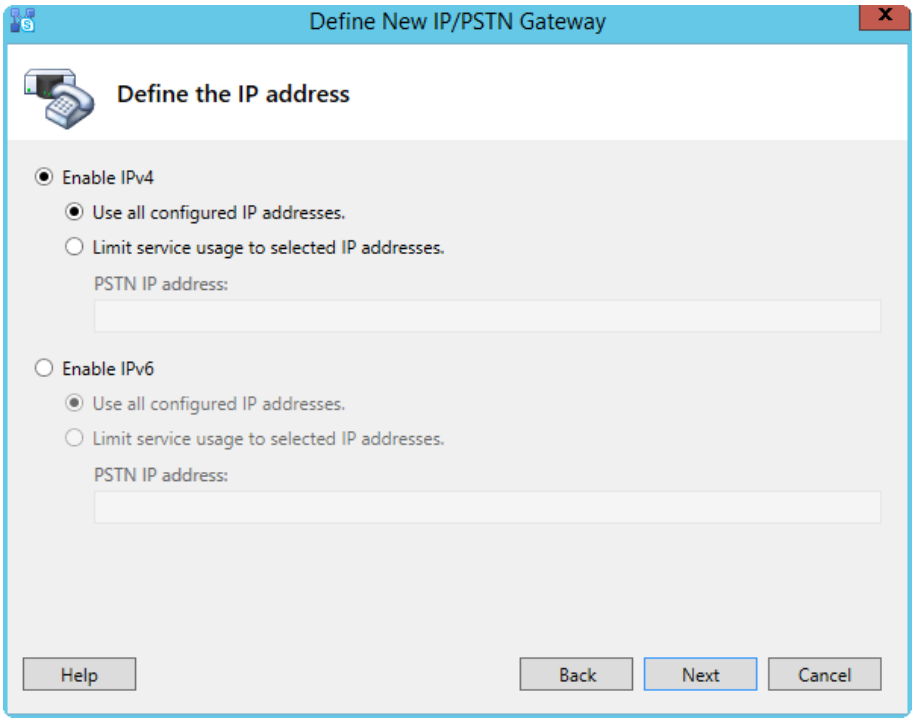


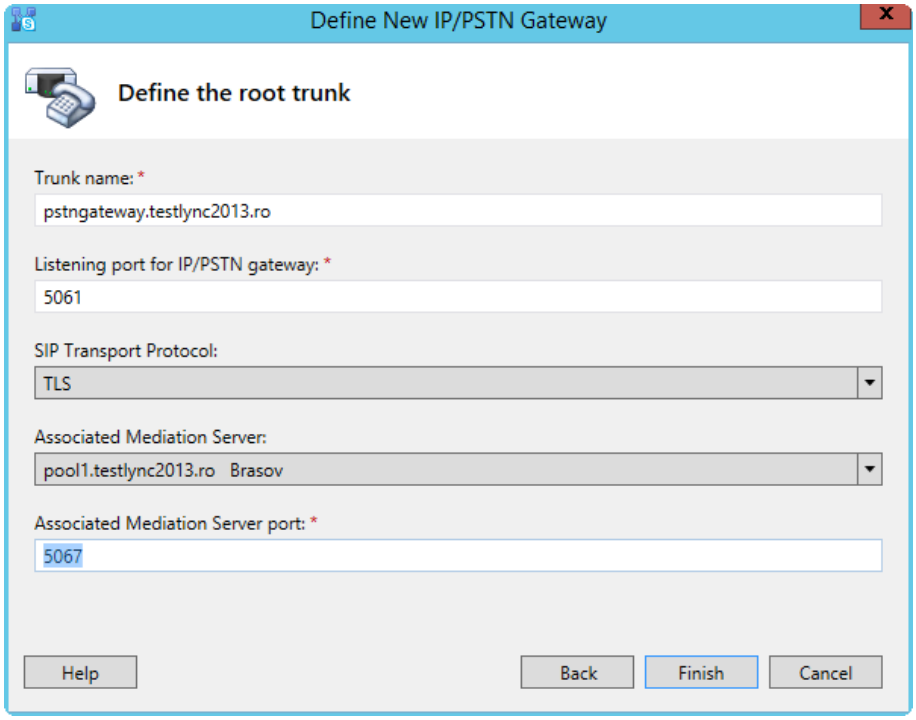
1) Gehen Sie im Dialogfeld Neues IP-/PSTN-Gateway definieren wie folgt vor:

2)
- Geben Sie unter Vollständig qualifizierten Domänennamen (FQDN) für PSTN-Gateway definieren die IP-Adresse oder den vollständig qualifizierten Domänennamen (FQDN) von OpenScape 4000 an.
- Wählen Sie unter IP-Adresse definieren die Option Alle konfigurierten IP-Adressen aus, wenn das Gateway in DNS definiert ist, oder wählen Sie die Option Dienst-Nutzung auf ausgewählte IP-Adressen beschränken aus, um die IP-Adresse manuell festzulegen.
- Legen Sie unter Root-Trunk definieren unter Eingangs-Port für IP-/PSTN-Gateway den Port auf 5060 für TCP-Verbindung oder 5061 für TLS-Verbindung fest.
- Klicken Sie unter SIP-Transport-Protokoll auf TCP für nicht sichere Verbindung oder auf TLS für sichere Verbindung.
- Wählen Sie unter Verknüpfter Vermittlungsserver den Vermittlungsserver aus.

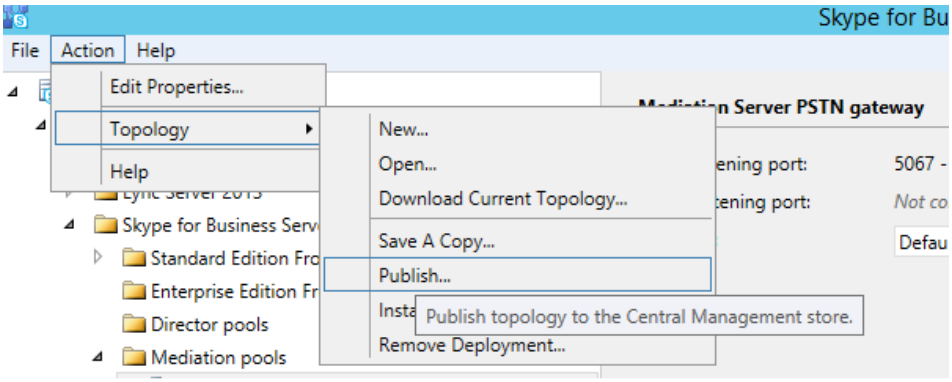
- Wählen Sie unter Verknüpfter Vermittlungsserver-Port die Option 5068 für TCP-Verbindung oder die Option 5067 für TLS-Verbindung aus.







3) Zeigen Sie zum Veröffentlichen Ihrer Änderung an der Topologie von Skype for Business Server 2015 im Aktionsbereich von Topology Builder auf „Topologie“, und klicken Sie dann auf „Veröffentlichen“.



14.9.3.5 Definition eines Wählplans

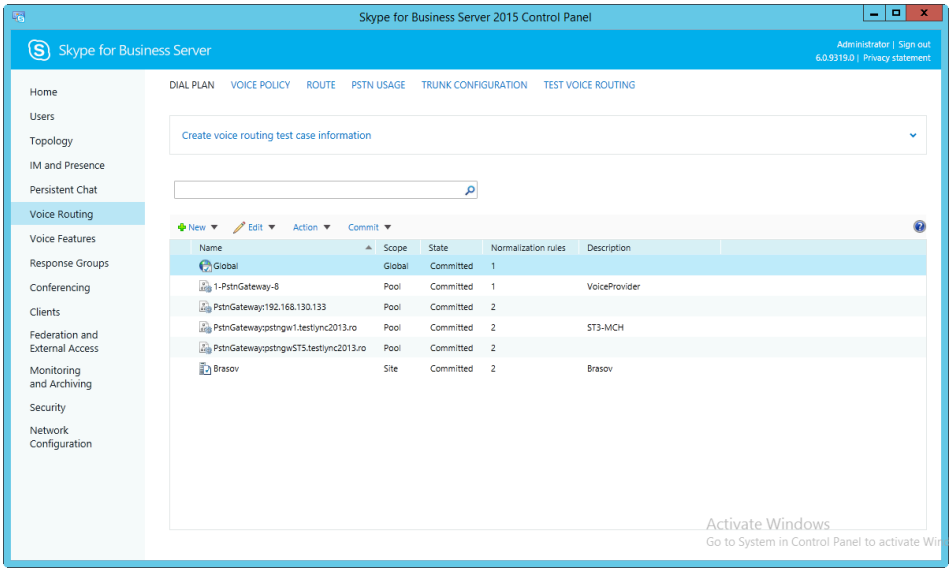
Definieren Sie Wählplan-Regeln in der Systemsteuerung von Skype for Business Server 2015.

1) Starten Sie die Systemsteuerung von Skype for Business Server 2015

2) Klicken Sie auf VoIP-Routing, und klicken Sie dann auf die Registerkarte Wählplan.

3) Erstellen Sie Normalisierungsregeln, die es „Skype for Business“-Benutzern ermöglichen, die Telefone und das PSTN für OpenScape 4000 anzuwählen.

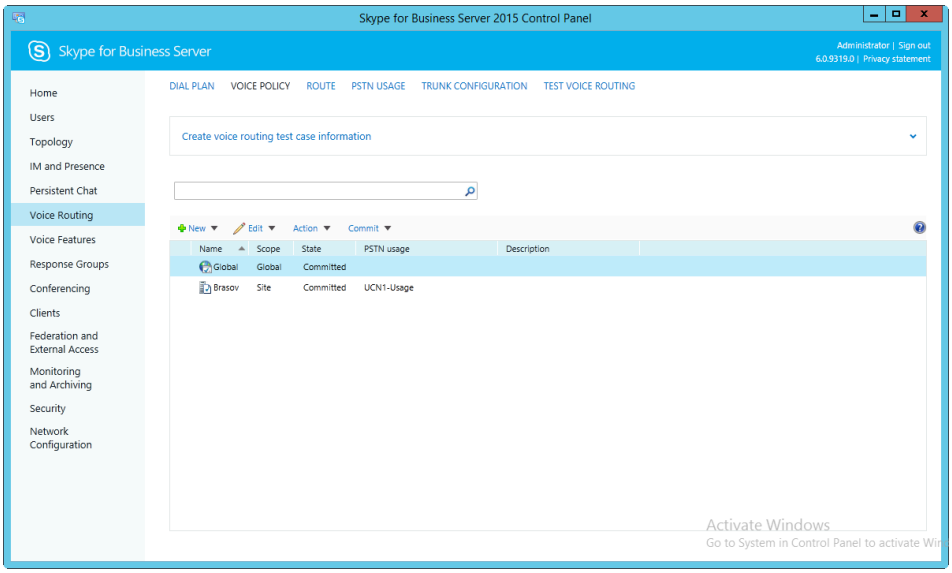
4) Klicken Sie zum Speichern Ihrer Änderungen auf Commit ausführen, und klicken Sie dann auf Commit für alle ausführen.



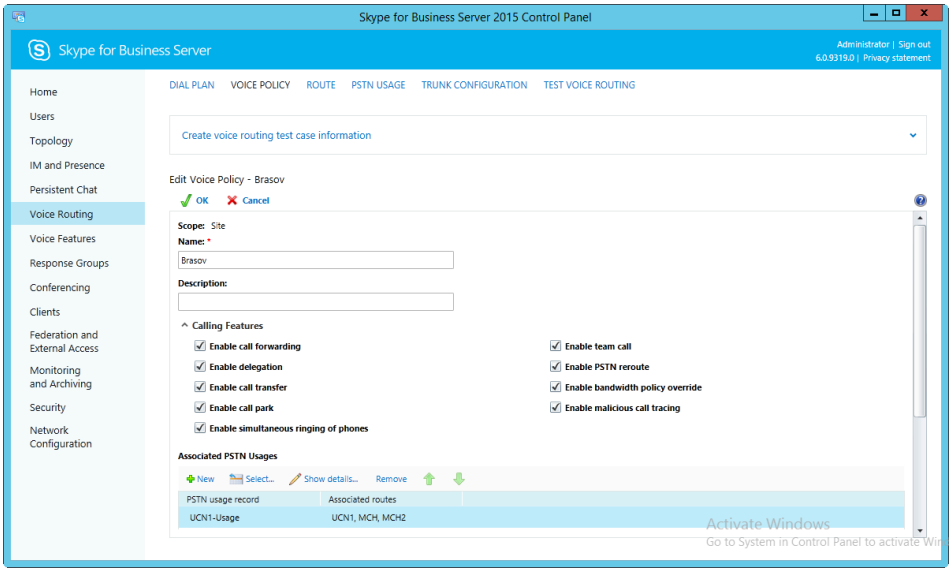
14.9.3.6 Erstellung einer VoIP-Richtlinie

Benutzer, die einer bestimmten VoIP-Richtlinie zugewiesen sind, können mithilfe einer direkten SIP-Verbindung das OpenScape-4000-System anwählen.

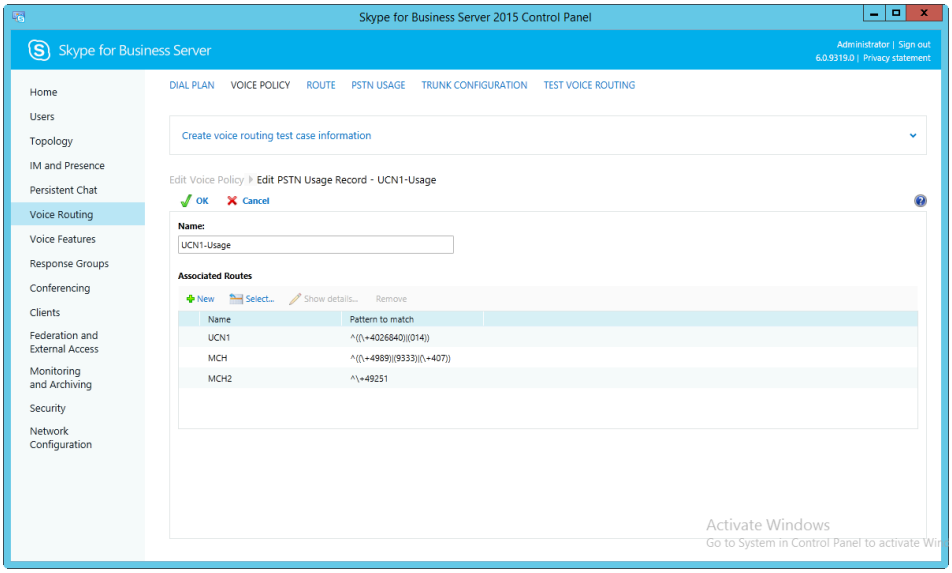
1) Klicken Sie auf VoIP-Routing, und klicken Sie dann auf die Registerkarte VoIP-Richtlinie.
2) Klicken Sie zuerst auf Neu und dann je nach Anwendungsbereich der zu erstellenden Richtlinie auf Site-Richtlinie oder Benutzer-Richtlinie.



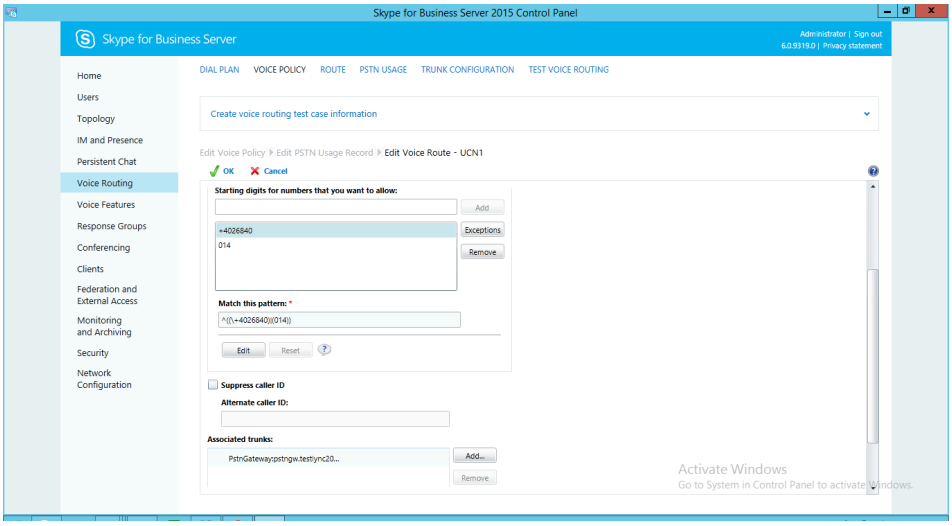
1) Vergeben Sie einen eindeutigen Namen für diese VoIP-Richtlinie und geben Sie eine Beschreibung ein (optional).
2) Erstellen Sie eine neue PSTN-Verwendung für diese Richtlinie und klicken Sie dann auf Neu.



1) Geben Sie einen Namen für den neuen PSTN-Verwendungseintrag an. Der Name muss für diese VoIP-Richtlinie eindeutig sein. Geben Sie auch eine detaillierte Beschreibung des PSTN-Verwendungseintrags ein.
2) Klicken Sie zum Verknüpfen einer Route mit dieser PSTN-Verwendung auf Neu.



1) Vergeben Sie einen Namen für diese Route und geben Sie eine aussagekräftige Beschreibung ein.
2) Klicken Sie zum Verknüpfen des OpenScape-4000-Gateways mit dieser neuen Route auf Hinzufügen.

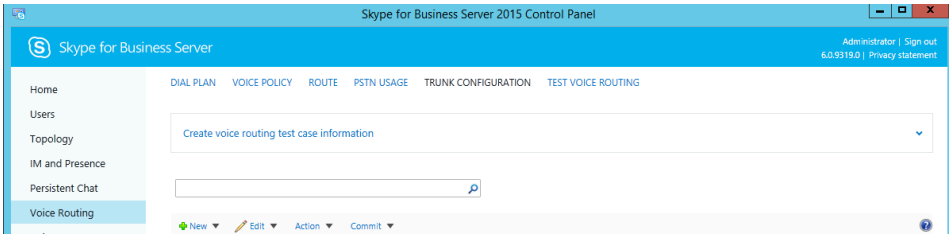


1) Wählen Sie das OpenScape-4000-Gateway aus, das Sie zuvor erstellt haben.
2) Klicken Sie in allen unterschiedlichen Dialogfeldern auf OK, um die Erstellung der VoIP-Richtlinie abzuschließen.
3) Klicken Sie zum Speichern Ihrer Änderungen auf Commit ausführen, und klicken Sie dann auf Commit für alle ausführen.

14.9.3.7 Definition einer Trunk-Konfiguration

Der nächste Schritt besteht darin, das OpenScape-4000-Gateway einer Leitung zuzuordnen, die wiederum einem Pool oder einer Site zugeordnet ist.

1) Klicken Sie in der Systemsteuerung von Skype for Business Server 2015 auf VoIP-Routing, und klicken Sie dann auf die Registerkarte Trunk-Konfiguration.
2) Klicken Sie zuerst auf Neu und dann je nach Anwendungsbereich der zu erstellenden Richtlinie auf Site-Konfiguration oder Pool-Konfiguration.

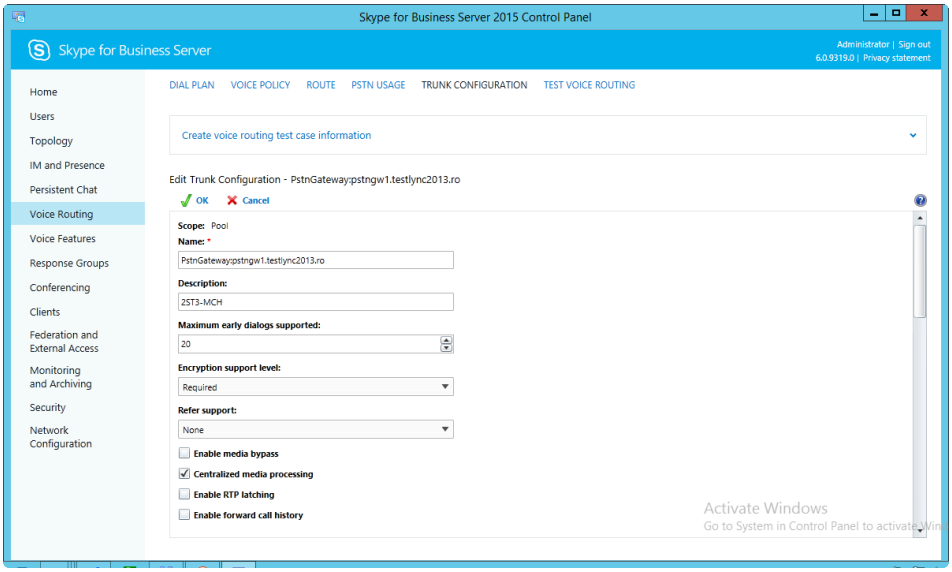


1) Wählen Sie einen Pool oder eine Site für diese Trunk-Konfiguration aus.
2) Klicken Sie im Dialogfeld Neue Trunk-Konfiguration auf OK.
3) Klicken Sie zum Speichern Ihrer Änderungen auf Commit ausführen, und klicken Sie dann auf Commit für alle ausführen.

Anmerkung: Stellen Sie sicher, dass die Option Media Bypass aktivieren deaktiviert ist, und dass Refer-Support aktivieren auf „None“ eingestellt ist.

---

1) Wählen Sie zum Aktivieren der Verschlüsselung die Option Erforderlich auf der Dropdown-Liste Support-Stufe für Verschlüsselung aus.

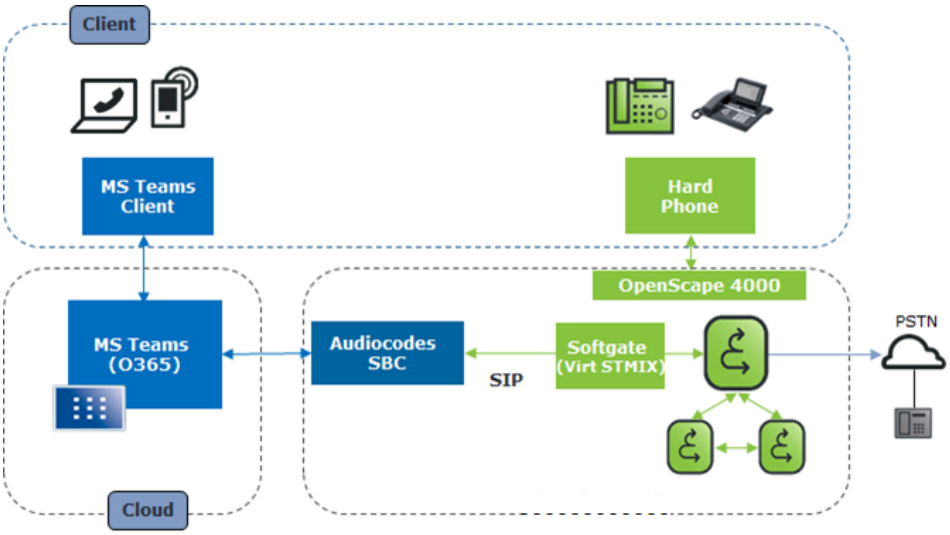


1) Klicken Sie zum Speichern Ihrer Änderungen auf Commit ausführen, und klicken Sie dann auf Commit für alle ausführen.

14.10 MS Teams DR mit Audiocodes SBC

14.10.1 Funktionsüberblick

Auf SoftGate/STMIX befindliche native SIP-Trunks werden berücksichtigt für die Interoperabilität zwischen OpenScape 4000 und MS Teams über Audiocodes SBC.



14.10.2 Einschränkungen und Hinweise

- Allgemeine Einschränkungen

Zuweisung („Refer“-Funktion) wird nicht unterstützt

- Funktionseinschränkungen

Informationen ausgeben: Rufnummer

Hinweis bei Halten: Warteschleifenmusik (keine Displayinformationen)

Keine Aktualisierung der Anzeige nach Anrufumleitung

14.10.3 Konfiguration

Siehe Kapitel Native SIP Trunking on page 898 für die allgemeine Konfiguration.

SIP-Trunk Profile MS-Teams

14.11 MS Teams Direct Routing mit OpenScape SBC

OpenScape 4000 verbunden mit Microsoft Teams Direct Routing über Atos-Unify OpenScape SBC.

14.11.1 Netzwerktopologie

Das folgende Blockdiagramm zeigt die Teams Direct Routing-Verbindungstopologie, wobei die Teams-Telefonanlage direkt mit OpenScape SBC verbunden ist.

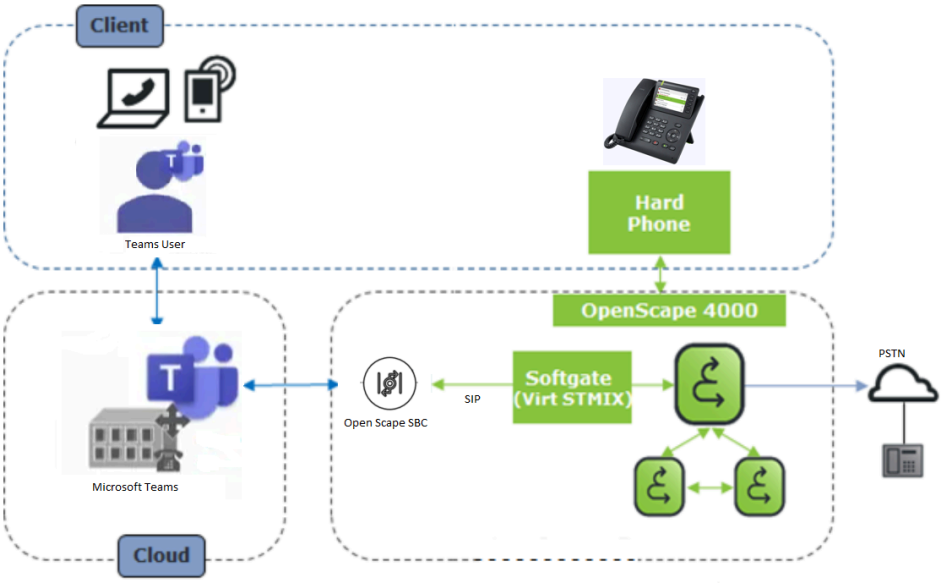


Abbildung 272: Teams Direct Routing-Verbindung

Auf dem SoftGate/STMIX befindliche native SIP-Leitungen werden für die Interoperabilität zwischen OpenScape 4000 und MS Teams über OpenScape SBC berücksichtigt.

14.11.2 Konfiguration OpenScape 4000

14.11.2.1 AMO-Konfiguration

OpenScape 4000 Interworking mit OS SBC und MS Teams unterstützt zwei Setups mit:

- Drei SIP-Trunks (Native SIP-Trunks auf dem SoftGate/STMIX), die über den Clustered-Modus mit dem SBC verbunden sind.
- Nur eine SIP-Leitung.

Zum Konfigurieren OpenScape 4000-Routings siehe Native SIP Trunking on page 898 für die allgemeinen Konfigurationsschritte.

14.11.2.2 STMIX/STMIY vHG WBM-Konfiguration

In diesem Kapitel wird die Konfiguration für die STMIX/STMIY/vHG WBM-Seite vorgestellt. Das MS Teams-Leitungsprofil muss konfiguriert und aktiviert werden.

Führen Sie die folgenden Schritte aus:

1) Gehen Sie zu **vHG WBM > Configuration > Voice Gateway**, klappen Sie **SIP Trunk Profiles (SIP-Leitungsprofile)** auf und klicken Sie auf **MS Teams**.

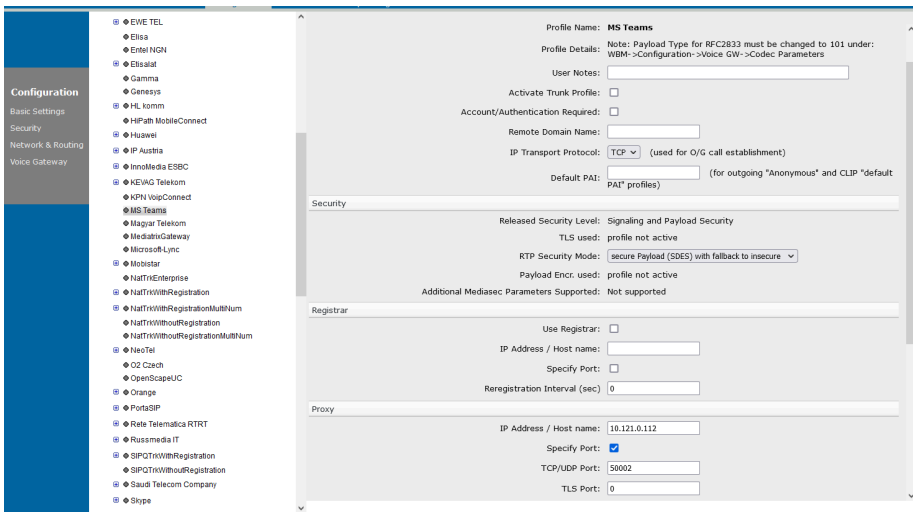


Abbildung 273: MS Teams

2) Aktivieren Sie in den **Proxy**-Einstellungen das Kontrollkästchen **Specify port (Port angeben)** und geben Sie Folgendes ein:

   - **IP-Adresse /Hostname:** SBC LAN IP.

     Anmerkung: SBC LAN IP ist die für das direkte Routing zu MS Teams verwendete Core Side IP des SBC.

   - **TCP/UDP-Port:** 50002.

   Klicken Sie auf die Schaltfläche „Apply“ (Übernehmen).

   Klicken Sie auf die Schaltfläche „OK“.

3) Nach dem Durchführen der obigen Konfiguration muss das Leitungsprofil aktiviert werden:

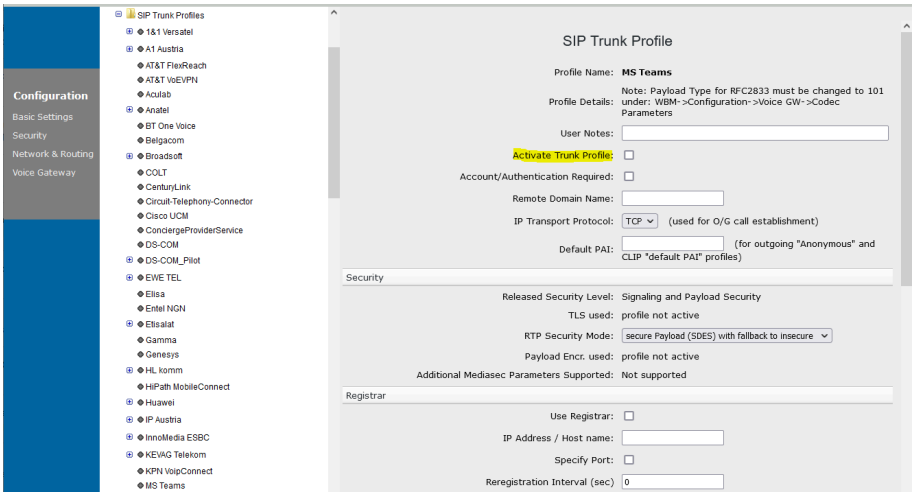


Abbildung 274: Leitungsprofil aktivieren

Aktivieren Sie das Kontrollkästchen **Activate Trunk Profile (Leitungsprofil aktivieren)**.

Klicken Sie auf die Schaltfläche „Apply“ (Übernehmen).

Klicken Sie auf die Schaltfläche „OK“.

4) Aktivieren Sie **SIP OPTIONS** für die Keep Alive-Kommunikation mit MS Teams:

   Gehen Sie zu **vHG WBM > Configuration > Voice Gateway > SIP Parameters**.

   Der Standardwert für **Trunking Parameters > SIP OPTIONS ping interval** ist **0**. Er muss auf einen höheren Wert gesetzt werden.

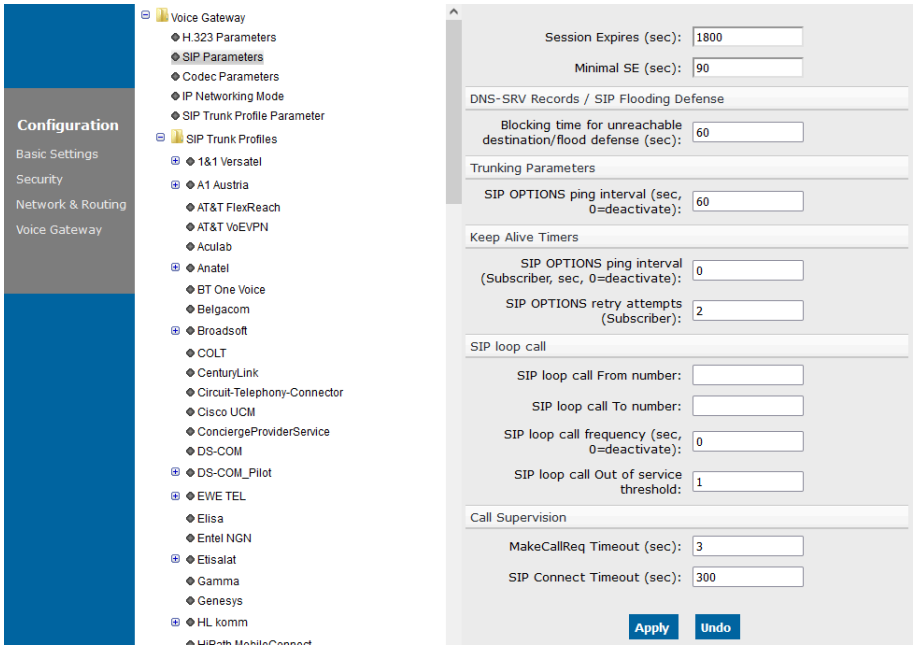


Abbildung 275: SIP OPTIONS Ping-Intervall

   Klicken Sie auf die Schaltfläche „Apply“ (Übernehmen).

   Klicken Sie auf die Schaltfläche „OK“.

5) Wiederholen Sie den Vorgang für die übrigen vHGs (wenn die gewünschte Konfiguration vier vHGs verwendet).

14.11.3 OpenScape SBC-Konfiguration

In diesem Kapitel wird die Konfiguration von OpenScape SBC für das Zusammenspiel mit Teams Direct Routing beschrieben. OpenScape SBC wird mit der Verbindung zu OpenScape 4000- und Teams Phone System (remote)-Endpunkten konfiguriert.

14.11.3.1 Kernbereichsschnittstelle

Verwenden Sie für die Verbindung von OpenScape SBCs eth0 (Core)-Schnittstelle zu OpenScape 4000 die TCP-Portnummer.

Gehen Sie zu **OS SBC Management Portal > Network/Net Services (Netzwerk/Netzdienste)**.

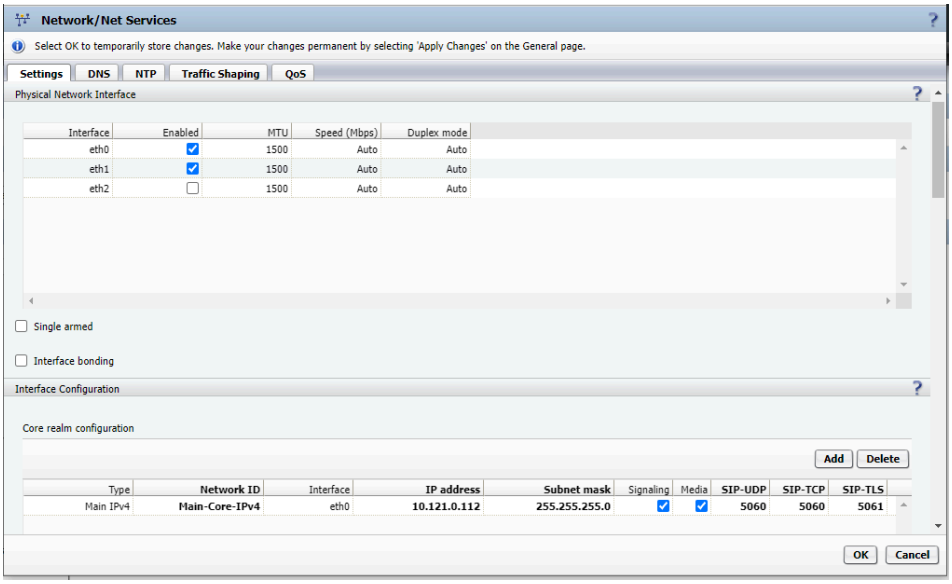


Abbildung 276: Netzwerk/Netzdienste

Stellen Sie auf der Registerkarte **Settings (Einstellungen)** im Bereich **Core Realm Configuration (Konfiguration des Kernbereichs)** sicher, dass für die Schnittstelle **eth0** der Wert des Felds **SIP-TCP** 5060 lautet.

Klicken Sie auf die Schaltfläche „OK“.

Klicken Sie auf der Hauptseite von SBC auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.2 SIP Server

Es gibt zwei mögliche Konfigurationen:

- Simplexmodus mit einem konfigurierten vHG.
- Clustermodus mit mehr als einer konfigurierten vHG

Die SIP-Konnektivität zu OpenScape 4000 wird im Fenster **OS SBC Management Portal > VOIP > SIP-Server-Einstellungen** konfiguriert.

Simplexmodus

Die folgenden Parameter müssen im Fenster **SIP-Server-Einstellungen** eingegeben werden:

- **Comm System Typ (Art des Kommunikationssystems)**: Simplex
- **Target Type (Zieltyp)**: Binding (Verbindlich)
- **Primärer Server:** 10.121.121.138 (vHG-Adresse)
- **Transportprotokoll:** TCP
- **Port:** 5060 (abhörender Port für vHG)

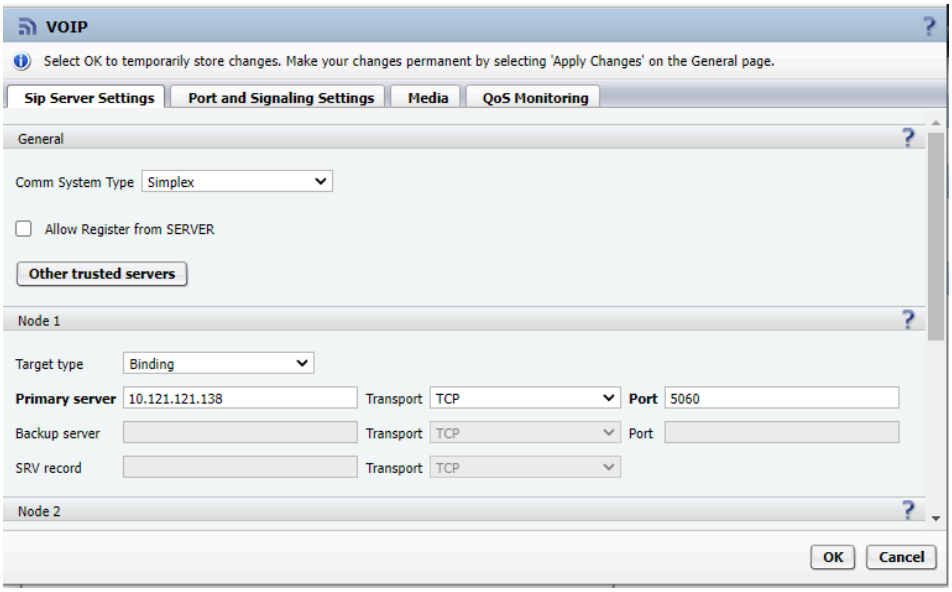


Figure 277: Simplexkonfiguration

Klicken Sie auf die Schaltfläche OK, wenn die oben genannten Parameter eingestellt sind. Klicken Sie anschließend auf der OS SBC-Hauptseite auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

Geclusterter Modus

Wählen Sie im Fenster „Sip Server Settings“ (Sip-Servereinstellungen) für „Comm System Type“ (Art des Kommunikationssystems) die Option „Clustered“.

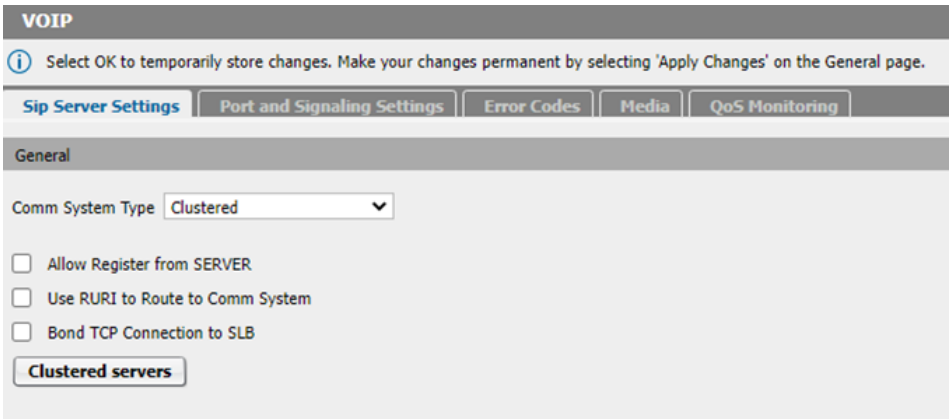


Figure 278: Geclusterter Modus

Klicken Sie anschließend auf die Schaltfläche **Clustered Server** und fügen Sie alle unter Kapitel 14.11.2.2 konfigurierten vHGs hinzu. Klicken Sie auf die Schaltfläche „Add“ (Hinzufügen), um jede vHG auszuwählen und die folgenden Parameter einzugeben:

- **Group Name (Name der Gruppe):** MS_TEAMS (Anzeigename)
- **Node Name:** Teams_SP1 (Anzeigename)
- **Priorität:** 1
- **IP-Adresse oder FQDN:** 10.121.121.138 (vHG-Adresse)
- **Port:** 5060 (abhörender Port für vHG)
- **Transportprotokoll:** TCP

Klicken Sie zweimal auf die Schaltfläche OK, wenn die oben genannten Parameter eingestellt sind. Klicken Sie auf der Hauptseite von OS SBC auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

Das Fenster **Clustered servers (Geclusterte Server)** sollte wie in der folgenden Abbildung aussehen:

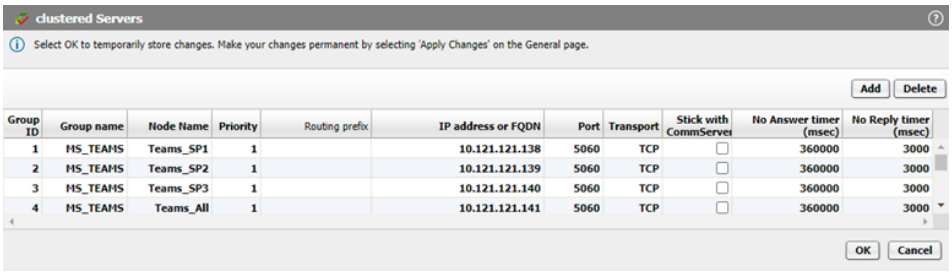


Figure 279: Geclusterte Server

Navigieren Sie zu **OS SBC Management Portal > VOIP > Fehlercodes** und stellen Sie sicher, dass die Option **Routing für alle Codes aktivieren** aktiviert ist.

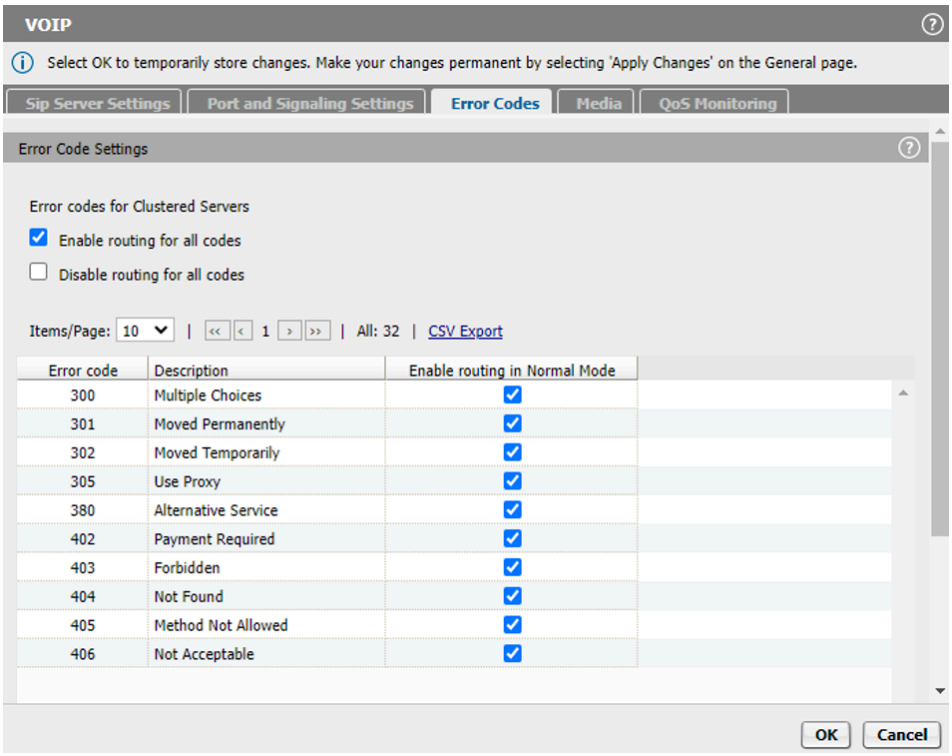


Figure 280: Routing für alle Codes aktivieren

Sobald die Option **Routing für alle Codes aktivieren** aktiviert ist, klicken Sie auf die Schaltfläche OK. Klicken Sie auf der Hauptseite von OS SBC auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.3 Zertifikate

Die Microsoft Phone System Direct Routing-Schnittstelle erlaubt nur TLS-Verbindungen für SIP-Verkehr von den SBCs mit einem Zertifikat, das von einer der vertrauenswürdigen Zertifizierungsstellen von Microsoft signiert wurde.

Das Zertifikat muss den FQDN des SBC als Common Name (CN) im Betrefffeld enthalten. Zertifikate mit einem Platzhalter im Feld „Subject Alternate Name“ (Alternativer Antragstellername) des Zertifikats, die RFC2818 entsprechen, werden ebenfalls unterstützt.

Weitere Informationen zum Zertifikat und die aktuell von Microsoft unterstützten Zertifizierungsstellen finden Sie auf der Microsoft-Website:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc.

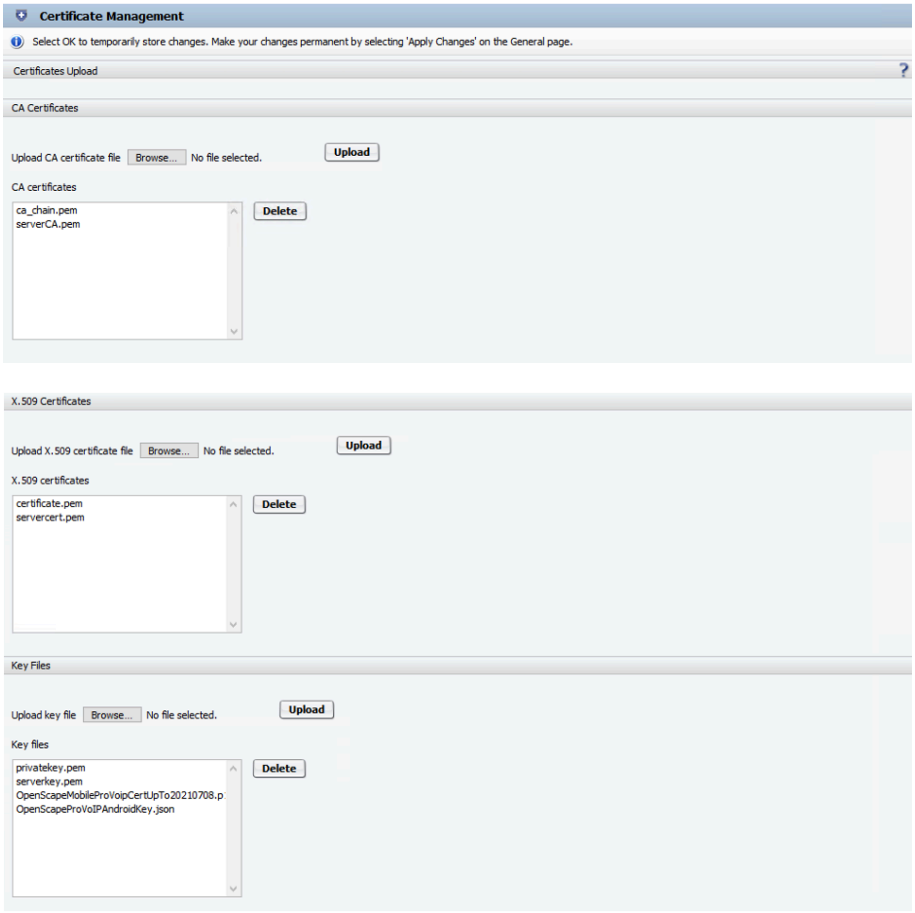
Für die OpenScape SBC TLS-Verbindung zur Microsoft-Telefonanlage werden 3 Dateien im pem-Format von der Zertifizierungsstelle benötigt:

- CA-Zertifikat (z. B. ca_chain.pem)
- Serverzertifikat für OS SBC (z. B. certificate.pem)
- Privater Schlüssel des OS SBC-Server-Zertifikats, der für die CSR an die CA verwendet wird (z. B. privatekey.pem)

Die oben genannten Dateien müssen auf OS SBC hochgeladen und für die TLS-Verbindung mit der Microsoft Phone System-Schnittstelle verwendet werden. Gehen Sie dazu wie folgt vor:

1) Navigieren Sie zu **OS SBC Management Portal > Security > General (OS SBC Management Portal > Sicherheit > Allgemein)** und klicken Sie auf **Certificate Management (Zertifikatsverwaltung).**

2) Laden Sie die Datei **ca_chain.pem** auf **CA Certificates (CA-Zertifikate)**, die Datei **certificate.pem** auf **X.509** und die Datei **privatekey.pem** auf **Key Files (Schlüsseldateien)** hoch, wie in den Abbildungen unten dargestellt:



3) Klicken Sie im gleichen Fenster auf die Schaltfläche „Add“ (Hinzufügen), um die Zertifikatsprofile zu erstellen.

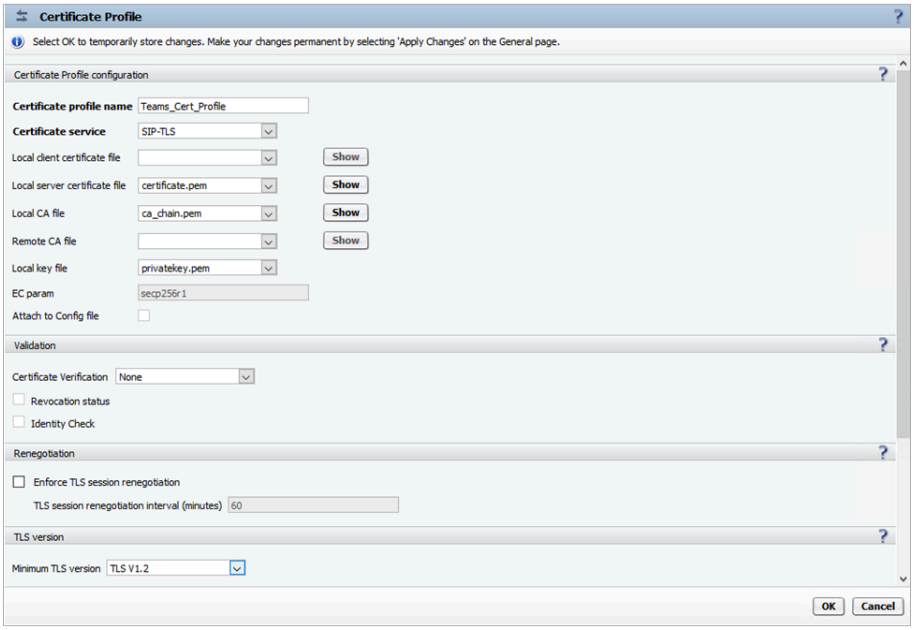


Abbildung 281: Zertifikatsprofil

4) Geben Sie im Fenster „Certificate Profile“ (Zertifikatsprofil) die folgenden Parameter ein:
   - **Name des Zertifikatsprofils:** Teams_Cert_Profile (Anzeigename)
   - **Zertifikatsdienst:** SIP-TLS
   - **Lokale Server-Zertifikatsdatei:** certificate.pem
   - **Lokale CA-Datei:** ca_chain.pem
   - **Lokale Schlüsseldatei:** privatekey.pem
   - **TLS-Mindestversion:** TLS V1.2
5) Klicken Sie auf die Schaltfläche „OK“.
6) Klicken Sie im Fenster **Certificate Management (Zertifikatsverwaltung)** auf die Schaltfläche OK.
7) Klicken Sie im Fenster **Security (Sicherheit)** auf die Schaltfläche OK.
8) Klicken Sie auf der Hauptseite von OS SBC auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.4 Teams Medienprofil

Die Kommunikation mit Teams Phone System ist mit Secure Audio (SRTP) gesichert.

Gehen Sie wie folgt vor, um das Teams Medienprofil zu konfigurieren:

1) Gehen Sie zu **OS SBC Management Portal > VOIP > Media (Medien)**.

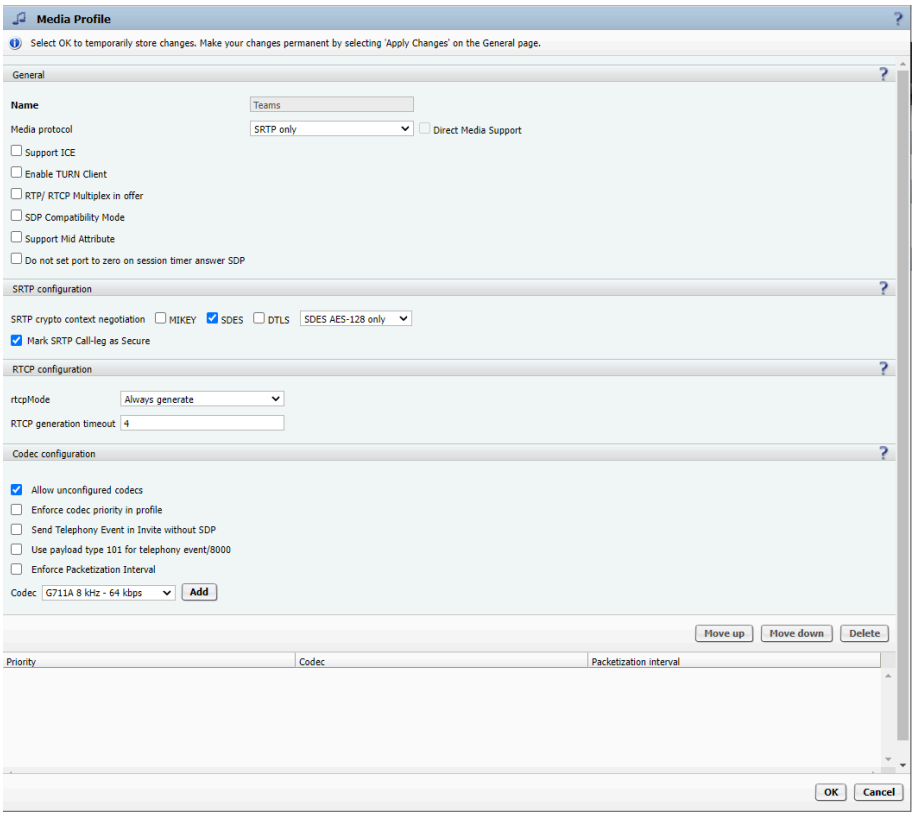


Abbildung 282: Medienprofile

2) Klicken Sie im Bereich „Media Profiles“ (Medienprofile) auf die Schaltfläche „Add“ (Hinzufügen), um das Medienprofil für OS SBC - Teams-Verbindungen zu erstellen. Die folgenden Parameter müssen eingegeben werden:
   - **Name:** Teams (Anzeigename)
   - **Media protocol (Medienprotokoll):** Nur SRTP
   - **Support ICE (ICE unterstützen):** Nicht markiert (für den Fall MB = OFF)
   - **SRTP crypto context negotiation (SRTP-Kryptokontext aushandeln)** SDES
   - **Mark SRTP Call-legasSecure:** Markiert
   - **rtcpMode:** „Bypass“ oder „Always Generate“ (Immer generieren)
   - **Allow unconfigured codecs (Unkonfigurierte Codecs zulassen):** Markiert
3) Klicken Sie im Fenster **Media (Medien)** auf die Schaltfläche OK.
4) Klicken Sie im Fenster **VOIP** auf die Schaltfläche OK.
5) Klicken Sie auf der OS SBC-Hauptseite auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.5 OpenScape 4000-Medienprofil

Zum Konfigurieren des OpenScape 4000-Medienprofils gehen Sie wie folgt vor:

1) Gehen Sie zu **OS SBC Management Portal > VOIP > Media (Medien).**

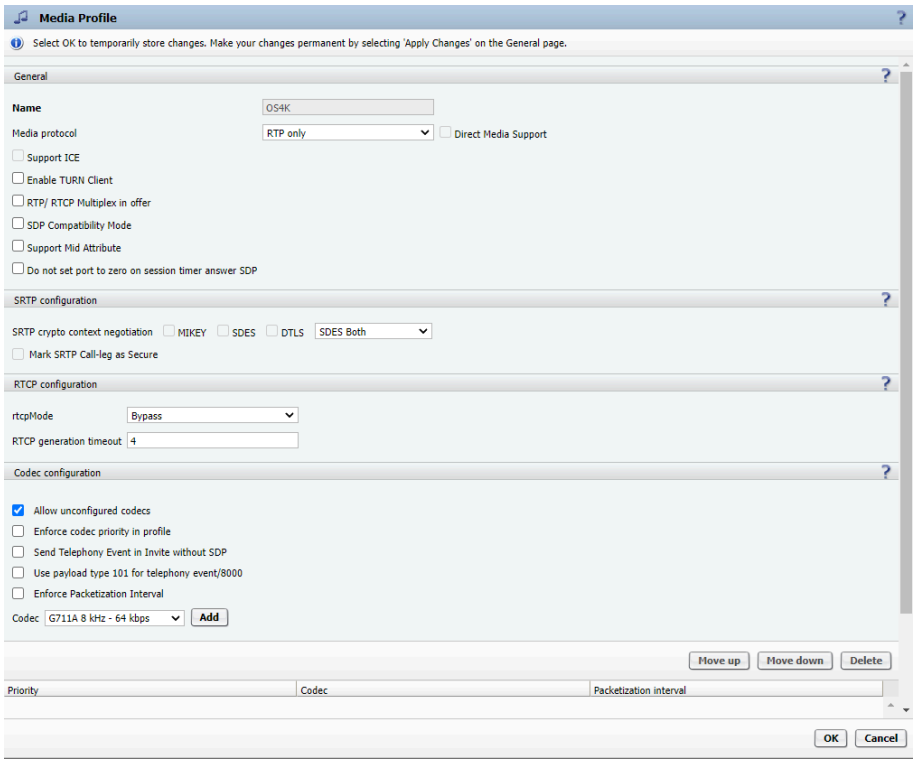


Abbildung 283: Medienprofil

2) Klicken Sie im Bereich **Media Profiles** (**Medienprofile)** auf die Schaltfläche **Add (Hinzufügen)** , um das Medienprofil für die Verbindung OS SBC - OpenScape 4000 zu erstellen. Folgende Parameter müssen konfiguriert werden:
   - **Name:** OS4K (Anzeigename)
   - **Media protocol (Medienprotokoll):** Nur RTP
   - **RTP/RTCP Multiplex in offer (RTP/RTCP Multiplexim Angebot):** Nicht markiert
   - **Allow unconfigured codecs (Unkonfigurierte Codecs zulassen):** Markiert
3) Klicken Sie im Fenster **Media (Medien)** auf die Schaltfläche OK.
4) Klicken Sie im Fenster **VOIP** auf die Schaltfläche OK.
5) Klicken Sie auf der OS SBC-Hauptseite auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.6 Allgemeine Medieneinstellungen

Nach der Erstellung der Medienprofile muss die allgemeine Medieneinstellung konfiguriert werden. Dazu ist das folgende Verfahren einzuhalten:

1) Gehen Sie zum Fenster **OS SBC Management Portal > VOIP** > **Media (Medien)**.

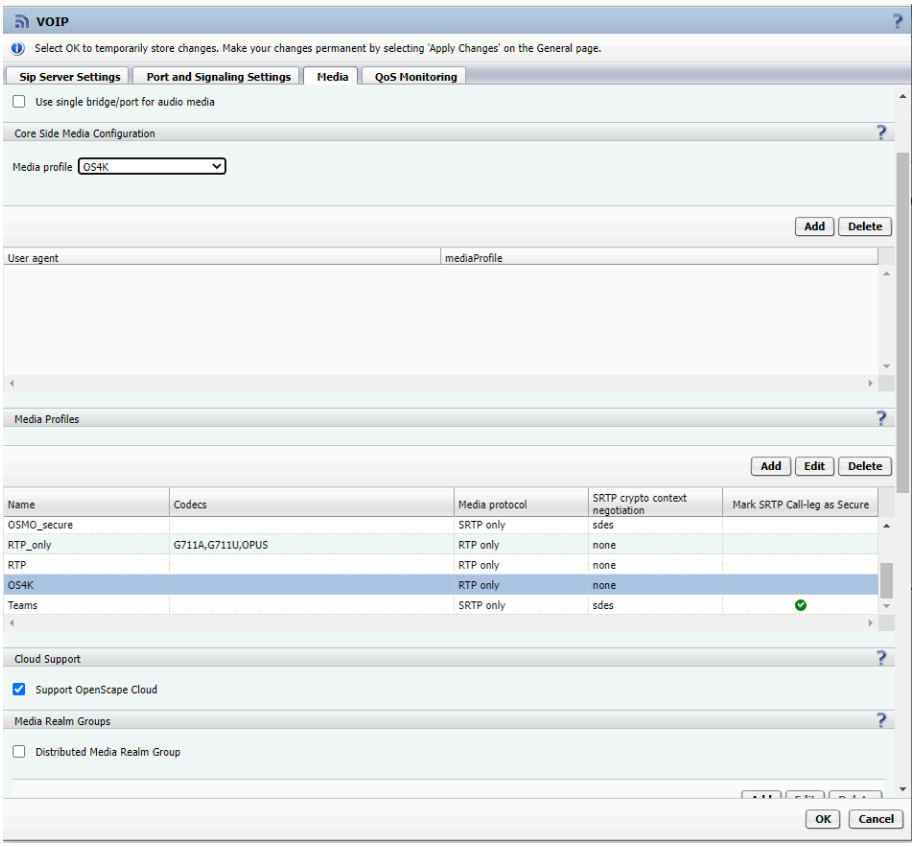


Abbildung 284: VOIP-Fenster

2) Wählen Sie unter **Core Side Media Configuration (Konfiguration Medien Kernseite)** aus der Dropdown-Liste das entsprechende Medienprofil aus, das im Abschnitt OpenScape 4000-Medienprofil auf Seite 1085hinzugefügt wurde.

   - **Medienprofil:** OS4K

3) Klicken Sie auf die Schaltfläche „OK“.
4) Klicken Sie auf der OS SBC-Hauptseite auf die Schaltfläche „Apply Changes“ (Änderungen übernehmen).

14.11.3.7 Externe Endpunkte

Die Konfiguration **Remote Endpoint (Externer Endpunkt)** für OS SBC mit Teams Phone System ist eingerichtet.

Um das MS Teams-Profil im SIP-Dienstanbieter-Profil festlegen zu können, ist eine Lizenz erforderlich.

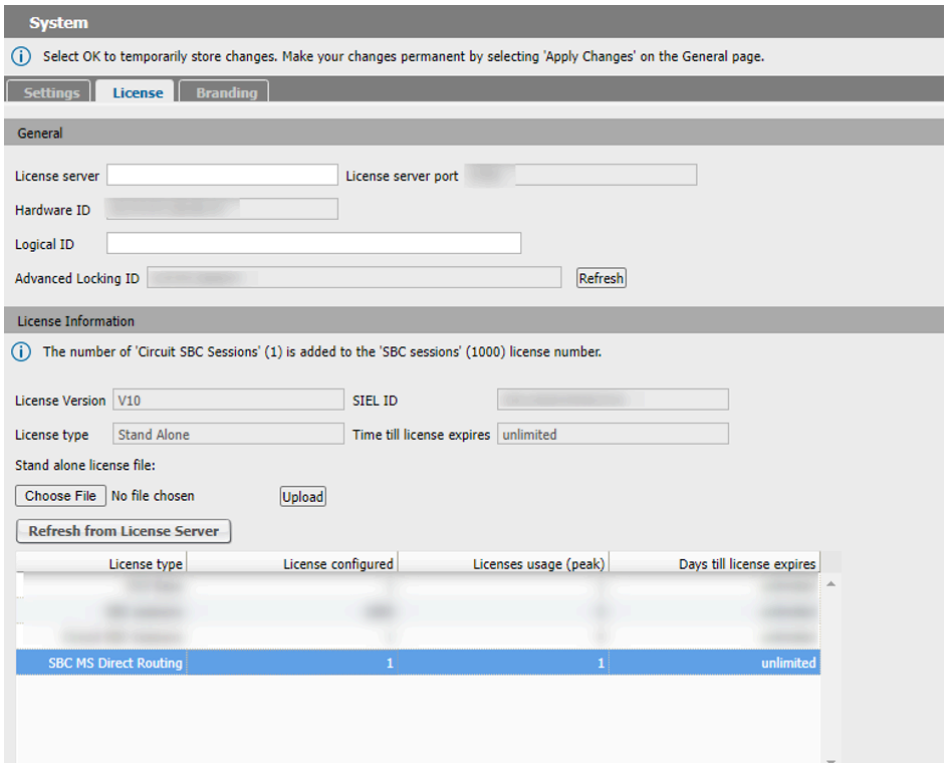


Figure 285: SIP-Dienstprofil-Lizenz

Navigieren Sie zum Fenster **OS SBC Management Portal > Merkmale**, um die Option **Fernendpunkte aktivieren** zu aktivieren und zu konfigurieren.

Klicken Sie im Fenster **Remote Endpoints (Externe Endpunkte)** im Bereich **SIP Service Provider Profile** auf die Schaltfläche **Add (Hinzufügen)** , um das Endpunktprofil für den Endpunkt OS SBC - Teams Phone System hinzuzufügen.

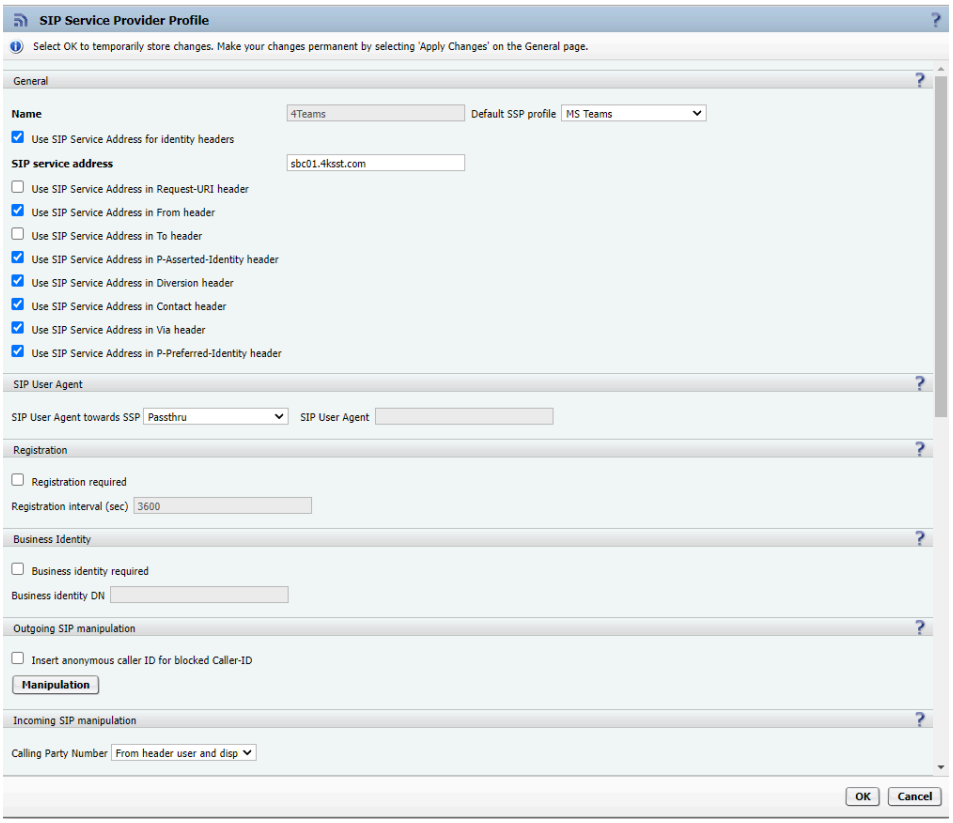


Figure 286: SIP Service Provider-Profil

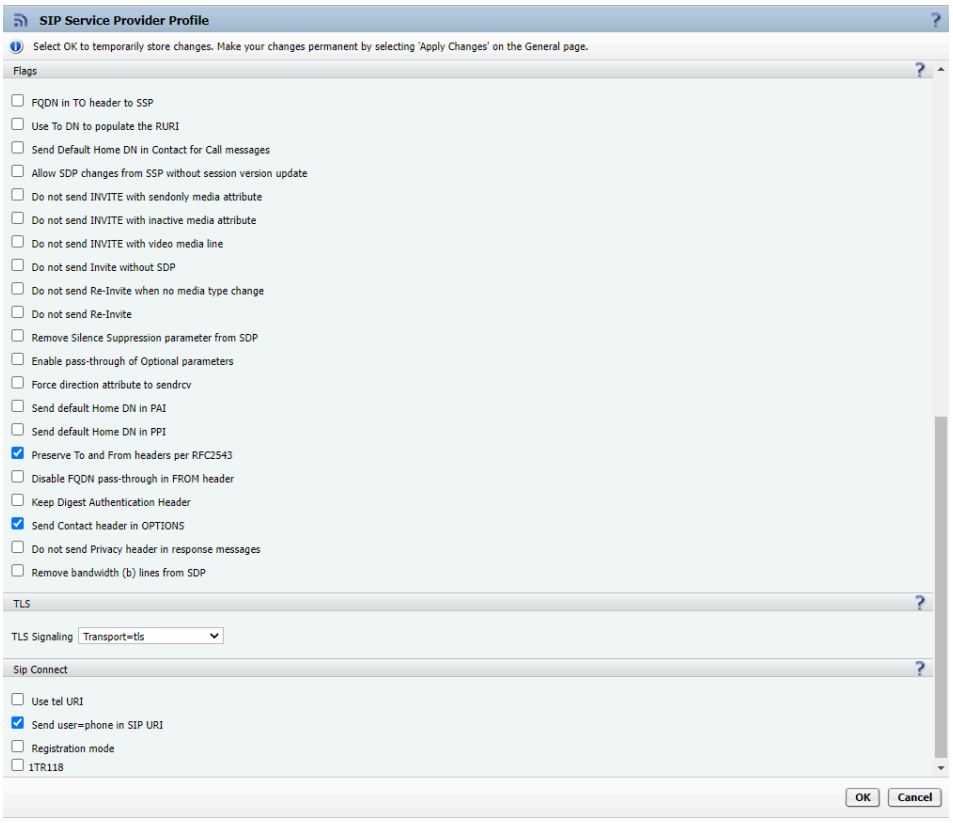


Figure 287: SIP Service Provider-Profil

Im Fenster **SIP Service Provider** müssen die folgenden Parameter konfiguriert werden:

- **Name:** 4Teams (Anzeigename)
- **Default SSP Profile (SSP-Standardprofil):** MS Teams
- **SIP Service Address (SIP-Dienstadresse):** sbc01.4ksst.com (öffentlicher FQDN des SBC)

Klicken Sie auf die Schaltfläche **OK** , um zum Fenster **Remote Endpoints (Externe Endpunkte)** zurückzukehren.

Klicken Sie im Bereich **Remote endpoint configuration (Konfiguration des externen Endpunkts)** auf die Schaltfläche **Add (Hinzufügen)**.

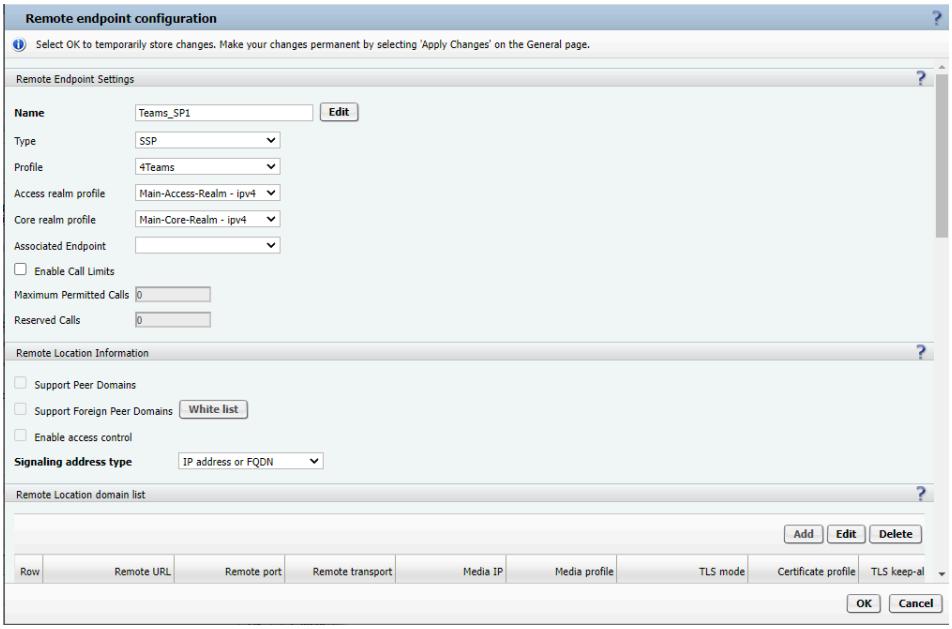


Figure 288: Remote Endpoint-Konfiguration

Im Fenster Remote endpoint configuration **(**Konfiguration des externen Endpunkts) müssen die folgenden Parameter konfiguriert werden:

- **Name:** Teams_SP1 (Anzeigename)
- **Typ:** SSP
- **Profil:** 4Teams

Klicken Sie im Bereich **Remote Location Domain List (Domänenliste des externen Standorts)** auf die Schaltfläche **Add (Hinzufügen).**

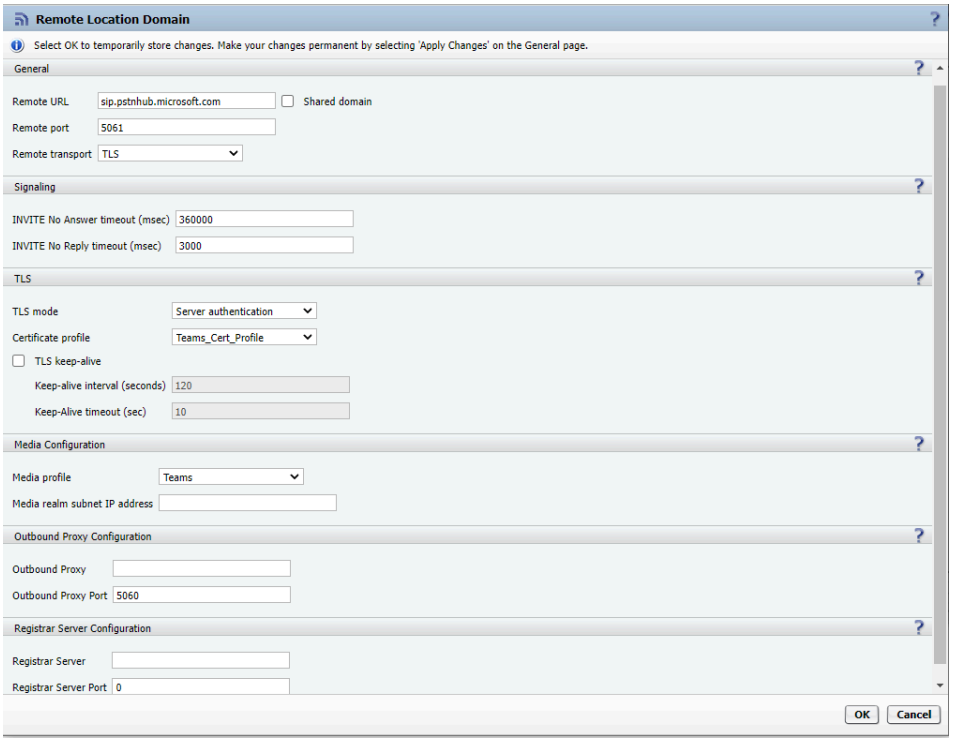


Figure 289: Externe Standortdomäne

Im Fenster **Remote Location Domain (Externe Standortdomäne)** müssen die folgenden Parameter konfiguriert werden.

- **Remote URL (Externe URL):** sip.pstnhub.microsoft.com (Teams FQDN 1)
- **Remote Port (Externer Port):** 5061
- **Remote transport (Externes Transportprotokoll):** TLS
- **TLS-Mode:** Server-Authentifizierung
- **Certificate profile (Zertifikatsprofil):** Teams_Cert_Profile (siehe Abschnitt SIP-Server)
- **Medienprofil:** Teams (siehe Abschnitt Zertifikate)

Klicken Sie auf die Schaltfläche **OK**, um zu **Remote endpoint configuration** (**Konfiguration des externen Endpunkts)**zurückzukehren.

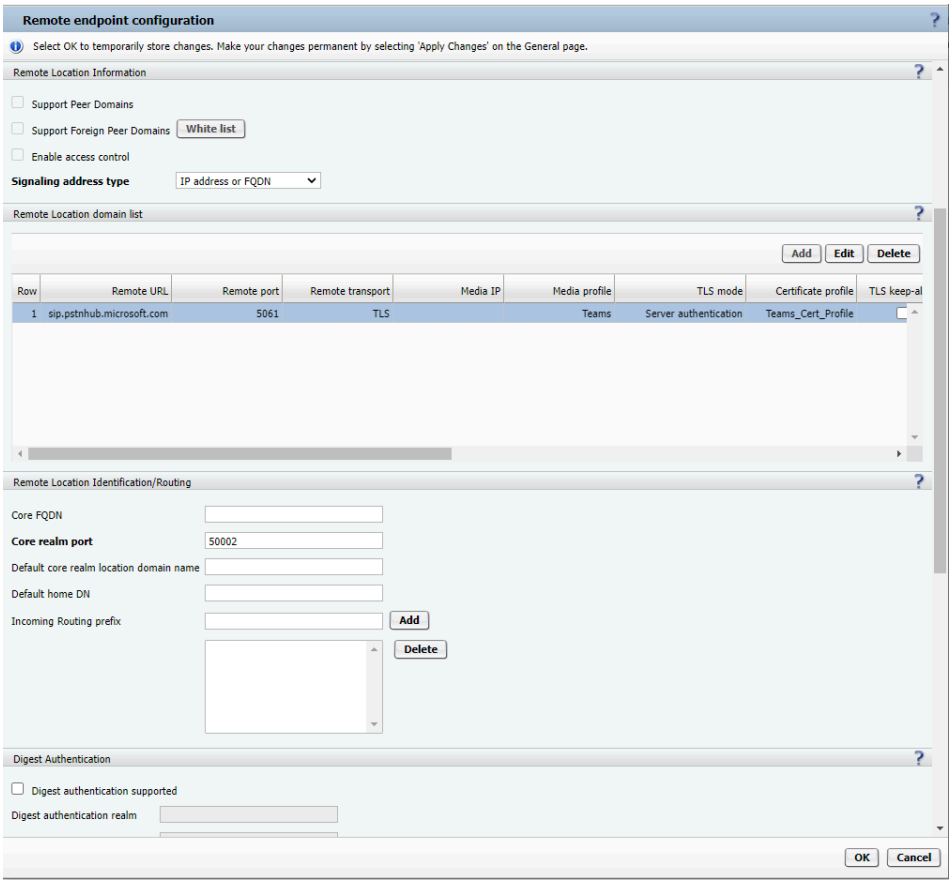


Figure 290: Remote Endpoint-Konfiguration

Im Fenster Remote endpoint configuration **(**Konfiguration des externen Endpunkts) müssen die folgenden Parameter konfiguriert werden:

- **Signaling address type (Typ der Signalisierungsadresse):** IP-Adresse oder FQDN
- **Core realm port (Kernbereichsport):** 50002 (unter vHG MS Teams SIP-Leitungsprofil konfiguriert)

Klicken Sie auf die Schaltfläche **OK** , um zum Fenster **Remote Endpoints** (**Externe Endpunkte)** zurückzukehren.

Wiederholen Sie die Prozedur für den Rest der Teams FQDNs (d. h. sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com).

Das Fenster **Remote Endpoints (Externe Endpunkte)** sollte wie in der folgenden Abbildung aussehen:

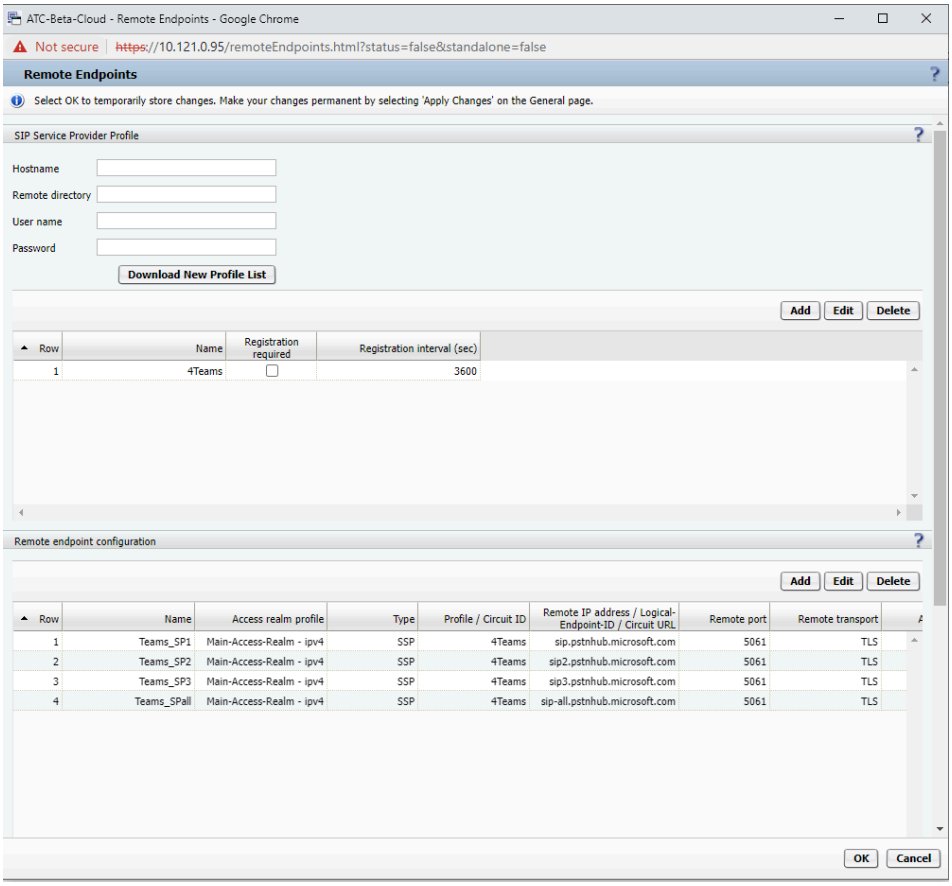


Figure 291: Externe Endpunkte

Klicken Sie in allen geöffneten Fenstern auf die Schaltfläche OK.

Klicken Sie auf der Hauptseite des OS SBC auf die Schaltfläche „Apply“ (Übernehmen).

14.11.4 MS Teams Direct Routing-Konfiguration

Dieses Dokument beschreibt, wie Sie den Unify OpenScape SBC (mit OpenScape 4000) an die Microsoft Teams Direct Routing-Konfiguration anschließen. Die Microsoft Teams Direct Routing-Konfiguration ist in diesem Dokument nicht enthalten und kann unter http://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure gefunden werden.

NOTICE:

Vergewissern Sie sich, dass der SBC mit der **Header-Einstellung Umleiten P-Asserted-Identity (PAI)** auf **Off** hinzugefügt wird.

Gehen Sie im Microsoft Teams-Admin-Zentrum im linken Navigationsbereich zu **Sprache > Direct Routing** und klicken Sie dann auf die **Registerkarte SBCs**.

Wählen Sie den bereits konfigurierten SBC aus (basierend auf der oben bereitgestellten offiziellen Microsoft-Dokumentation) und klicken Sie auf

die **Schaltfläche** Bearbeiten. Setzen Sie dann die **Kopfzeile Umleiten P-Asserted-Identity (PAI)** auf off und klicken Sie auf die Schaltfläche Save.

NOTICE:

Sie müssen in Ihrer Firewall Ports für die IP-Adressbereiche öffnen, um ein- und ausgehenden Datenverkehr zu und von den Adressen für Signalisierungszwecke zu ermöglichen. Weitere Informationen finden Sie in der Microsoft-Dokumentation: https://learn.microsoft.com/en-us/microsoftteams/direct-routing-plan

---

14.11.5 Verfügbare Funktionen (Überblick)

- Basisanruf
- CLIP/CLIR-Funktionen – Übermittlung von Anrufer-Name und -Rufnummer (Zugelassen und Eingeschränkt)
- Halten / Abrufen
- Umschalten nach Beratung
- Übertragung (betreut/blind)
- Konferenz
- Anrufumleitung
- Senden / Empfangen von DTMF-Tönen
- Parken / Entparken
- Paralleles Klingeln

14.11.6 Allgemeine Einschränkungen und Begrenzungen

MS Teams P-Asserted-Identity (PAI) Header wird derzeit von OS4K nicht unterstützt und muss in der MS Teams SBC Direct Routing-Konfiguration deaktiviert werden.

Das Telefondisplay wird nach der Übertragung (und bei Weiterleitungsszenarien) nicht aktualisiert, da Teams keine PAI im 200OK-Ereignis sendet (selbst wenn ForwardPAI beim Mandanten aktiviert ist). Außerdem werden die von der anderen Seite erhaltenen PAI vernachlässigt. Teams liest die Anzeigeinformationen aus der Kopfzeile „FROM“ aus.

Bei einem Konferenzgespräch wird die Anzeige nicht aktualisiert, was eine Einschränkung der nativen SIP-Leitung ist.

NOTICE: DMC kann nicht auf der SIP-Trunk-Schnittstelle zu MS Teams verwendet werden.

Park / Unpark wird nicht unterstützt, wenn Media-Bypass aktiviert ist.

14.12 SIP-URI-Wahl

Für interne Videoanrufe mit OpenScape 4000, OpenScape SBC und OpenScape UC gibt es derzeit zwei Möglichkeiten:

- Videoanrufe zwischen OpenScape 4000/ OpenScape UC-Endpunkten;
- Videokonferenzen, die von der OpenScape UC Conference Bridge für OpenScape 4000/ OpenScape UC-Endpunkte abgehalten werden.

Für Videoanrufe und Videokonferenzen mit anderen Unternehmen unterstützt OpenScape 4000 die folgenden zwei Anwendungsfälle:

- **Ausgehende Videowahl**: OpenScape UC-Clients geben einen SIP-URI-String ein und nehmen an Videokonferenzen anderer Unternehmen teil (die über das Internet geleitet werden).
- **Eingehende Videowahl**: Benutzer aus anderen Unternehmen geben einen SIP-URI-String ein und nehmen als unbekannte Benutzer an der OpenScape UC Videokonferenz teil.

Die Funktionalität wird mit den folgenden Videokomponenten erreicht:

- Anrufsteuerung: OpenScape 4000
- Video-Gateway: OpenScape SBC
- Video MCU: Server für Videokonferenzen
- Video-Clients: OS UC-Clients: Fusion, WebRTC-Client
- Video Room-Systeme von Poly: z.B. Group-Serie, Group 7500

14.12.1 Video-Auswahl

Bei der Video-Auswahl-Methode geben die UC-Clients einen SIP-URI-String ein und können an Videokonferenzen anderer Unternehmen teilnehmen (die über das Internet geleitet werden).

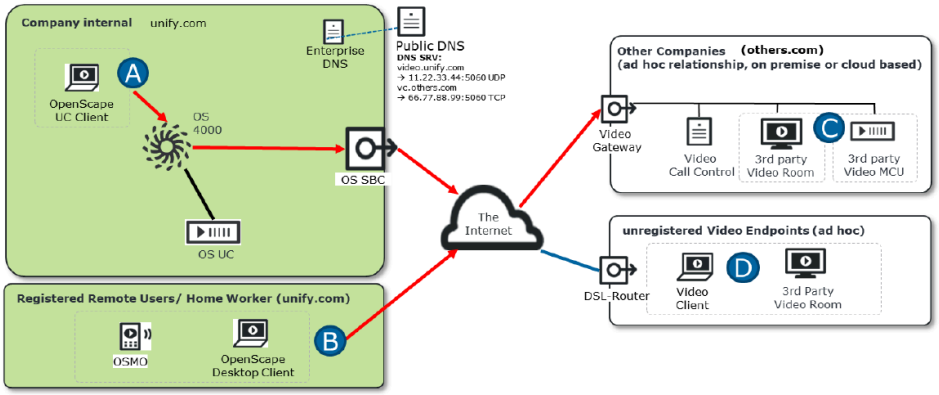


Figure 292: Video-Auswahl

Table 81: D1 und D2 sind verbunden

Produkt	Auswahlszenario: Aufgabe/Verantwortlichkeit
OpenScape UC Client OpenScape UC	• Eingabe der SIP-URI-Adresse • Weiterleitung an OpenScape 4000 (über CSTA) OpenScape 4000

Produkt	Auswahlszenario: Aufgabe/Verantwortlichkeit
OpenScape 4000	• Analyse von SIP URI • Weiterleitung des Anrufs an SBC (Wildcard-basiert oder domänenbasiert im SBC definiert)
OpenScape SBC	• Auflösung der SIP-URI in IP-Adresse • Anruf ins Internet senden

14.12.1.1 Anrufweiterleitung von externen alphanumerischen SIP URIs

OpenScape 4000 muss Videoanrufe über eine externe SIP-URI-Adresse an den definierten SBC weiterleiten (wenn mehr als ein SBC installiert ist). Extern bedeutet, dass die gewählte SIP-URI keinem OpenScape 4000-Teilnehmer zugewiesen ist oder innerhalb der eigenen oder einer vertrauenswürdigen Domain liegt.

OpenScape 4000 muss SIP-URI-Rufe weiterleiten/routen, ohne die gewählte alphanumerische SIP-URI zu verändern. Dadurch kann der nächste SIP-Peer den Anruf an das richtige Ziel weiterleiten, ohne dass wichtige Parameter (z. B. der Port) verloren gehen.

OpenScape 4000 muss SIP URI Invites mit einer unbekannten Domain an einen vordefinierten SBC (z.B. SBC1) weiterleiten, wobei Wildcard-Routing verwendet wird.

Zusätzlich muss OpenScape 4000 SIP URI Invites mit bestimmten Domänen an vordefinierte SBCs weiterleiten (domänenbasiertes Routing zum Trunk in Richtung SBC, z.B. Domäne „customer1.com“ soll an SBC2, Domäne „customer2.com“ soll an SBC3 weitergeleitet werden).

14.12.1.2 SIP-URI-Wahl über die CSTA-Schnittstelle

Die UC-Clients stellen die Video-Clients innerhalb der OpenScape 4000-Lösung dar.

Die UC-Clients sind iun OpenScape 4000 registriert. Die Anrufe von UC-Clients werden über CSTA an OpenScape 4000 initiiert.

OpenScape 4000 muss daher die SIP-URI-Wahl innerhalb von CSTA entsprechend interpretieren und auflösen.

OpenScape 4000 muss SIP-URI-Anrufe, die von den UC-Clients oder dem OpenScape UC-Medienserver eingehen, annehmen und weiterleiten.

14.12.1.3 SIP-Q-Support

SIP-Q unterstützt nicht den Transport von alphanumerischen SIP-URIs.

Die UC-Clients sind iun OpenScape 4000 registriert. Die Anrufe von UC-Clients werden über CSTA an OpenScape 4000 initiiert.

Jede Route in der Übersetzung, die zu einem alphanumerischen SIP-URI führt, der als angerufener Teilnehmer an einen SIP-Q-Endpunkt gesendet wird, wird von der Übersetzung als „Route nicht verfügbar“ behandelt.

14.12.2 Video-Einwahl

Benutzer aus anderen Unternehmen wählen den SIP-URI-String und nehmen als unbekannte Benutzer an der Videokonferenz des OpenScape UC-Konferenzservers teil.

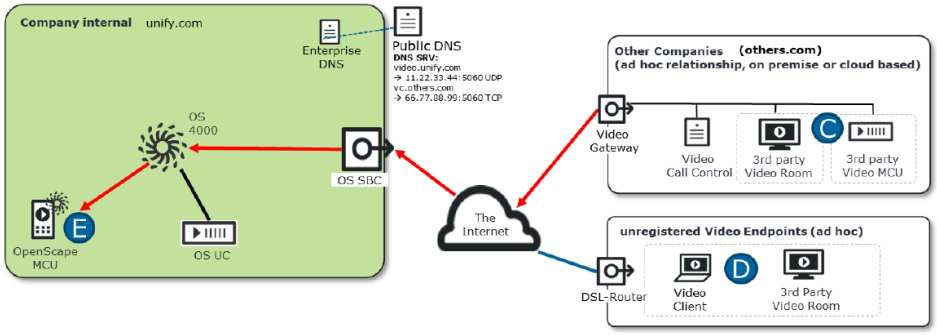


Figure 293: Video-Einwahl

Table 82: D1 und D2 sind verbunden

Produkt	Einwahlszenario: Aufgabe/Verantwortlichkeit
Anderes Unternehmen	• SIP-URI-Adresse des OpenScape UC-Konferenzservers wählen, z. B. video10@unify.com • Der Anruf wird über das Internet an OpenScape SBC weitergeleitet
OpenScape SBC	• Eintrag in das Unternehmensnetzwerk • Überprüfung eingehender Anrufe (z. B. Whitelists) • Anrufumleitung zu OpenScape 4000 • Anruf ablehnen/ignorieren
OpenScape 4000	• Anruf an OpenScape UC MediaServer / MCU weiterleiten
OpenScape UC MS/ MCU	• Nachweis der PIN am Konferenzportal/ Begrüßungsbildschirm • Route zur Konferenz • Anruf beenden

Die UC-Clients sind iun OpenScape 4000 registriert. Die Anrufe von UC-Clients werden über CSTA an OpenScape 4000 initiiert.

Jede Route in der Übersetzung, die zu einem alphanumerischen SIP-URI führt, der als angerufener Teilnehmer an einen SIP-Q-Endpunkt gesendet wird, wird von der Übersetzung als „Route nicht verfügbar“ behandelt.

14.12.2.1 Anrufverarbeitung - Einladungen von OS-SBC (Internet)

Einwahlanrufe an SIP URI, die an die OpenScape UC MCU weitergeleitet werden, werden akzeptiert.

14.12.2.2 URI-Mapping-Dienst

Ein neuer URI-Mapping-Dienst verwaltet die Zuordnung von SIP URI Domains zu Nummern (vorkonfigurierte Trunk Access Codes).

Die Mapping-Tabelle ist über AMO CLIMA konfigurierbar.

14.12.3 SIP-URI-Format für ausgehende Videowahl

OpenScape 4000 muss die folgenden SUP URI-Formate, die für Videoanrufe verwendet werden, weiterleiten:

SIP-URI-Format sip:<user>@<domain>

- Der Benutzerteil darf nicht leer sein.
- Der Domänenteil kann sein:
  - FQDN
- Beispiele:

  4989700712345@unify.com

  Erika.Mustermann@polycom.com

Die obige Definition ist ein reduzierter Ansatz, der die gängigsten SIP-URI-Formate umfasst (SIP-URI-Definition RFC 3261).

14.12.4 MS Teams DR mit Audiocodes SBC

14.12.5 Einschränkungen

Eingehende SIP-URI-Wahl wird in Kombination mit dem OpenScape 4000 SIP Load Balancer nicht unterstützt.

14.12.6 Konfiguration

Anrufe an eine Domäne werden auf der Grundlage der Konfiguration über AMO CLIMA an eine bestimmte Leitung weitergeleitet.

Mit AMO CLIMA kann eine Mapping-Tabelle mit einer DOMAIN-NUMBER konfiguriert werden, wobei NUMBER für einen vorkonfigurierten Trunk Access Code steht.

In Anbetracht der Tatsache, dass CLIMA jetzt die vorrangige Suche ist, muss jeder, der DNS-Namen verwendet, zwischen internen SIP-Funktionen und URI-Domänenwahl unterscheiden.

AMO LDPLN

- Für die neue Tabelle DOMAIN muss ein DOMAIN NUMBERING PLAN konfiguriert werden.
- Der Nummerierungsplan 790 im LCR-Pool 8 wird für die Tabelle DOMAIN reserviert.

```
ADD-LDPLN:LCRADM,790,8,20,"DOMAIN PATTERN PLAN";
```

NOTICE: Der Nummerierungsplan 790 im LCR-Pool 8 ist für die Tabelle DOMAIN reserviert und darf daher von UPLOL nicht in die Objekte LDPLNS und LDPLN aufgenommen werden.

AMO CLIMA

- Eine neue TABLE namens DOMAIN wurde für das Domain Mapping hinzugefügt.
- Die Domäne wird einer Nummer zugeordnet, die eine vorkonfigurierte Amtskennziffer ist.
- Die Anrufe an eine bestimmte Domäne werden entsprechend dem mit AMO CLIMA konfigurierten DOMAIN-NUMBER-Paar an die konfigurierte Leitung weitergeleitet.

```
ADD-CLIMA:DOMAIN,ATOS.NET,101;
// die Domain ATOS.NET wird an die vorkonfigurierte Amtskennziffer 101
 weitergeleitet
 <ADD-CLIMA
TABLE = ?
TABLE           : TABLE TYPE
CHARACTERISTIC  : REQUIRED CONDITIONAL
POSS. VALUES    : DDI          DDI TABLE
                  CLI          CLI TABLE
                  DOMAIN       DOMAIN TABLE

TABLE = DOMAIN

DOMAIN = ?
DOMAIN          : DOMAIN; ALLOWED: 0..9,A-Z,A-Z,_,.,
CHARACTERISTIC  : REQUIRED
POSSIBLE VALUES : MAX. OF 63 POSITIONS

DOMAIN = ATOS.NET

NUMBER = ?
NUMBER          : TRUNK ACCESS CODE
CHARACTERISTIC  : REQUIRED
POSSIBLE VALUES : MAX. OF 22 POSITIONS
NUMBER = 101;
ADD-CLIMA:DOMAIN,ATOS.NET,101;
H500: AMO CLIMA STARTED
```

```
H04: DOMAIN HAS BEEN ADDED FOR DOMAINNO 6.

AMO-CLIMA-111 CLI MANIPULATION
ADD COMPLETED;



DIS-CLIMA:DOMAIN;
H500: AMO CLIMA STARTED
-------------------------------------------------------------------------
| DOMAIN TABLE                                                          |
-------------------------------------------------------------------------
| DOMAINNO : 1                                                          |
| DOMAIN   : ABA.COM                                                    |
| NUMBER   : 100                                                        |
-------------------------------------------------------------------------
| DOMAINNO : 6                                                          |
| DOMAIN   : ATOS.NET                                                   |
| NUMBER   : 101                                                        |
-------------------------------------------------------------------------
| DOMAINNO : 7                                                          |
| DOMAIN   : SIEMENS.COM                                                |
| NUMBER   : 102                                                        |
-------------------------------------------------------------------------

AMO-CLIMA-111 CLI MANIPULATION
DISPLAY COMPLETED
```

NOTICE: Weitere Informationen zur Konfiguration von SIP URI finden Sie in *OpenScape Solution Set V10, OpenScape SIP URI Configuration Guide, Administrator Documentation*.

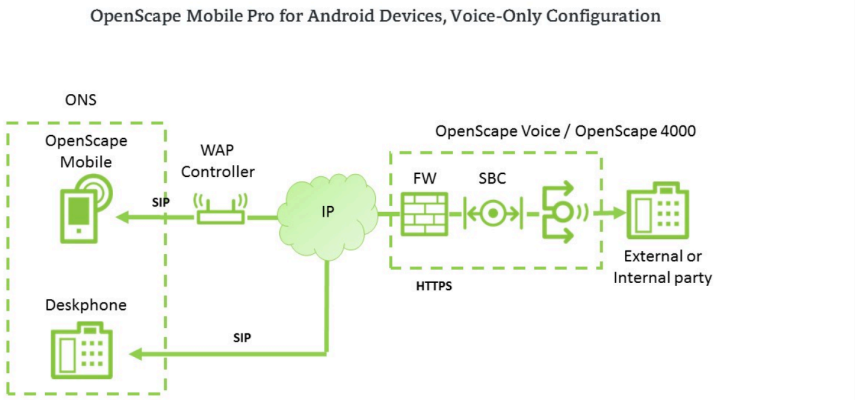
15 OpenScape Mobile Pro Client

15.1 Überblick

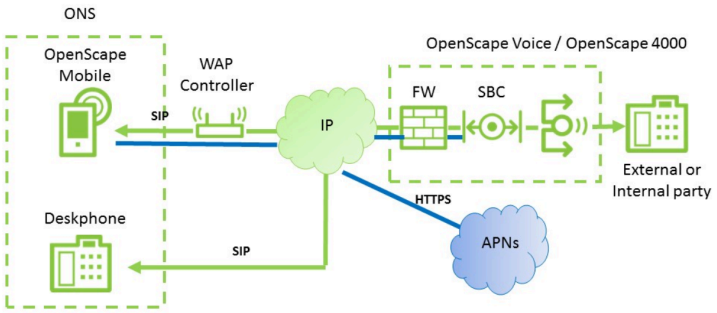
OpenScape 4000 V8R2 und höher unterstützen nur OSMO Pro.

OSMO auf dem OpenScape4000 verwendet das gleiche Verhalten wie das OSV – das sogenannte Auto Pilot Routing. Es ist vergleichbar mit einem Sammelanschluss. Sobald der OSMO angemeldet ist, wird das Auto Pilot Routing aktiviert. Eingehende Anrufe werden immer in dieser Reihenfolge geroutet: Zuerst klingelt der OSMO und nach einer systemweit eingestellten Zeit (Standard=15 s) wird der Anruf an das Deskphone geroutet (Info: Funktion kann auch ohne dediziertes Deskphone verwendet werden). Von da an wird die normale 4k-Anrufbearbeitung (No Answer Advance ANSADV / Rufweiterschaltung RWEITER) durchgeführt.Wenn für den OSMO Pro-Client eine Zellennummer konfiguriert ist und der Anruf zur Zelle weiterleiten in den OSMO Pro-Einstellungen aktiv ist, wird ein eingehender Anruf an die Zellennummer weitergeleitet, falls der Client abgemeldet ist. Eingehende Anrufe an eine OSMO Pro / Desk Phone-Kombination werden im Nur-Sprache-Modus mit einem Besetztzeichen beim dritten Anrufer signalisiert (z. B. solange das Autopilot-Routing ein freies Gerät findet, wird der Anruf an dieses Gerät weitergeleitet). . Im kombinierten Modus ist es möglich, das bevorzugte Gerät auf ein dediziertes Gerät einzustellen, und dann ist es beim zweiten Anruf besetzt.

Beispiel für eine Nur-Sprache-Konfiguration:

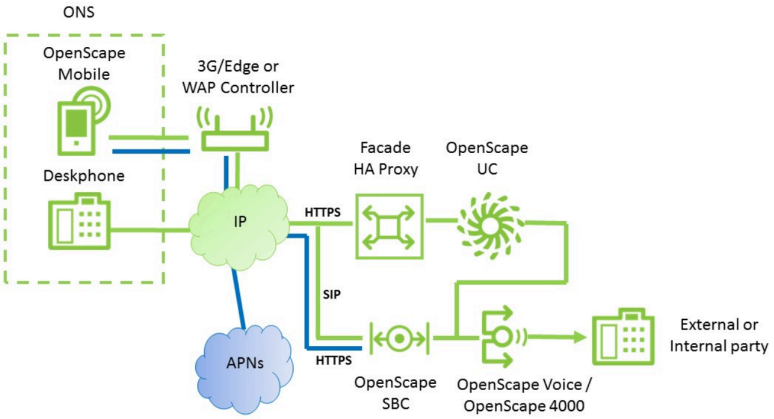


OpenScape Mobile Pro for Apple Devices, Voice-Only Configuration

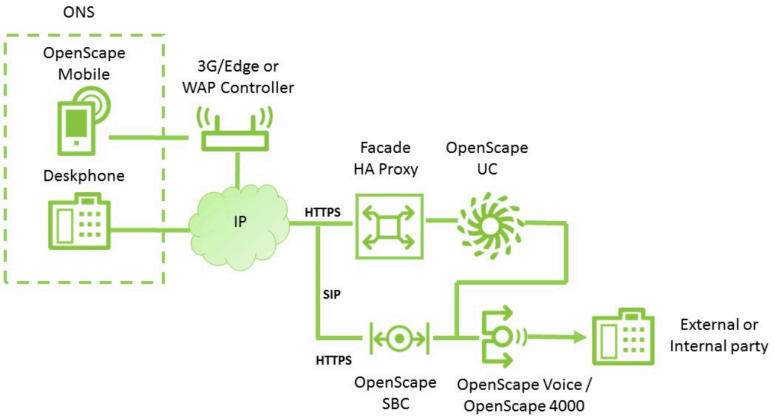


Konfigurationsbeispiel für den kombinierten Modus (integriert):

OpenScape Mobile Pro for Apple Devices, Integrated Configuration



OpenScape Mobile Pro for Android Devices, Integrated Configuration



Eine ausführliche Beschreibung finden Sie in OpenScape Mobile Pro, Administrator-Dokumentation.

Anmerkung: Eine Übergabe zwischen den beiden Topologien ist nicht möglich.

15.1.1 Allgemeine Einschränkungen und Begrenzungen

Es gelten die folgenden Einschränkungen

- Es wird nicht unterstützt, dass ein Benutzer OMO Pro, Schaltkreis-ATC, OSCC, C4B-Telefon usw. parallel verwendet.
- OSMO Pro wird mit STMIX/STMIY oder SoftGate unterstützt; klassisches STMI wird nicht unterstützt
- Videoanrufe werden vom OSMO Pro-Anruf-Client nicht unterstützt.
- DMC wird für den OSMO Pro-Client nicht unterstützt.
- Emergency Release und Override werden für den OSMO Pro Client nicht unterstützt.
- Die Annahme von Anrufen aus dem OpenScape Mobile Pro Client ist in den folgenden Fällen nicht möglich:
  - Rückruf auf DESK-Telefon
  - OpenScape Mobile Pro Client ONS ist HG-Mitglied: HG wurde angerufen, Anruf klingelt am Desk Phone

  Dieselbe Einschränkung gilt, wenn der Anruf im OpenScape Mobile Pro Client eingeht und der OSMO Pro-Benutzer wählt, dass er den Anruf über das Tischtelefon oder eine andere Nummer mit dem OpenScape Mobile Pro Client annimmt.
- Rückruf- und Abholgruppe (mit OpenScape Mobile Pro Client):
  - Der Rückruf an eine Client-Desk-Konfiguration wird nur dann ausgeführt, wenn diese Konfiguration vollständig inaktiv ist, nicht aber, wenn der OpenScape Mobile Client eine Station, die Mitglied derselben Abholgruppe ist, anruft.
- Netzwerk-Abholgruppe (OpenScape Mobile Pro Client):
  - Nicht unterstützt
- CHESE-Gruppe (Chef / Sekretär):
  - Nicht unterstützt
- Paralleles Klingeln (Klassische ONS-Gruppe):
  - Nicht unterstützt
- ACD/AGENT-Leistungsmerkmal:
  - Nicht unterstützt
- Persönliche Gerätegruppe (Twinning):
  - Nicht unterstützt – OpenScape Mobile Pro Client und Twinning schließen sich gegenseitig aus
- COM-Gruppen
  - Nicht unterstützt
- SPS (Signaling and Payload Separation)
  - Nicht unterstützt
- Lautsprecher-Anruf - Einseitig
  - Nicht unterstützt

- DSS -Schlüssel mit OpenScape Mobile Pro Client unterstützt. Beispiel: OpenScape 4000-Teilnehmer hat DSS-Taste in AMO ZIEL mit Nummer der OpenScape Mobile Pro Client/Desk-Konfiguration als Ziel konfiguriert. Wenn OpenScape Mobile Pro Client einen eingehenden Anruf im OpenScape Mobile Pro Client hat, blinkt der DSS-Schlüssel nicht. Die Taste beginnt zu blinken, wenn der Anruf an das Tischtelefon weitergeleitet wird (nach Ablauf von FWDDESK).

  NOTICE: Ab OpenScape 4000 V11R1 ist diese Einschränkung nicht mehr vorhanden.

- OpenScape Mobile Pro Client CA4000-Konnektivitätsadapter darf nicht mit anderen Anwendungen, die keine vollständigen E164 -Zahlenformate verwenden, geteilt werden.

15.1.1.1 Einschränkungen des kombinierten OSMO Pro-Modus

- TLS1.2 wird von OS4K Assistant erst ab UCV9R4.10 unterstützt. Bitte verwenden Sie TLS1.2 mit Fallback auf TLS1.0.
- Im kombinierten OSMO Pro-Modus muss die Nummer des Anrufers im internationalen E164-Format gesendet werden. Für den KNFOR-Eintrag des Knotens, der die OSMO Pro-Clients hostet, muss TONIN auf INTERPRE gesetzt sein. Falls für Nicht-OSMO Pro-Geräte kein internationales Format erwünscht ist, muss für die OSMO Pro-Clients eine separate Knoten-ID verwendet werden.
- Bitte lesen Sie auch den UC Planning Guide und die UC-Versionshinweise, um sich über allgemeine Einschränkungen des kombinierten OSMO Pro-Modus zu informieren.
- Seamless Handover mit der OSMO-Anwendung wird von UC nicht richtig gehandhabt. Daher werden Handover-Optionen in der UC-Schnittstelle nach Verschiebungsaktionen in OSMO nicht aktualisiert. Anrufsteuerungsfenster fehlt in UC, wenn der Anrufer den Anruf von OSMO auf das Bürotelefon (Tischtelefon) verschiebt.

15.1.1.2 Hinweise für SIP-Gerät als OpenScape Mobile Client Deskphone

1. DTMF auf SIP ist über CSTA_GENERATE_DIGITS_REQUEST möglich

2. HOLD von OpenScape Mobile Client, wenn der Anruf auf dem DESK-Telefon erfolgt

SIP-UFIP als DESK-Funktion: CSTA HOLD für SIP-UFIP als DESK implementiert

1) CSTA HOLD ist eine exklusive RMX-CP-Funktion (keine Gerätefunktion)

2)
- Wenn CSTA HOLD aufgerufen wird, darf nur CSTA RETRIEVE die Verbindung wiederherstellen
- Wenn SIP HOLD aufgerufen wird, darf nur SIP RETRIEVE die Verbindung wiederherstellen
- Wenn CSTA HOLD aufgerufen wird, wird das SIP-Telefon nicht benachrichtigt (dem Gerät selbst ist nicht bekannt, dass sich sein Partner in HOLD befindet). In diesem Fall verfügt das SIP-Telefon über die Option HOLD im Telefonmenü, aber wenn der Benutzer diese Option

auswählt, wird sie abgelehnt. Dasselbe gilt für die Optionen NEW CALL und TRANSFER, die HOLD als ersten Schritt verwenden

3. RETRIEVE vom OpenScape Mobile Client bei Anruf auf dem Tischtelefon SIP-UFIP als DESK-Funktion: CSTA RETRIEVE für SIP-UFIP als DESK implementiert

- CSTA RETRIEVE ist eine exklusive RMX-CP-Funktion (keine Gerätefunktion)
- Wenn CSTA HOLD aufgerufen wird, darf nur CSTA RETRIEVE die Verbindung wiederherstellen
- Wenn SIP HOLD aufgerufen wird, darf nur SIP RETRIEVE die Verbindung wiederherstellen

4. CALLBACK keine Antwort auf UFIP / Jeder Rückruf von UFIP SIP-UFIP-Funktion: Rückruf auf SIP ist nur automatischer Rückruf, da in SBCSU keine MAILBOX für SIP-UFIP konfiguriert werden kann

5. Anruf auf OOS UFIP-Tischtelefon verschieben – Anruf auf Desktop verschieben erscheint, wenn der OOS-Status des SIP-UFIP-Tischtelefons im RMX nicht sichtbar ist (siehe AMO SDSU). RMX beruht auf einem im Gateway implementierten Mechanismus, der den OOS-Status von SIP meldet. Dieser Mechanismus zeigt diesen Status nicht in Echtzeit an, daher gibt es Fälle, in denen das SIP-Telefon OOS ist, aber RMX dies nicht weiß.

Wichtig: Aktionen, die von OpenScape Mobile Client (über CSTA) initiiert wurden, sollten nicht mit Aktionen gemischt werden, die vom SIP-UFIP-Telefon eingeleitet werden, oder umgekehrt. Es wird empfohlen, nur OpenScape Mobile Client-Aktionen (über CSTA) oder nur physische Aktionen vom SIP-UFIP-Telefon zu verwenden.

15.1.2 Konfiguration

OpenScape Mobile Pro Clients müssen in einem OpenScape 4000 System als UFIP SIP Gerät konfiguriert werden. Es gibt ein UFIP SIP Gerät pro OpenScape Mobile Pro Client-Benutzer. Dieses UFIP SIP-Gerät fungiert als Proxy für alle OpenScape Mobile Pro Clients des Benutzers. Das UFIP SIP ist ein Hilfsgerät, daher wird seine Nummer auf keinem Telefondisplay angezeigt und nur dem Systemadministrator bekannt.

OSMO Pro-Lizenzen sind erforderlich, um OSMO Pro Clients zu konfigurieren. Ein OSMO Pro-Benutzer benötigt eine flexlicense für das Tischtelefon und eine OSMO Pro-Lizenz für die Clients. (wenn ein Benutzer den Client auf mehreren Smartphones/Tablets parallel ausführen möchte, ist nur eine OSMO Pro-Lizenz erforderlich).

Direktanrufe zu UFIP SIP-Geräten sind nicht möglich. Die OpenScape Mobile Pro Clients sind mit der OpenScape 4000-Tischtelefonnummer des Benutzers erreichbar. Die Benutzer Tischtelefon ONS Nummer ist über AMO SBCSU mit dem zusätzlichen UFIP SIP-Gerät verbunden (siehe unten Konfigurationsbeispiel).

"Reguläre" SIP Endpunkte und UFIP OpenScape Mobile Pro Clients können parallel auf einer Gateway-Platine konfiguriert werden.

Anmerkung: Hintergrundarchitekturinformationen eines OpenScape Mobile Pro Client-Registrierungsprozesses: Der OpenScape Mobile Pro Client verwendet die ONS-Tischtelefonnummer für eine Dummy-Registrierung, sobald sich der OpenScape Mobile Pro Client bei seiner OpenScape Mobile Pro Client-Anwendung anmeldet. Die Daten, die für die Registrierung des Clients mit dem Gateway (UFIP SIP-Hilfstelefonnummer) benötigt werden, werden über CSTA über SIP an den Client gesendet. Sobald der Kunde alle diese Daten erhalten hat, registriert er sich als SIP-Client mit der GW. Nach erfolgreicher Registrierung ist der Client in Betrieb.

Anmerkung: Für UFIP SIP Clients-Fähigkeiten siehe Abschnitt Abschnitt , “SIP-Abonnent”.

Die Clients müssen auch über Administration mit dem Desktop-Telefon des Benutzers verbunden werden. (AMO SBCSU, Parameter CLNTDESK).

Die Clients müssen als OSMO Pro Clients konfiguriert sein (AMO SBCSU parameter OSMO = JA)

Für Mobile Pro Clients kann dem Client als konfigurierbare Option die Mobiltelefonnummer des Benutzers zugewiesen werden (AMO ZIEL).

Weitere Parameter für OSMO Pro werden mit AMO ZANDE Zweig OSMO konfiguriert. Diese Parameter werden an den OSMO Pro Client gesendet, wenn sich der Benutzer anmeldet.

- SERVMAIL E-Mail-Adresse für den Kundendienst
- OSVTLS-Stufe des Zertifikat-Sicherheitsüberprüfungs-Gateways (0=keine Prüfung, 1=Prüfung)
- SBCSTLS SBC-Stufe der Zertifikatsüberprüfung (0=keine Prüfung, 1=Prüfung)
- QOSVIDEO Servicequalität für Video (0..254)
- DSCPTOS aktivieren/deaktivieren DSCPTOS (ja, nein)
- WMM aktivieren/deaktivieren drahtlose Multimedien (ja, nein)
- SECOSV Mediensicherheitsmodus Gateway (rtp, srtp, Best-Effort)
- SECOSBC Mediensicherheitsmodus SBC (rtp, srtp, Best-Effort)
- FEATLIST OSMO Pro-Merkmalsliste. Bitte verwenden Sie Parameter ALL, um alle festzulegen. Falls es Probleme mit bestimmten Merkmale wie der MOVE-Schaltfläche gibt, löschen Sie das Merkmal SST aus der Liste und die MOVE-Schaltfläche ist ausgegraut.
  - Anrufweiterleitung CF
  - Einzelschritt-Übergabe SST
  - TransferONHold TOH
  - HandoverFrom HF
  - Sip über Datenverbindung SIP
  - Nahtlose Übergabe SEHO
  - Erweiterte Alarmierung XA
  - Konsultationsaufruf CSC
  - Snooze DnD SDND
- VCPRIO1 bevorzugter Video-Codec (VP8 oder H264)
- VCPRIO2 alternativer Video-Codec (VP8 oder H264)

- SBCFQDN1-5 SBC Vollqualifizierter Domainname
- SBCADDR1-5 SBC IP-Adresse
- PORT1-5 SBC PORT

Anmerkung:

Im Allgemeinen definiert der FWDDESK Timer in AMO CTIME (Zweig CP2) die Zeit, zu der ein Anruf nach der Alarmierung an den Schreibtisch weitergeleitet wird, wenn der Anruf nicht angenommen wird.

Um die Weiterleitungszeit an das Tischtelefon im Falle eines nicht erreichbaren OSMO Clients zu reduzieren, ist es möglich, einen zusätzlichen Timeout-Wert im Gateway zu konfigurieren.

Dies führt zu einer schnelleren Weiterleitung an den Schreibtisch bei z. B. Netzwerkfehlern.

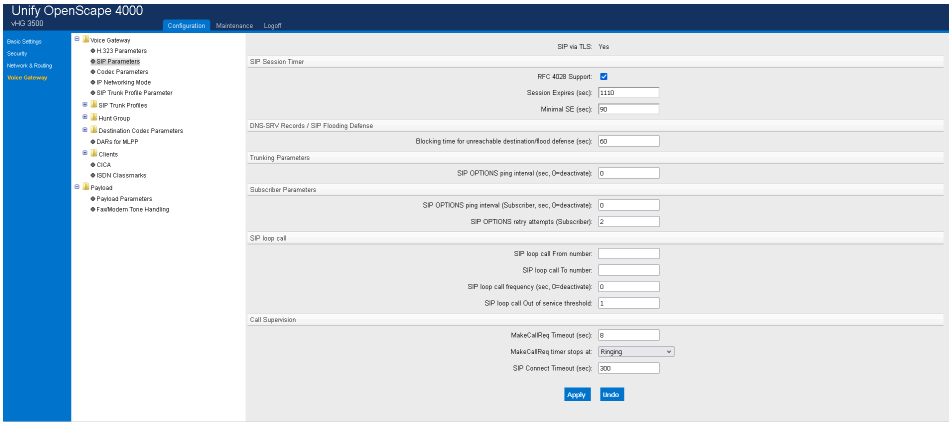
Timeout-Parameter:

”MakeCallReq Timeout” (SIP-Parameter - Anrufüberwachung).

Zusätzlich der Parameter:

"MakeCallReq Timeout stoppt bei" muss auf "Klingeln" festgelegt werden.

Siehe Beispiel unten:



15.1.3 Konfigurationsbeispiel

15.1.3.1 Konfiguration aufseiten von OpenScape 4000

Die OpenScape Mobile Clients werden über SoftGate (vHG-SIP) oder STMIX mit OpenScape4000 verbunden. Neben der regulären SoftGate-/STMIX-Konfiguration muss auch die Verknüpfung zwischen vHG und SG-CICA (Anwendung, die von CSTA gehostet wird) berücksichtigt werden.

Die IP-Adresse für CSTA/CICA wird vom NGS an das SoftGate/STMIX geliefert.

Daher muss die NGS-IP-Adresse im Portal konfiguriert werden. Das Portal konfiguriert automatisch die NGS-IP-Adresse in AMO SIPCO: LSNET, NGS; (obligatorisch für die SoftGates/STMIX beim Start).

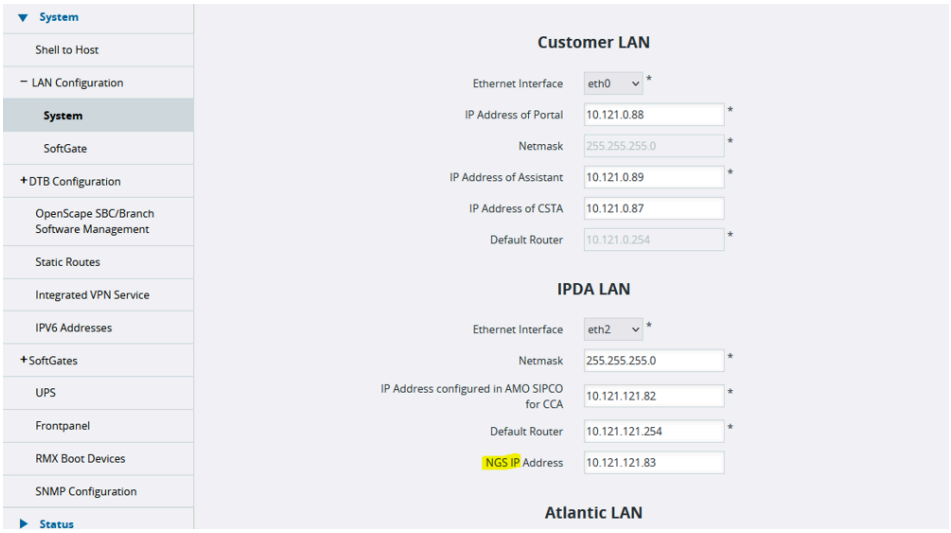


Abbildung 294: NGS-Konfiguration (Portal)



Abbildung 295: NGS-Konfiguration (SoftGate)

Wichtig: Wenn die IP-Adresse des NGS nach der Inbetriebnahme des SoftGate konfiguriert wird, muss das SoftGate neu gestartet werden.

Anmerkung: Ein gültiger KNDEF-Eintrag ist obligatorisch mit definiertem CC, AC und LC für E164-UFIP-Registrierung bei OpenScape Mobile Client. Für Länder, die keine KNDEF-Codes verwenden, kann stattdessen ein KNDEF KNOWNET-Eintrag erstellt und mit AMO SDAT mit OpenScape Mobile Client-Geräten verknüpft werden.

CSTA-Konfiguration

CICA in CSTA kann als eigene Anwendung betrachtet werden.

Standardmäßig wird Port 1040 für die Verbindung zu CA4000_default verwendet.

Am verwendeten Port/CA4000 muss die Unterstützung des E164-Rufnummernformats und die ONS-Überwachung aktiviert sein.

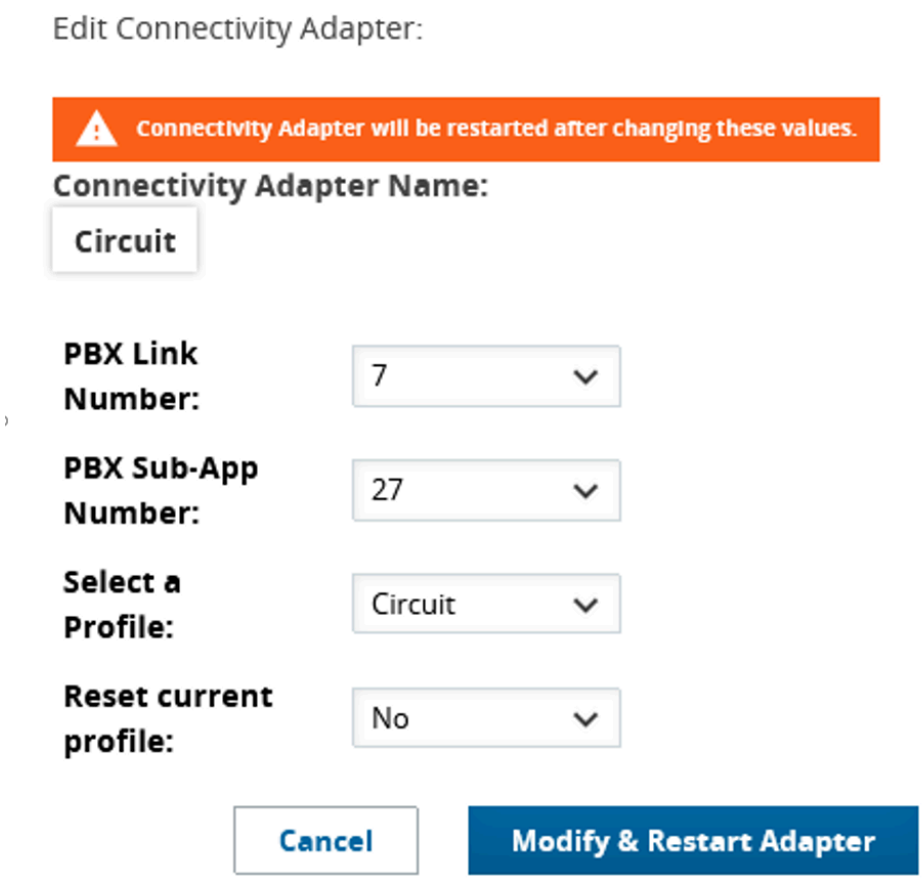


Abbildung 296: CA4000 Standardkonfiguration

Die CICA-Anwendung muss mit der richtigen Anschlussnummer konfiguriert und dann durch Aktivieren der Option „Auto start“ und Klicken auf „Start“ gestartet werden:

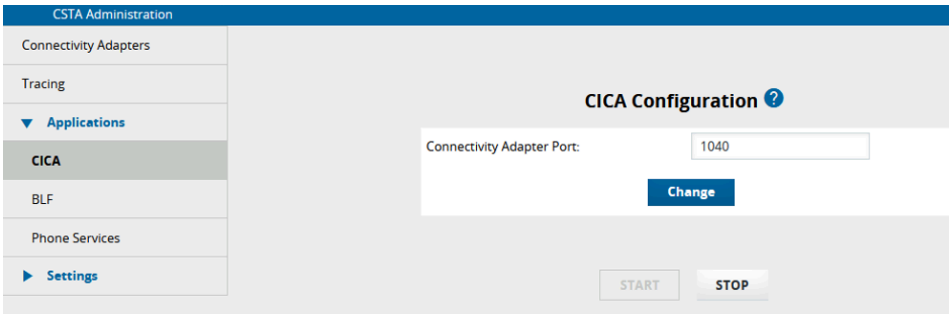


Abbildung 297: CICA-Konfiguration

Bei Bedarf kann die Standardkonfiguration geändert und ein neuer/anderer Port bzw. eine neue/andere Anwendung konfiguriert werden.

Nachdem Sie die NGS IP-Adresse konfiguriert und sich vergewissert haben, dass die CSTA CICA-Anwendung mit der richtigen Konfiguration gestartet wurde, können Sie ihren Status im WBM der vHG (SIP)-Baugruppe überprüfen. Die vHG, bei der sich die OpenScape Mobile Clients am

OpenScape 4000 anmelden werden, muss unter der Registerkarte „CICA Verbindungsstatus“ den Status „Registrierung bei CICA erfolgreich“ anzeigen:

Die Standardkonfiguration sollte wie in der folgenden Abbildung aussehen:

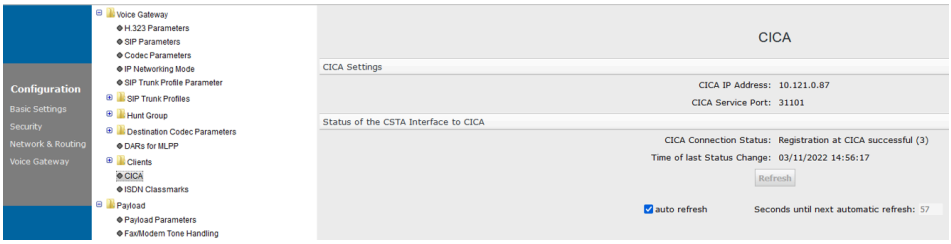


Abbildung 298: vHG WBM CICA-Statusseite

Benutzerkonfiguration in OpenScape 4000

Jeder OpenScape Mobile Client Client wird in OpenScape 4000 als UFIP SIP-Gerät registriert: Der Client wird über den Parameter CLNTDESK mit einem tatsächlichen Desktop-Telefon verknüpft:
`ADD-SBCSU:STNO=<UFIP_STN>,OPT=OPTI,CONN=IP2,PEN=<X-Y-Z-T>,DVCFIG=UFIP, CLNT▶`
`DESK=<DSKTP_PHN_STN>`

Die korrekte Verknüpfung kann wie folgt geprüft werden:

DIS-SBCSU für UFIP STN zeigt Folgendes an:
`DESK=<DSKTP_PHN_STN>`

DIS-SBCSU für Desktop-Telefon STN zeigt Folgendes an:
`CLIENT=<UFIP_STN>`

Der Parameter CLNTDESK kann nicht über CHANGE-SBCSU geändert werden. Um ihn zu ändern, muss der UFIP-SIP-Client gelöscht und mit dem neuen CLNTDESK-Wert neu konfiguriert werden. UFIP-SIP-Clients werden aus der Perspektive der Lizenz nicht gezählt.

Nach der Konfiguration der SBCSU-Kopplung zwischen Deskphone und Client kann die Konfiguration auf dem SIP HG WBM unter Konfiguration -> Voice Gateway -> Clients -> UFIP SIP überprüft werden (Abbildung 7). Weiterhin kann überprüft werden, ob alles korrekt konfiguriert ist und die Verknüpfung zu der ONS-Nummer passt, die für die Kundenregistrierung verwendet wird. Auch nach einer erfolgreichen Registrierung wird der Eintrag fett gedruckt.

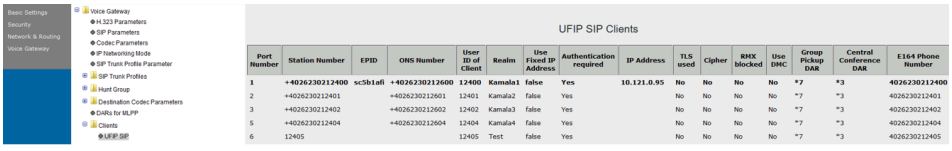


Abbildung 299: Clientkonfiguration

Der Anruf wird vom OpenScape Mobile Client auf das Desktop-Telefon verschoben, wenn der FWDDESK-Timer abläuft. Der FWDDDESK-Timer ist mit folgendem AMO-Befehl konfigurierbar:
`AENDERN-CTIME:TYPESWU=CP2,FWDDESK=xx;`

Anforderungen

- OpenScape Mobile UFIP-Teilnehmer müssen auf SoftGate vHG mit SIP-Funktionalität (BFDAT) konfiguriert werden.
- „Enable Cluster Server“ (wie in „Remote Endpoints“ für Circuit Advanced Telephony Connector verwendet) wird für „Remote Subscribers“ (die für die OpenScape Mobile-Endpunkte verwendet wird) nicht unterstützt. Bitte beachten Sie daher – falls Clustered Server verwendet werden –, dass nur

das erste OS4K-Gateway in der Cluster Server Liste für OSMO-Endpunkte verwendet werden kann.

- Das Tischtelefon kann TDM, HFA oder UFIP SIP sein.

Wichtig: Die Sicherheit muss auf der OpenScape4000-Seite aktiviert sein.

15.1.3.2 CICA-Konnektivität zu OS4K

Das vom OpenScape Mobile Client verwendete CSTA-Protokoll ist ein Klartextprotokoll, das keine Verschlüsselung unterstützt. Die integrierte VPN-Funktion erhöht die Sicherheit, da ein virtuelles privates Netzwerk erstellt wird, in dem der Netzwerkverkehr verschlüsselt übertragen wird; dieses Netzwerk verbindet die entfernten Komponenten eines OpenScape 4000-Systems (OS4k).

Anmerkung: Detaillierte Informationen zur Einrichtung des integrierten VPN-Dienstes finden Sie in OpenScape 4000 V8 - Plattform-Administration (Portal), Administratordokumentation, Kapitel Integrierter VPN-Dienst.

Wenn die VPN-Funktion aktiviert ist, wird zwischen dem OS4k-Hostsystem und den SoftGates ein VPN-Netzwerk erstellt, in dem der Datenverkehr zwischen den vHG-Baugruppen und CSTA verschlüsselt übertragen wird. Dies umfasst auch den CICA-Konnektivitätsverkehr.

Wenn die Einrichtung der integrierten VPN-Funktion fehlschlägt, wird der CICA-Verkehr direkt über das IPDA-LAN geleitet (immer noch im Klartext).

15.1.3.3 Konfiguration von OpenScape Mobile Client

Gehen Sie in der OpenScape Mobile-Anwendung auf Einstellungen > Konto und fügen Sie die erforderlichen Parameter hinzu:

Teilnehmernummer: <Die ONS-Nummer des 4K-Deskphones, z. B. +4989700731000 >

Serveradresse: <IP/Hostadresse von HG (SG/STMIX) oder SBC> (TLS Port 5061 wird automatisch hinzugefügt)

Passwort: <SBCSU Passwort von UFIP Konfiguration>

Mobilenummer: <z. B. +4916098947000>

Die detaillierte Konfiguration entnehmen Sie bitte der OpenScape Mobile-Anwendungsdienstdokumentation: **OpenScape Mobile V9, Administratorendokumentation**, **OpenScape Mobile V9, Android-Geräte, Bedienungsanleitung**, **OpenScape Mobile V9, Apple-Geräte, Bedienungsanleitung**.

15.1.3.4 OpenScape SBC-Konfigurationsbeispiel

OpenScape SBC-Nutzung ist obligatorisch

Merkmal Fernabonnent in OpenScape SBC muss aktiviert und verwendet werden, um die OSMO Pro Clients über den OpenScape SBC beim OS4K-Gateway, das die UFIP-Proxy-Geräte hostet, zu registrieren. Eine detaillierte Konfiguration von OpenScape SBC finden Sie im OpenScape SBC-Konfiguratonshandbuch.

Die detaillierte Konfiguration der Verbindung zum Apple-Push-Benachrichtigungsserver entnehmen Sie bitte der OpenScape Mobile Pro Administrator-Dokumentation.

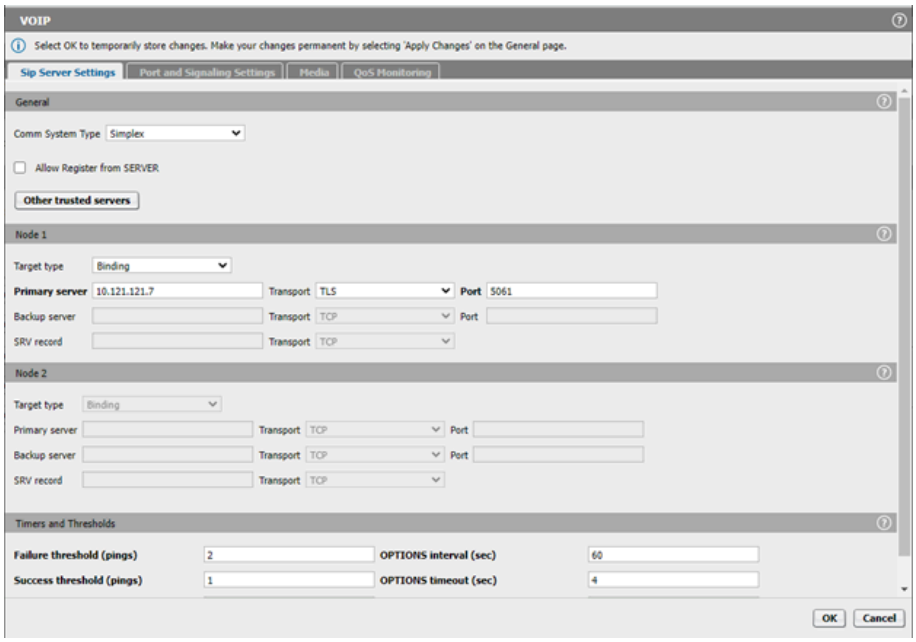
Es folgt ein kurzes Beispiel für eine OpenScape SBC-Konfiguration für OSMO Pro:

VoIP

Sip-Server-Einstellungen

4K Gateways (SIP-Abonnenten-Gateway > SoftGate/STMIX z. B. 10.121.121.7) werden über TCP auf 5060 oder TLS auf 5061 (für sichere Verbindung zwischen OS-SBC und 4K) in zwei Modi konfiguriert:

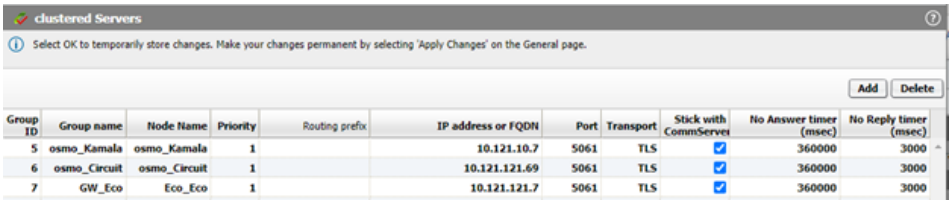
1) **Simplex-Modus** (Ein einzelner 4K GW wird verwendet):



2) **Clustered-Modus** (mehr 4K GW's auf demselben OS-SBC konfiguriert sind => mehr als 240 OSMO-Benutzer):

Wechseln Sie vom Simplex-Modus in den Cluster-Modus und fügen Sie die OS4K-Gateways mit "Priorität 1" hinzu.

Gehen Sie zu **VoIP> Sip-Server-Einstellungen>Comm Systemtyp** und wählen Sie **Clustered**.



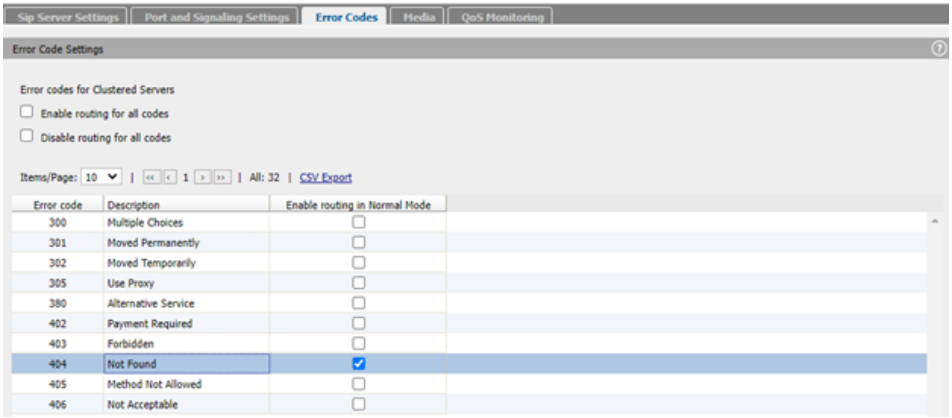
Als nächstes fügen Sie die Clustered Server hinzu.

IMPORTANT: Stick mit CommServer muss geprüft werden! Dies ist eine dedizierte Einstellung für OSMO-OS4K und SBC.

Aktivieren Sie den Fehlercode für 404 (SBC wird eine Nachricht umleiten, wenn es einen 404 Not Found erhält)

Zunächst sendet der SBC bei der OSMO-Client-Registrierung die REGISTER-Meldung an jeden GW, bis er eine positive Antwort erhält (100 Trying/200 OK), von den anderen GWs erhält er eine 404 Not Found.

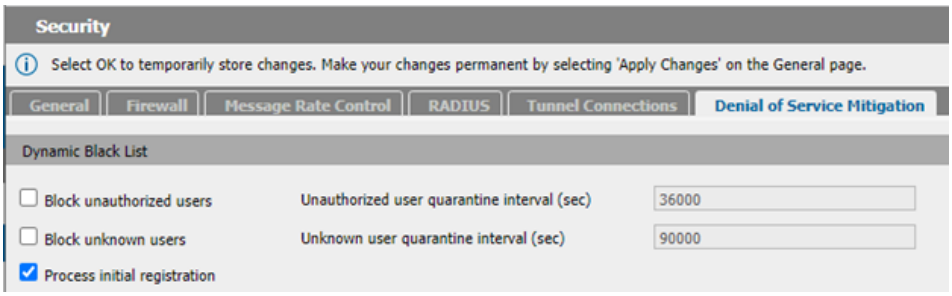
Gehen Sie zu **VoIP>Fehlercode** und aktivieren Sie das Kontrollkästchen **Weiterleitung für Fehlercodes aktivieren** für den Fehlercode 404.



NOTICE: Durch Auswählen von **Weiterleitung für alle Codes aktivieren**können alle Fehlercodes gleichzeitig für die Weiterleitung aktiviert werden.

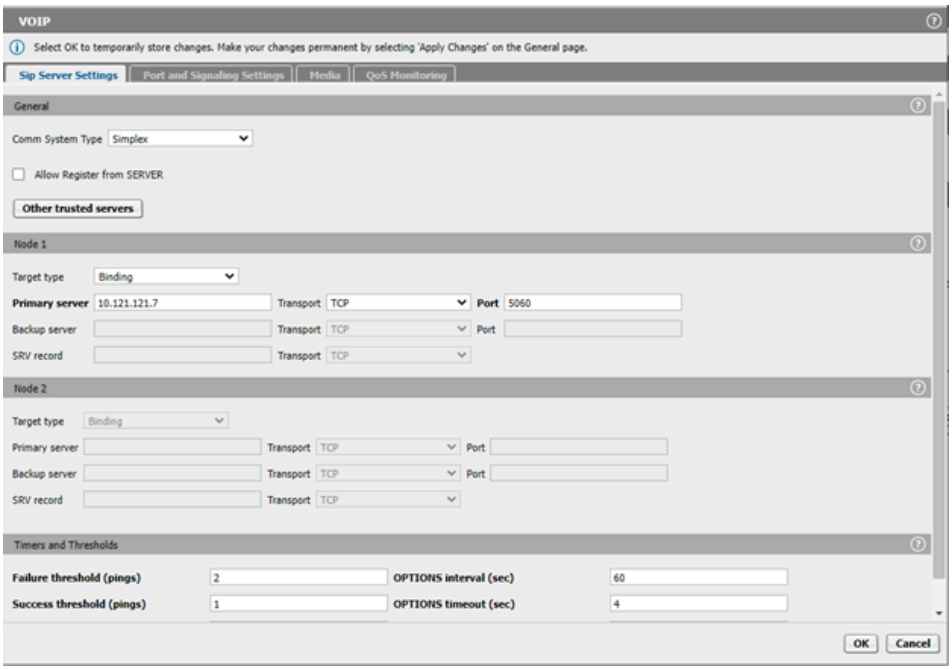
Aktivieren Sie das Flag **Erstregistrierung des Prozesses**, um den Registrierungsprozess zu erleichtern (andernfalls dauert der OSMO-Registrierungsprozess länger als 50 Sekunden).

Gehen Sie zu **Sicherheit**> **Denial-of-Service** und aktivieren Sie das Kontrollkästchen **Erstregistrierung des Prozesses**, um ihn zu aktivieren.

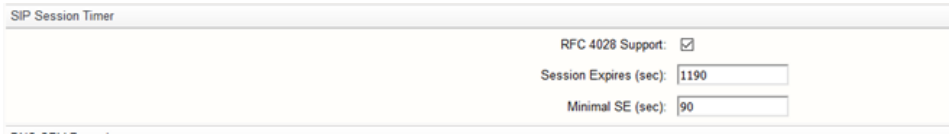


Port- und Signalisierungseinstellungen

Standardmäßig verwendet der OS-SBC für Nutzlast (z. B. Sprache) einen mit "Medienunabhängigen RTP-Ports" konfigurierten UDP-Portbereich. In diesem Beispiel wurden diese Ports von "Port Min" 35500 auf "Port Max" 35600 reduziert:



TCP-Verbindungslebensdauer muss einen Wert haben, der größer ist als der Sitzungsaktualisierungs-Timer im 4K-GW (SIP-Sitzungs-Timer-Sitzung läuft ab (Sek.)). Stellen Sie zum Beispiel die Lebensdauer der SBC-TCP-Verbindung auf die maximal zulässige Dauer (**1200 s**) und die der 4K GW-Verbindung auf **1190 s.**



Medien

OSMO-Medienmodus

Mögliche Konfigurationen:

OS4K (AMO ZANDE:OSMO)	...	**OS-SBC**
RTP	>	Nur RTP
SRTP	>	Nur SRTP **oder** Best-Effort-SRTP
BESTEFRT	>	Nur SRTP **oder** Best-Effort-SRTP

Für **RTP**, das in ZANDE:OSMO konfiguriert ist, müssen diese Änderungen vorgenommen werden:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = RTP
   SECOSBC   = RTP
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +---------------------------------------+
   |     VIDEO CODEC LIST                  |
   +---------------------------------------+
   | PRIO1 :  CODEC = H264                 |
   | PRIO2 :  CODEC = VP8                  |
   +---------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                    |
   |                      QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                  |

 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                    |
   |SBCFQDN4 =
                    |
   |SBCFQDN5 =
                    |

 +-------------------------------------------------------------------
+

AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

Für SRTP oder Best-Effort-SRTP, die in ZANDE:OSMO konfiguriert sind, müssen diese Änderungen vorgenommen werden:

SRTP:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = SRTP
   SECOSBC   = SRTP
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +----------------------------------------+
   |     VIDEO CODEC LIST                   |
   +----------------------------------------+
   | PRIO1 :  CODEC = H264                  |
   | PRIO2 :  CODEC = VP8                   |
   +----------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                  |
   |                     QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                 |

 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                  |
   |SBCFQDN4 =
                  |
   |SBCFQDN5 =
                  |

 +-------------------------------------------------------------------
+

AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

Best-Effort-SRTP:

```
DISP-ZANDE:OSMO;
H500:  AMO ZANDE STARTED
   SERVMAIL  = test@unify.net
   OSVTLS    = 0
   SBCSTLS   = 0
   QOSVIDEO  = 0
   DSCPTOS   = NO
   WMM       = YES
   SECOSV    = BESTEFRT
   SECOSBC   = BESTEFRT
   FEATLIST  = CF&SST&TOH&HF&SIP&SEHO&XA&SDND&CSC&FC1&GPC
   +----------------------------------------+
   |     VIDEO CODEC LIST                   |
   +----------------------------------------+
   | PRIO1 :  CODEC = H264                 |
   | PRIO2 :  CODEC = VP8                   |
   +----------------------------------------+

 +-------------------------------------------------------------------
+
   |                         LIST OF IP ADDRESSES OR FULLY
                    |
   |                      QUALIFIED DOMAN NAMES FOR SBC
 GATEWAYS                  |

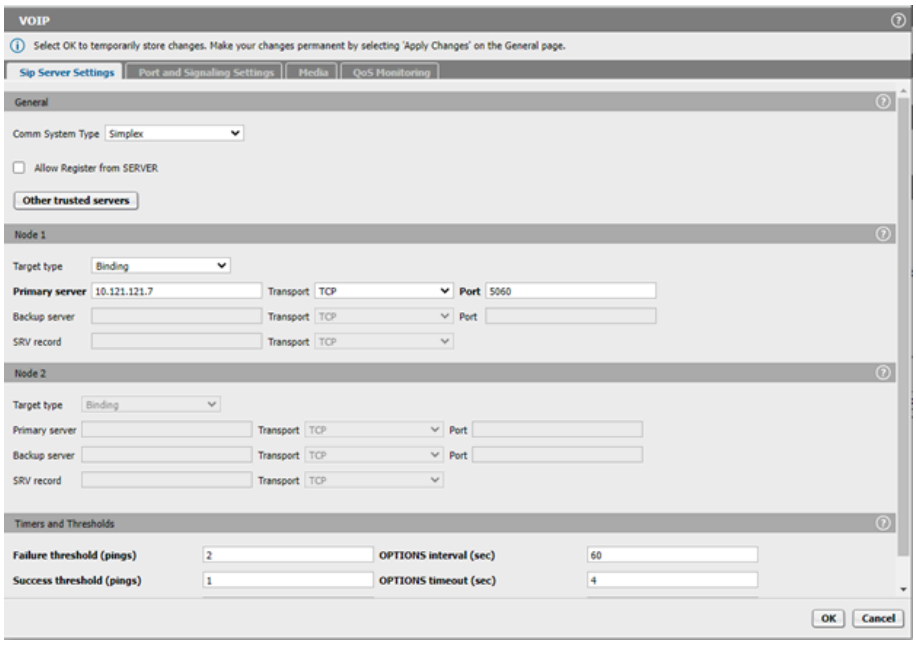
 +-------------------------------------------------------------------
+
   |SBCADDR1 = x.x.x.x.       PORT1 = 5061
    |
   |SBCADDR2 = x.x.x.x        PORT2 = 5061
    |
   |SBCFQDN3 =
                    |
   |SBCFQDN4 =
                    |
   |SBCFQDN5 =
                    |

 +-------------------------------------------------------------------
+

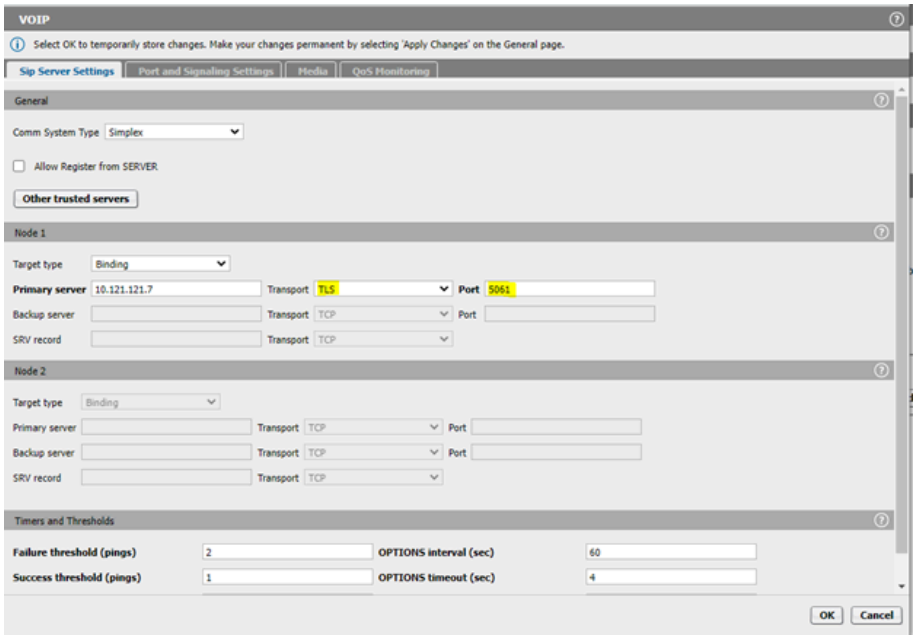
AMO-ZANDE-111       SYSTEM DATA - EXTENDED
DISPLAY COMPLETED;
```

1) Falls **TLS** zusammen mit **SRTP** oder **Best-Effort-SRTP** gegenüber dem 4K verwendet werden soll, muss zuerst **SPE (Signalisierung und Nutzlast-Verschlüsselung)** auf 4K-Seite aktiviert werden (SPE darf nicht für **TCP** und die Nutzung von **RTP**aktiviert sein)

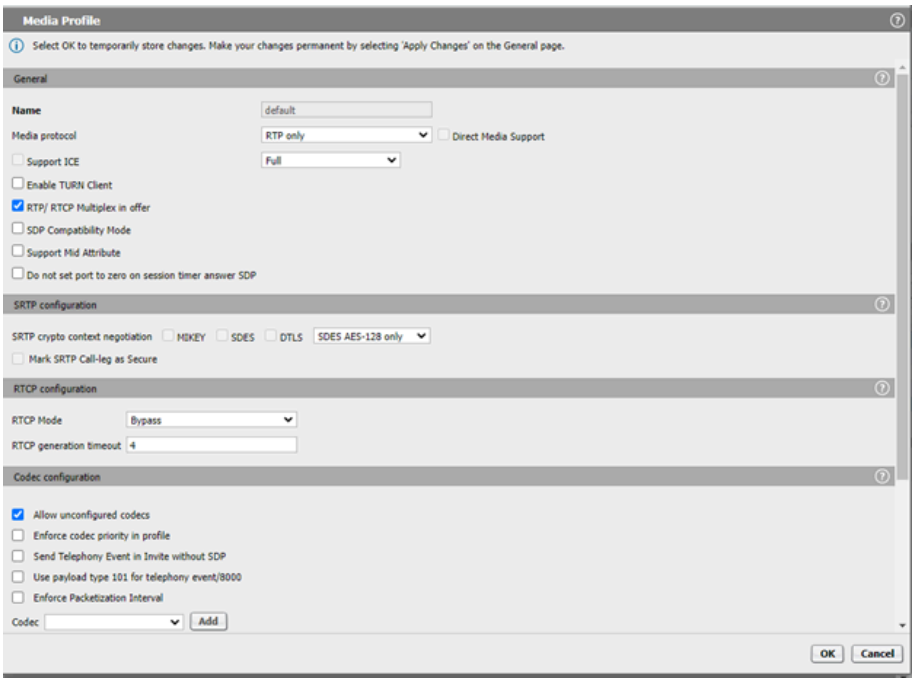
2) OS-SBC: VoIP > Sip-Server-Einstellungen, Switch-Transport für 4K GW als: über TCP und 5060 wenn **RTP** verwendet wird



über TLS und 5061 wenn **SRTP** oder **Best-Effort-SRTP** verwendet wird:

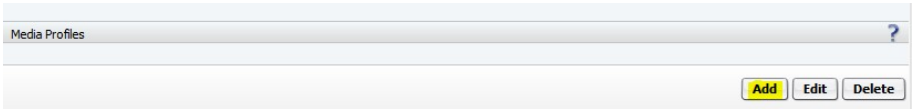


3) Für OSMO müssen dedizierte Medienprofile erstellt werden:

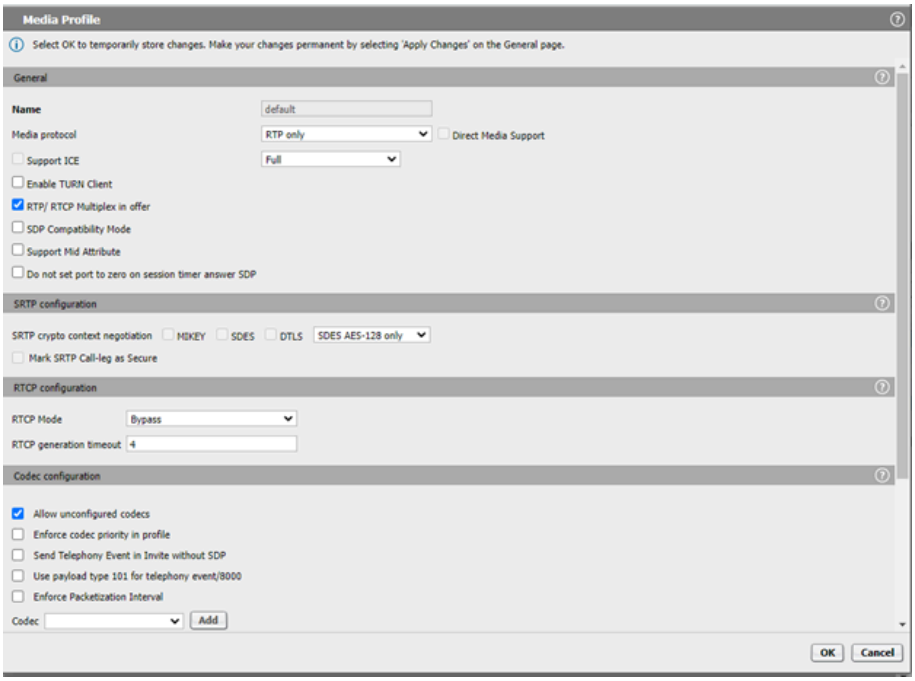


VoIP > Medien > Hinzufügen des neuen **Medienprofils:**

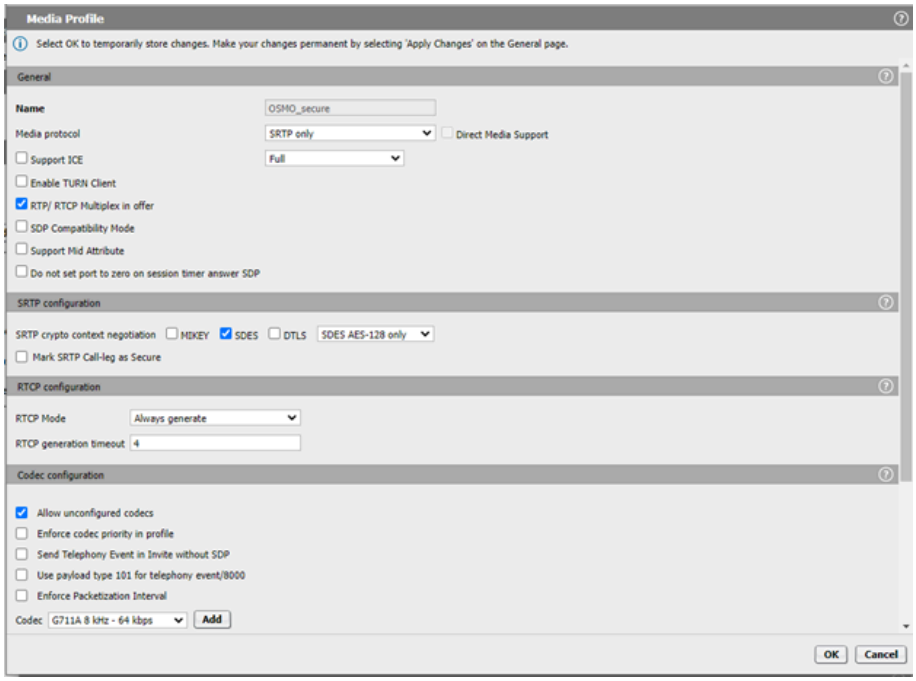
RTP:

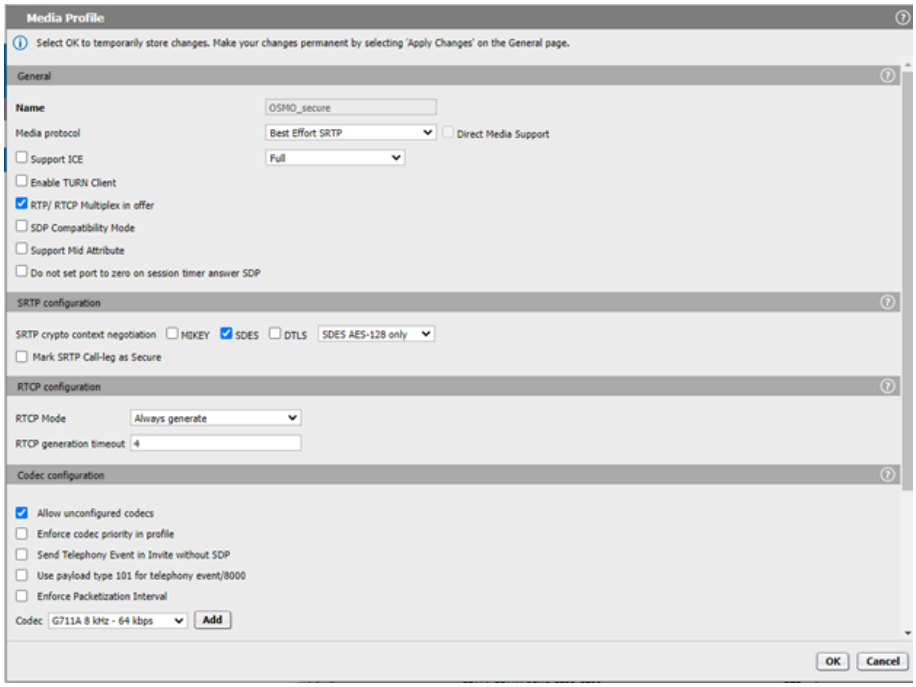


SRTP (Nur mit SDES verwendet):

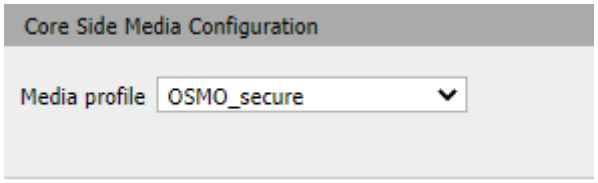


Best-Effort-SRTP (Nur mit SDES verwendet)



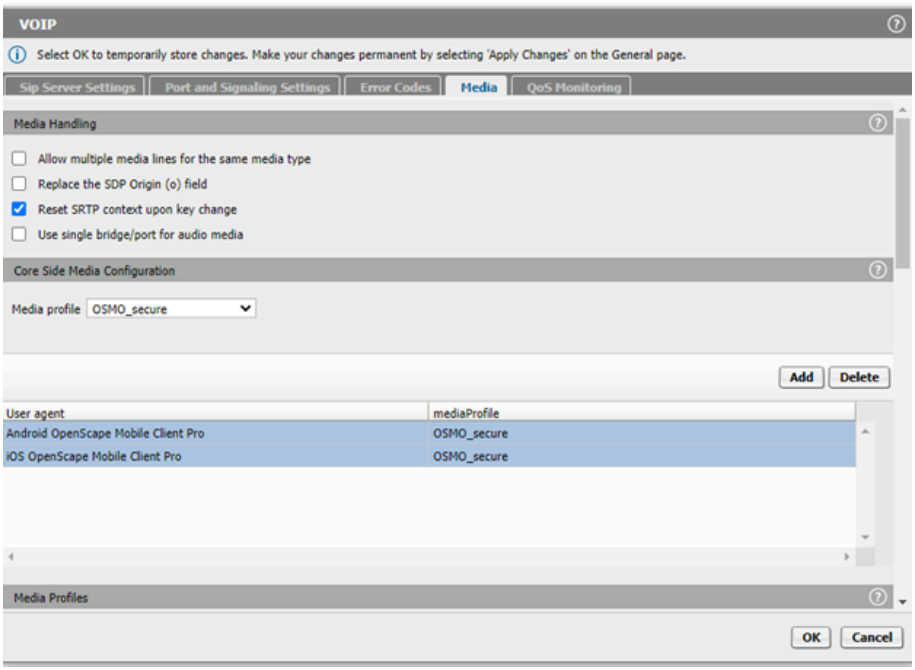


4) Wählen Sie dann das gewünschte Profil als "Kernseitige Medienkonfiguration" entsprechend Ihrer Konfiguration (RTP, SRTP oder BEST-Effort-SRTP)



5) Fügen Sie das bereits oben konfigurierte Medienprofil zum Benutzeragenten des OSMO-Clients hinzu:

- Android OpenScape Mobile Client Pro
- iOS OpenScape Mobile Client Pro



Denken Sie daran, dass Sie die Konfiguration immer speichern müssen, vergessen Sie nicht, die Änderungen zu übernehmen (auf der Hauptseite):



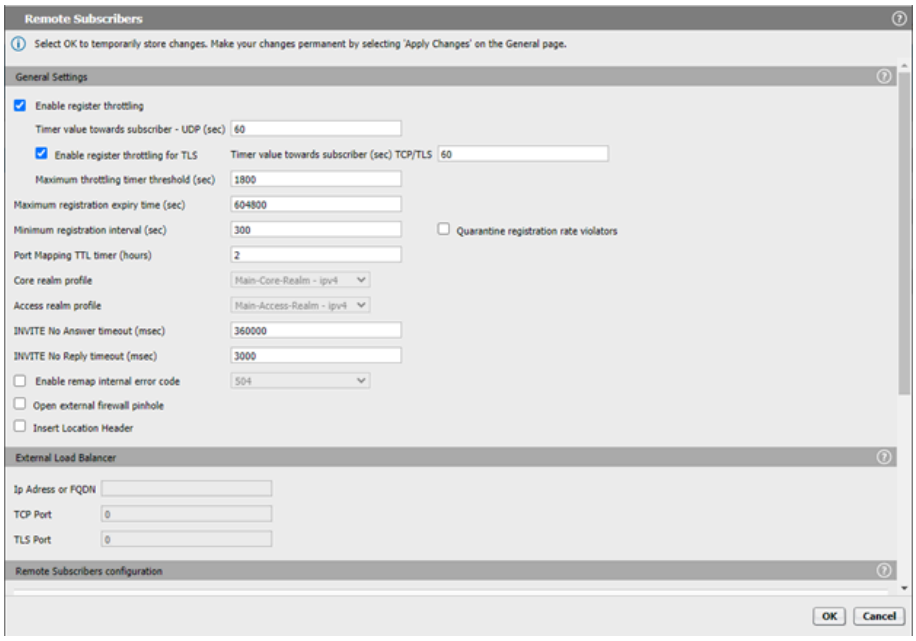
6) Gehen Sie zu Merkmale > und aktivieren Sie Enable Remote Subscribers



7) Drücken Sie Konfigurieren:

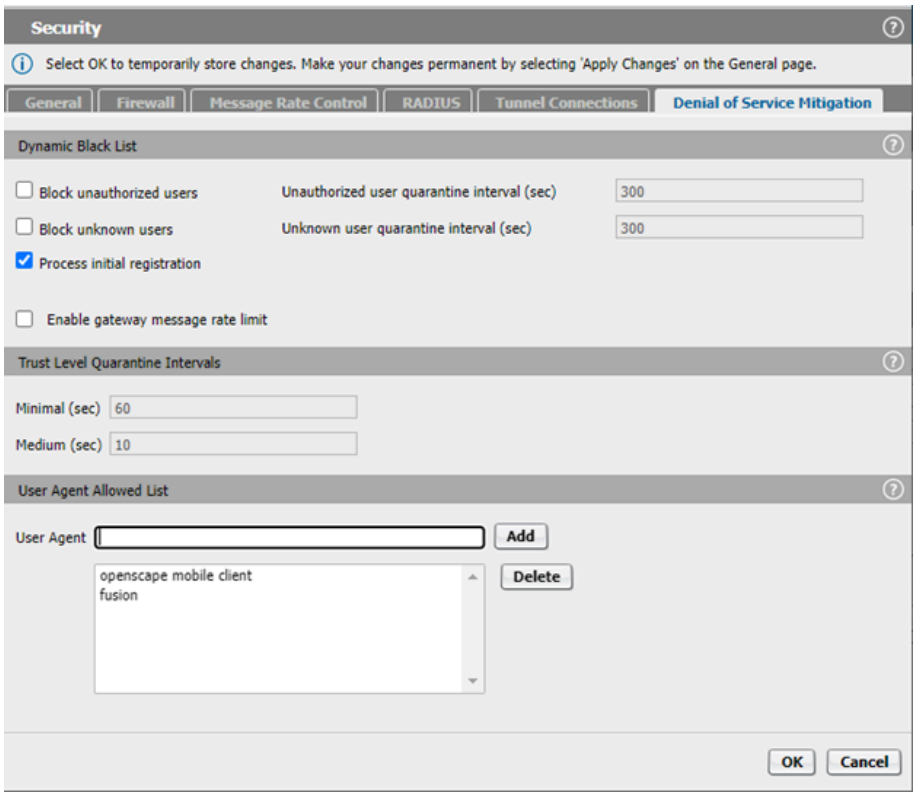


8) Konfigurieren Sie die Parameter wie unten beschrieben:



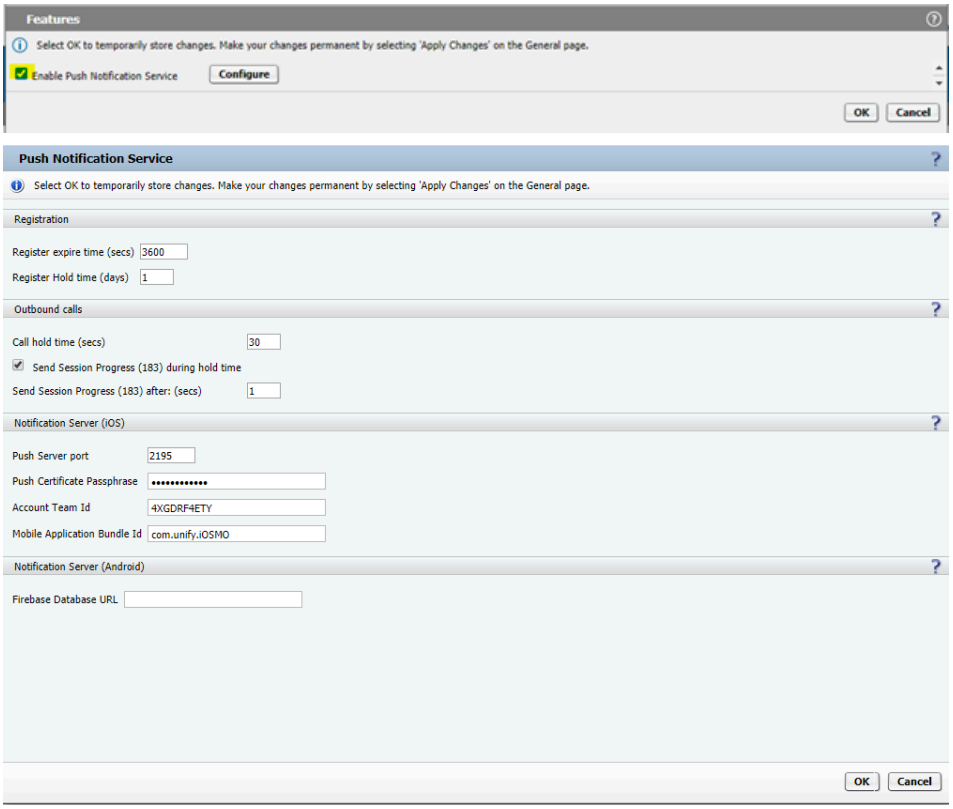
9) Navigieren Sie zu **Sicherheit > Denial-of-Service-Minderung** und aktivieren Sie **Prozess-Erstregistrierung**.

Wenn Sie eine **Liste der zulässigen Benutzeragenten**haben, stellen Sie sicher, dass der **openscape mobile client** Benutzeragent hinzugefügt wurde.



OpenScape Mobile Pro iOS verwendet APNs (Apple Push Notification), diese im OS-SBC aktiviert werden müssen:

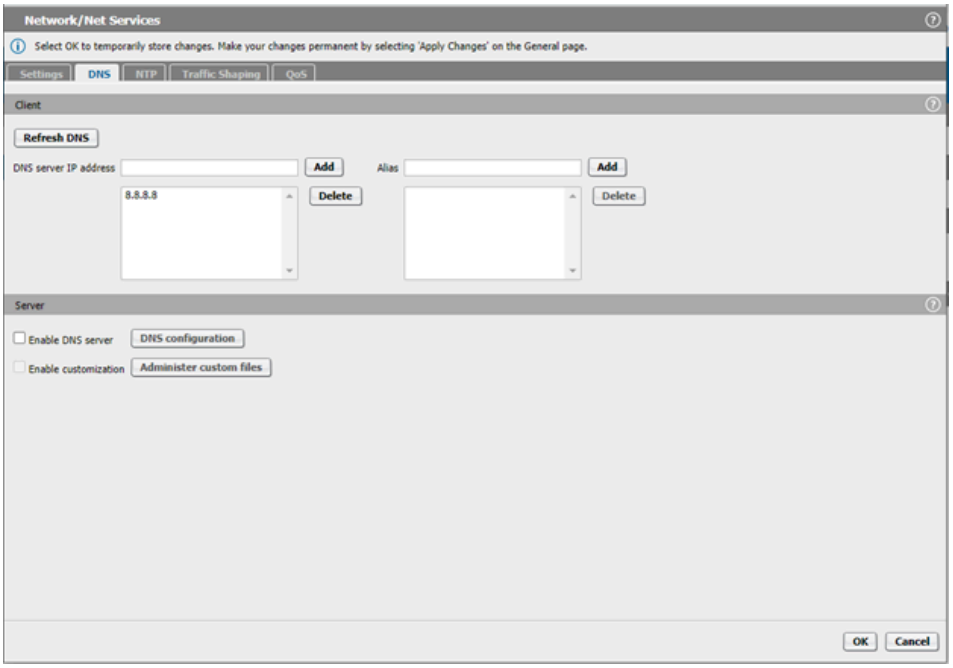
Merkmale > und aktivieren Sie Enable Push Notification Service



Wenn die Konfiguration des Benachrichtigungsservers, z. B. Push-Zertifikat-Passphrase, Account Team Id oder Mobile Application Bundle Id, nicht eingestellt ist, lesen Sie bitte die OpenScape Mobile Pro Administrationsdokumentation.

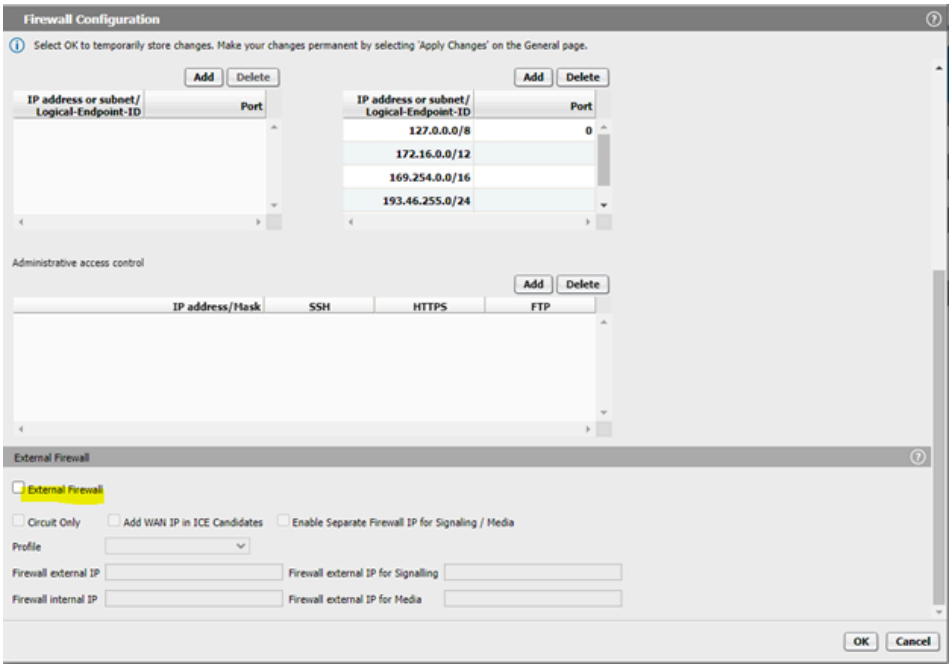
Netzwerk/Netzdienste > DNS

Der OS-SBC muss den Hostnamen des Apple Push Notification Service auflösen, dazu benötigt er eine Verbindung zu einem DNS-Server, z. B.



Sicherheit > Firewall

Befindet sich die Zugriffsseite des OS-SBC im NAT hinter einer externen Firewall, dann konfigurieren Sie bitte die IP-Adresse der externen Firewall entsprechend:



15.1.3.4.1 OpenScape SBC Redundanz-Modus

Siehe dazu OpenScape SBC V10 Konfigurationshandbuch, Kapitel 3.4.3.9.3 OS SBC Kollokierte Redundanz.

Die einzige spezifische Konfiguration, die für die Verbindung OpenScape 4000 - SBC vorgenommen werden muss, ist die Änderung der öffentlichen SBC-IP in AMO ZANDE:OSMO. Hier muss die (oben konfigurierte) **virtuelle WAN-IP** angegeben werden.

15.1.3.5 Facade and UC configuration

Please see UC documentation for installation and configuration

OpenScape UC Application V9, Installation and Upgrade, Installation Guide

OpenScape UC Application V9 Configuration and Administration Guide

16 Unify Phone Konnektivität

16.1 Überblick

Unify Phone ist ein Telefonieanschluss für Unify Video. Es fungiert als Brücke zwischen OpenScape 4000 und Unify Video und ermöglicht es den Benutzern, mit Unify Phone-Clients Anrufe über ihre geschäftliche Telefonnummer zu tätigen und entgegenzunehmen.

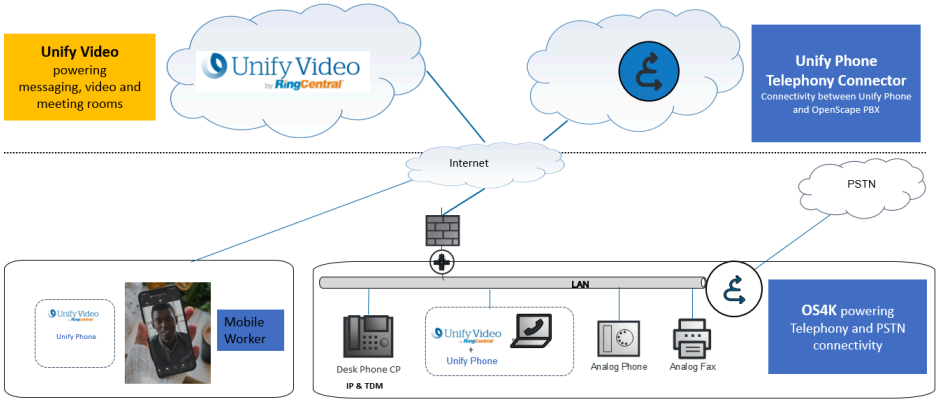


Figure 300: Unify Phone Übersicht

16.1.1 Leistungsmerkmale

Unify Phone unterstützt die folgenden Merkmale:

- Einen Anruf tätigen
- Einen Anruf annehmen, ablehnen oder ablehnen
- DTMF-Befehle in einem Aufruf senden
- Halten und abrufen
- Stummschalten/Stummschaltung aufheben
- Einen Anruf weiterleiten
- Anrufe von anderen Unify Phone Clients, Tischtelefonen oder alternativen Geräten abrufen
- Drücken Sie den Anruf auf ein Tischtelefon oder ein alternatives Gerät, falls ein alternatives Gerät konfiguriert ist
- Einen zweiten Anruf tätigen oder annehmen
- Anrufe austauschen (abwechselnd)
- Zwei Anrufe zu einer Konferenz zusammenführen
- Anrufumleitung
- Alternative Nummer (One Number Service)
- Anruf-Routing
- Voicemail
- Cross-Launch von Unify Video
- Abholgruppe (nur für Web-Clients unterstützt)
- Sammelanschlüsse beginnend mit OS4K RMX V11R0.22.3 (mit Ausnahme der parallelen Sammelanschlüsse, die eine Beschränkung darstellen)

16.1.2 Architektur

Jeder Unify Phone-Benutzer muss in einem OpenScape 4000-System als UFIP-SIP-Gerät konfiguriert werden. Für dieses Client-Gerät ist eine Unify Phone-Lizenz erforderlich, aber es wird keine Flex-Lizenz verwendet (ähnlich wie bei OSMO). Dennoch erfordert das Tischgerät eines Unify Phone-Benutzers eine Flex-Lizenz, auch wenn das Tischtelefon nicht physisch vorhanden ist. Das UFIP SIP ist ein Zusatzgerät, daher sind direkte Anrufe nicht möglich und seine Nummer wird auf keinem Telefondisplay angezeigt. Die Unify Phone-Clients sind über die OpenScape 4000-Tischtelefonnummer des Benutzers erreichbar. Das physische Tischtelefon ist jedoch nicht zwingend erforderlich, es kann außer Betrieb sein oder ausgesteckt werden, aber die abgemeldeten Anschlüsse werden nicht als Tischtelefone unterstützt.

Der OpenScape 4000 Assistant synchronisiert die Benutzerdaten mit dem Unify Phone Telephony Connector. Daher muss der Assistant in der Lage sein, über das Internet auf den Telephony Connector zuzugreifen (entweder direkt oder über einen HTTPS-Proxy). Der OpenScape 4000 Assistant ruft alle Unify Phone-Benutzer, die in Unify Video konfiguriert sind, vom Telephony Connector ab. Wenn der Assistant eine passende Unify Phone-Konfiguration für einen Benutzer findet (basierend auf der E-Mail-Adresse), lädt er die erforderlichen Verbindungsdaten in den Unify Phone Connector hoch.

Unify Phone Web- und Mobile-Clients sind über SBC mit OpenScape 4000 verbunden. Der Clustermodus erlaubt es, die UFIP SIP-Geräte auf mehrere Gateways (GWY) auf SoftGates oder STMIX zu verteilen. Unify Phone-Clients können direkte Anrufe zu allen anderen OpenScape 4000-Teilnehmern, externe Anrufe (über Trunks) und umgekehrt tätigen. Es sind mehrere Registrierungen für denselben Unify Phone-Benutzer möglich. Alle registrierten Unify Phone-Clients und die Tischtelefone werden bei eingehenden Anrufen gleichzeitig benachrichtigt, wenn der Unify Phone-Benutzer "Standard-Routing" konfiguriert hat. Wenn ein zweiter Anruf signalisiert wird oder besetzt ist, hängt die Weiterleitung von den "Besetzt-Einstellungen" des Unify Phone-Benutzers ab.

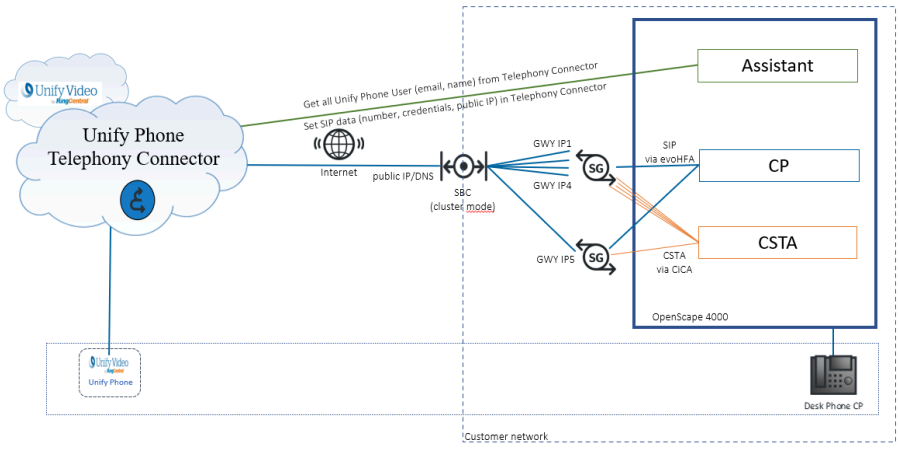


Figure 301: Unify Phone-Architektur

16.2 Interaktion mit Merkmalen und Einschränkungen

Die Zusatzgeräte für Unify Phone (z. B. OSMO) müssen auf einem SoftGate oder STMIX/STMIY konfiguriert werden (STMI2/STMI4 werden nicht

unterstützt). Das Zusatzgerät ist mit einem Tischtelefon verbunden, das die E.164-Nummer des Unify Phone-Benutzers definiert.

Die TDM-, HFA-, DECT- (klassisch und IP) und UFIP-SIP-Geräte können als Tischgeräte verwendet werden (klassische SIP- und analoge Geräte werden nicht unterstützt). Die Tischgeräte können außer Betrieb oder nicht angeschlossen sein. Es ist derzeit nicht möglich, die Verknüpfung eines Hilfsgeräts nach der Konfiguration zu ändern, aber Sie können den Typ des Hilfsgeräts über den Parameter CLNTTYPE in AMO-SBCSU ändern. Um die Verknüpfung zu ändern, muss das Hilfsgerät gelöscht und neu konfiguriert werden und in AMO-SBCSU muss ein neuer Wert für den Parameter CLNTDESK hinzugefügt werden.

Es ist möglich, Unify Phone und OSMO auf demselben SBC wie OpenScape 4000 zu konfigurieren, aber ein Unify Phone-Benutzer darf nicht für die parallele Nutzung von Unify Phone und anderen Anwendungen (z. B. UC, OSCC, C4B Xphone, OSMO usw.).

Da die CICA-Komponente von Unify Phone und OSMO gemeinsam genutzt wird, muss das UnifyPhone CSTA-Profil verwendet werden. Die Verwendung dieses Profils für OSMO-Clients im reinen SIP-Modus führt zu einer kurzen Verzögerung des Rufaufbaus von 2 Sekunden. Der CSTA-Konnektivitätsadapter, der für CICA verwendet wird, darf nicht gemeinsam mit anderen Anwendungen genutzt werden, die nicht das E.164-Nummernformat verwenden.

Es wird empfohlen, G.711 als bevorzugten Codec zu verwenden, da DTMF über OPUS-Codec noch nicht funktionsfähig ist.

Die folgenden OpenScape 4000-Funktionen werden in Verbindung mit Unify Phone nicht unterstützt:

- Gruppe CHESE (Chef/Sekretariat);
- Direktruftasten, die über AMO ZIEL mit der Tischtelefonnummer eines Unify Phone-Benutzers konfiguriert sind, signalisieren einen eingehenden Anruf erst, wenn er an das Tischtelefon weitergeleitet wird;

  NOTICE: Ab OpenScape 4000 V11R1 ist dieses Leistungsmerkmal nicht mehr verfügbar.

- Paralleles Klingeln (klassische ONS-Gruppe);
- Persönliche Gerätegruppe (Twinning);
- Parallele Sammelanschlüsse;
- Unterstützung für mehrere Leitungen;
- COM-Gruppen und einseitiges Direktansprechen.
- Geheimnummern (SSTNO = Y in AMO SBCSU) [14]
- Wenn das DECT-Endgerät ausgeschaltet ist, wird das Auto-Pilot-Routing nicht ausgeführt (z. B. Routing zu Alternativnummer oder Voicemail wird nicht ausgeführt)
- Die automatische Beantwortung von DECT-Endgeräten wird nicht unterstützt (ausgehende Anrufe, die aus der Anwendung mit der Option deskphone getätigt werden, müssen von einem physischen DECT-Endgerät beantwortet werden)

NOTICE:

[14] Dies ist eine vorübergehende Einschränkung.

Wenn die F5-Taste auf einem Web Client während eines aktiven Anrufs gedrückt wird, wird der Anruf abgebrochen.

F5 kann gedrückt werden, um Anzeigeprobleme zu beseitigen, die nur im Ruhezustand auftreten.

16.3 Konfiguration

Für die Erstkonfiguration muss die Konnektivität zwischen OpenScape 4000, SBC und Unify Phone Telephony Connector hergestellt werden. Weitere Informationen finden Sie in Connector-Konfiguration.

Nach der Erstkonfiguration können neue Unify Phone-Benutzer von OpenScape 4000 aus konfiguriert werden. Weitere Informationen finden Sie in Benutzerkonfiguration.

16.3.1 Connector-Konfiguration

16.3.1.1 Konfigurieren des Unify Phone Telephony Connectors

Registrieren Sie Ihren Unify Video-Mandanten in Unify Phone Telephony Connector über https://phoneapp.unify.com/tenant/. Um sich zu authentifizieren, benötigen Sie ein Unify Video-Konto mit der Rolle "Super Admin".

Weitere Informationen finden Sie unter Unify Phone Administration.

16.3.1.2 OpenScape 4000 konfigurieren

Konfigurieren Sie den Zugang zu Unify Phone Telephony Connector

1) Öffnen Sie den OpenScape 4000 Assistant und navigieren Sie zu **Konfigurationsverwaltung** > **Unify Phone**, um die Konnektivität zum Unify Phone Telephony Connector zu konfigurieren.

2) Überprüfen Sie den Status von **Unify Phone Cloud** in der oberen linken Ecke des Fensters:

   - **Unify Phone Cloud ist nicht erreichbar** bedeutet, dass Sie möglicherweise einen Proxy konfigurieren müssen, um auf das Internet zuzugreifen.
   - **Kein oder falscher API-Schlüssel** bedeutet, dass der Connector erreichbar ist, Sie aber den API-Schlüssel Ihres Mandanten nicht eingegeben haben.

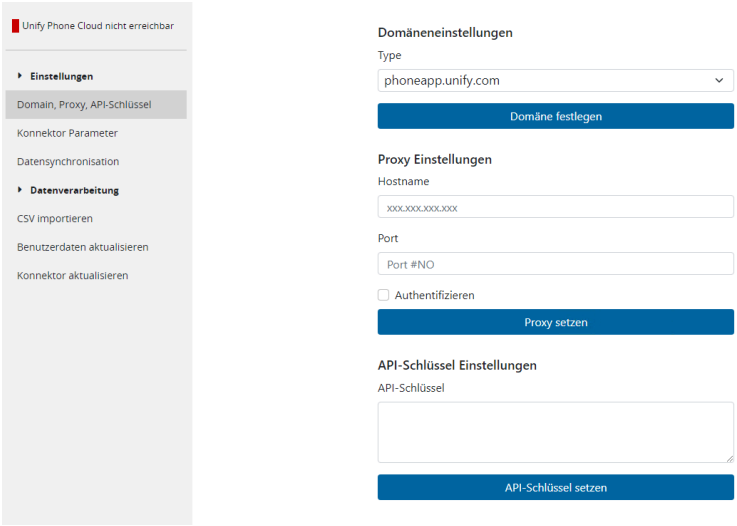


Figure 302: Unify Phone Cloud-Status

3) Melden Sie sich beim Unify Phone Telephony Connector über https://phoneapp.unify.com/tenant/ mit einem Super-Admin-Konto an.

   Auf der Registerkarte **Telephony Connector** können Sie den API-Schlüssel kopieren, dann in das Feld API-Schlüssel einfügen und auf **API-Schlüssel festlegen** klicken.

   Wenn der API-Schlüssel korrekt ist, ändert sich der Status in grün **Unify Phone Cloud ist erreichbar**. Nach dem Festlegen des API-Schlüssels wird die Eingabe aus Sicherheitsgründen ausgeblendet.

CICA konfigurieren

Unify Phone erfordert eine aktive CICA-Verbindung für alle Gateways, bei denen Zusatzgeräte zur Weiterleitung von CSTA-Nachrichten zwischen Client und CSTA konfiguriert sind. Ohne eine aktive CICA-Verbindung kann sich Unify Phone nicht registrieren und zeigt **Telefonie ist nicht aktiv** an. Die Gateways verbinden sich aus Sicherheitsgründen über VPN mit dem CICA-Service-Port 31101. Weitere Informationen finden Sie im Kapitel "Integrierter VPN-Dienst" im Dokument OpenScape 4000 V10, Plattformadministration (Portal).

Der Status kann im WBM-Bereich des Gateways überprüft werden:

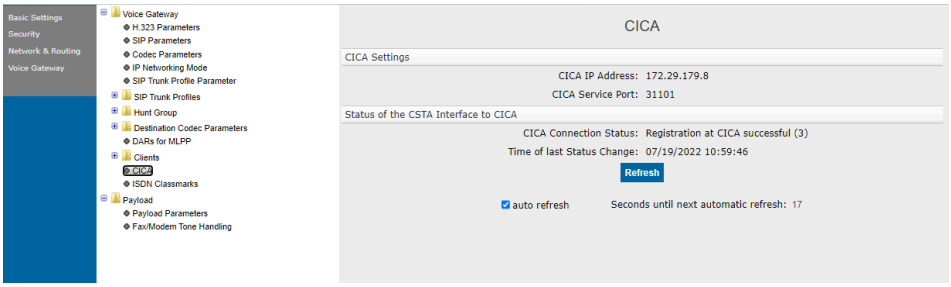


Figure 303: CICA konfigurieren

CICA ist eine spezielle Anwendung in CSTA. Standardmäßig wird der Port 1040 des Standardkonnektivitätsadapters verwendet, aber Unify Phone benötigt das **Circuit**-Profil. (E164_NUMBER_FORMAT=1, OFFERED_MODE_NEEDED=1, ONS_MONITORING=1).

Wenn der Standard-Konnektivitätsadapter für andere Anwendungen verwendet wird, empfiehlt es sich, einen eigenen Konnektivitätsadapter mit dem Circuit-Profil an einem anderen Port zu erstellen. Gehen Sie dafür wie folgt vor:

1) Navigieren Sie zu **Expertenmodus** > **CSTA** und klicken Sie auf **Konnektivitätsadapter hinzufügen**.
2) Wählen Sie eine verfügbare **PBX-Link-Nummer** (z. B. 7) und **PBX-Sub-App-Nummer** (z. B. 27) aus und wählen Sie dann das **Circuit**-Profil, wie in der Abbildung unten dargestellt.

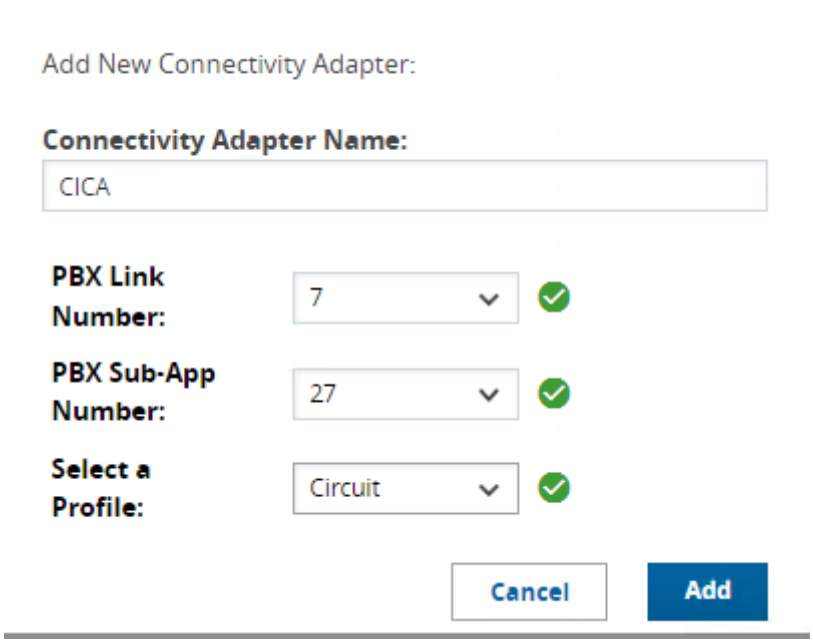


Figure 304: Name des Konnektivitätsadapters

Klicken Sie auf **Hinzufügen**.

3) Klicken Sie unter **CSTA-Verwaltung** > **Konnektivitätsadapter** auf die Schaltfläche **Neue Anwendung hinzufügen** neben dem im vorherigen Schritt erstellten Konnektivitätsadapter.

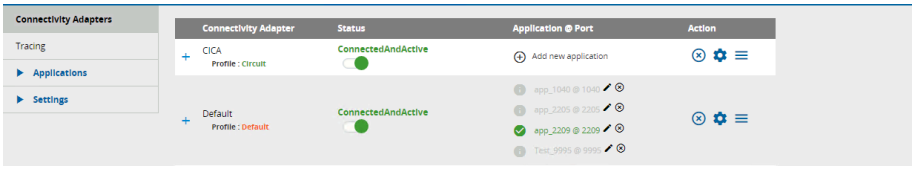


Figure 305: Hinzufügen einer neuen Anwendung in der CSTA-Verwaltung

4) Definieren Sie einen Port (z. B. Port 1041) für CICA und konfigurieren Sie denselben Port auf der Seite CICA-Konfiguration.

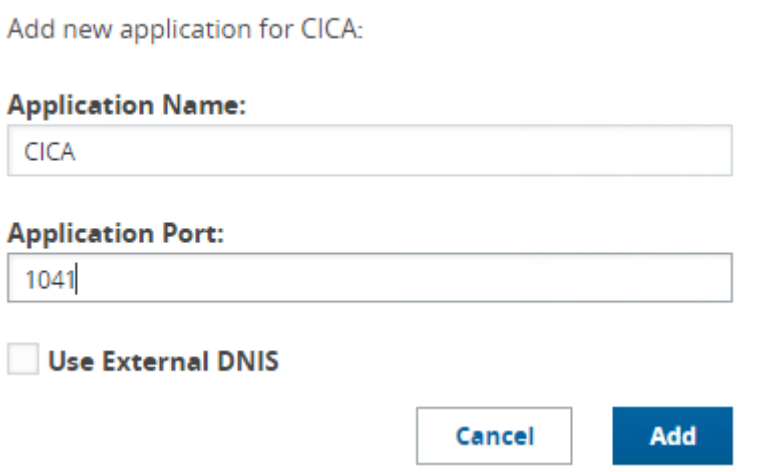


Figure 306: Definieren des CICA-Ports

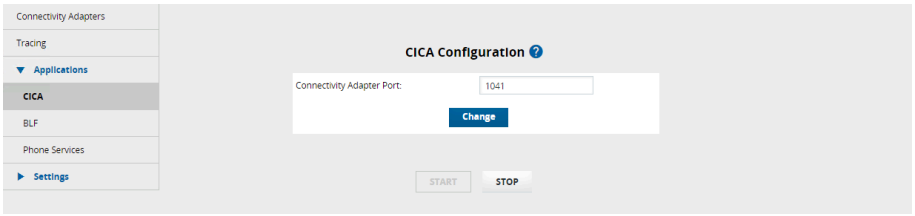


Figure 307: CICA-Konfigurationsport

Konfigurieren einer externen SBC-Adresse

Unify Phone wird von OpenScape 4000 immer sicher konfiguriert (TLS). Die externe IP des SBC (bei NAT ist es die externe IP der Firewall) und der SIP-TLS-Port müssen im OpenScape 4000 Assistant (ähnlich OSMO) in der AMO-ZANDE im OSMO-Zweig konfiguriert werden. Nur IP-Adresse 1 wird für Unify Phone verwendet.

Sie können entweder einen FQDN-Namen oder eine IP-Adresse konfigurieren:

- Befehl AMO-ZANDE:
  ```
  CHANGE-ZANDE:TYPE=OSMO, SBCFQDN1="os4k.unify.com",
   SBCADDR1=0.0.0.0, PORT1=5061;
  ```

- Mit OpenScape 4000 Assistant oder Manager, indem Sie zu **Konfigurationsverwaltung** > **Netzwerk** > **System** navigieren, wie in der folgenden Abbildung dargestellt.

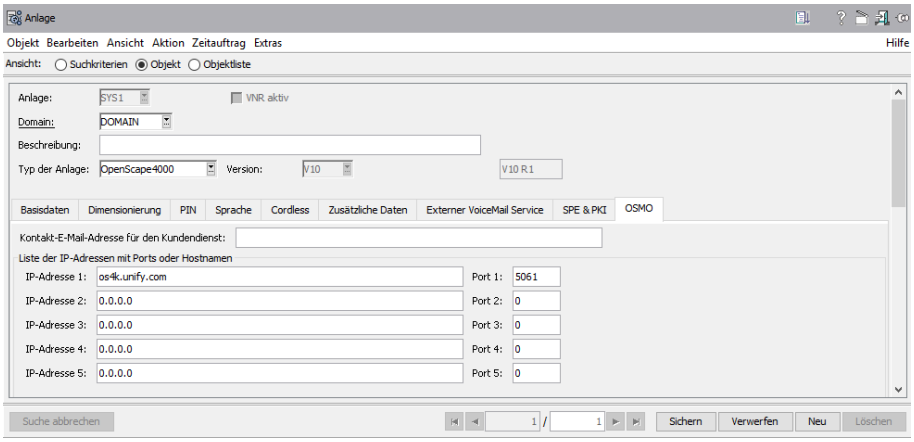


Figure 308: Konfigurieren der IP-Adresse 1 in der Konfigurationsverwaltung

16.3.1.3 OpenScape SBC konfigurieren

Die Nutzung von OpenScape SBC ist für die Unify Phone-Konfiguration obligatorisch.

Das Merkmal **Remote-Abonnent** in OpenScape SBC muss aktiviert werden. Unify Phone Clients registrieren sich über OpenScape SBC in den OpenScape 4000 Gateways, auf denen UFIP-Hilfsgeräte gehostet werden. Weitere Informationen zur OpenScape SBC-Konfiguration finden Sie im OpenScape SBC-Konfigurationshandbuch.

Befolgen Sie die folgenden Schritte, um den Clustermodus zu aktivieren:

1) Navigieren Sie zu **VoIP > Sip-Server-Einstellungen**.
2) Wählen Sie **Clustered** als Comm-Systemtyp aus.

3) Klicken Sie auf die Schaltfläche **Clusterserver** und fügen Sie alle Gateways, die UFIP-Hilfsgeräte für Unify Phone oder OSMO hosten, hinzu.

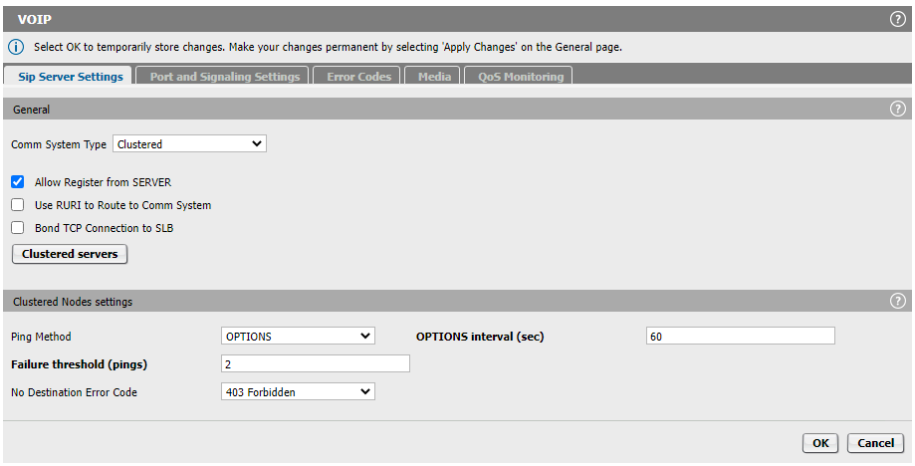


Abbildung 309: Sip-Server-Einstellungen

Jedes Gateway muss Priorität **1** und die Option und **Bleiben Sie bei CommServer** aktiviert haben, wie in der Abbildung unten angezeigt.

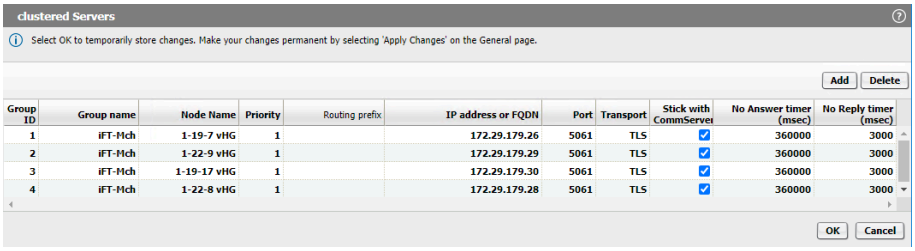


Abbildung 310: Clusterserver

4) Navigieren Sie zu **VoIP > Fehlercodes** und aktivieren Sie **404 Not Found**, wie in der Abbildung unten angezeigt.

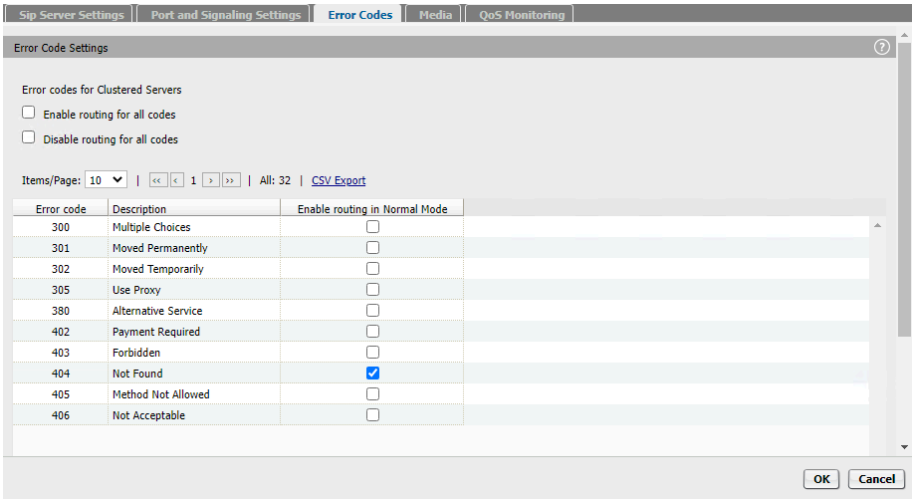


Abbildung 311: Fehlercodes

Wenn der SBC die erste SIP-Registrierung erhält, sendet er REGISTER an jedes konfigurierte Gateway, bis er eine Antwort erhält, die nicht "404 Not Found" lautet. Nur das Gateway, auf dem das Gerät konfiguriert ist,

antwortet mit 200 OK. Nach der ersten Meldung sendet der SBC weitere SIP-Meldungen nur an die GWY, in der das Gerät konfiguriert ist.

5) Navigieren Sie zu **VoIP > Medien** und fügen Sie das Medienprofil **Unify_Phone_default** zum Benutzeragenten **OpenScape Mobile Client - WebRTC NGTC** hinzu.

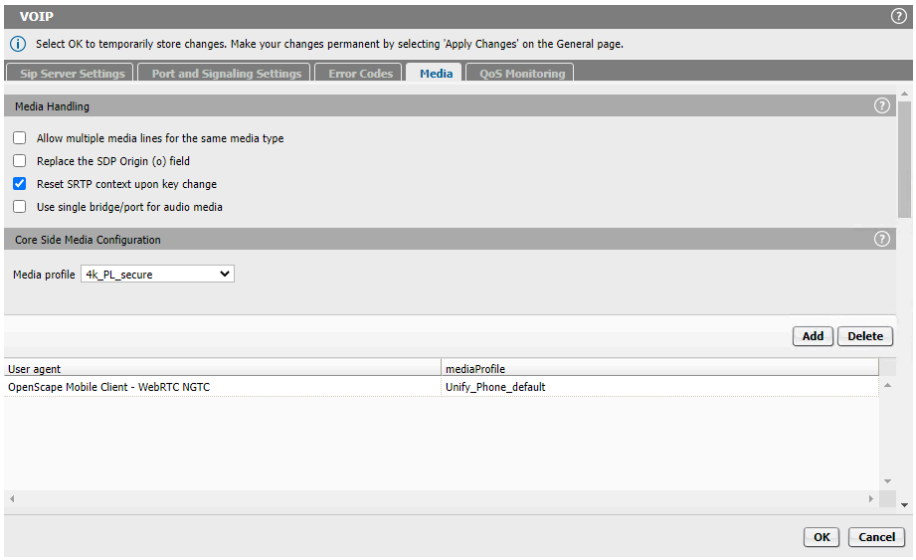


Abbildung 312: Medienprofil

6) Navigieren Sie zu **Merkmale** und aktivieren Sie die Kontrollkästchen für **Remote-Abonnenten aktivieren** und **Codec-Unterstützung für Transcodierung aktivieren**.

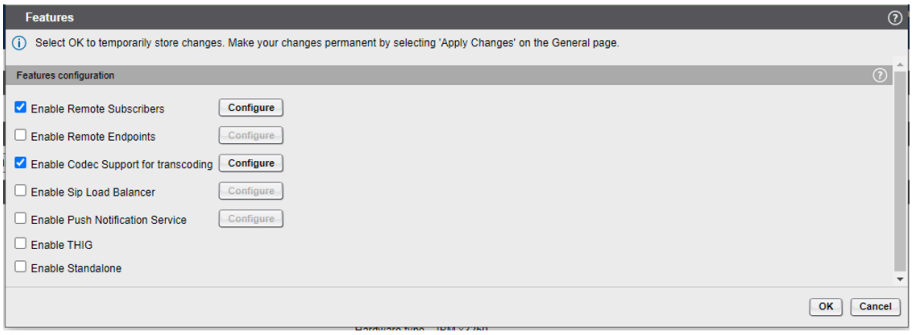


Abbildung 313: Leistungsmerkmale

Auf der Registerkarte **Remote-Abonnenten aktivieren** ist keine Eingabe erforderlich.

Unter **Codec-Unterstützung für Transcodierung aktivieren** können die folgenden Codecs aktiviert werden:

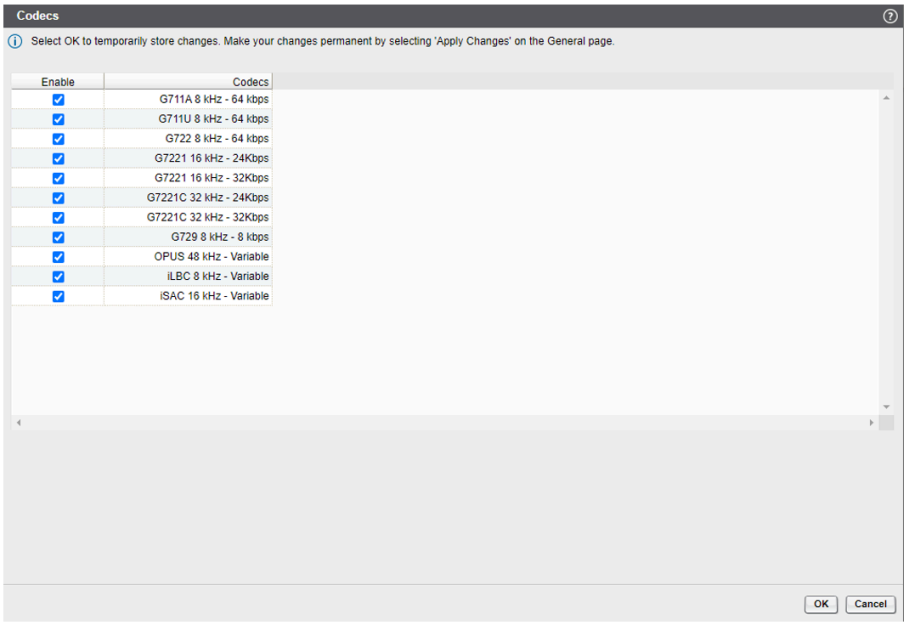


Abbildung 314: Codecs

16.3.2 Benutzerkonfiguration

16.3.2.1 Unify Video konfigurieren

Jeder Unify Phone-Benutzer muss über ein Unify Video-Konto mit **Video Pro+**-Lizenz und aktivierter Cross-Launch-Funktion verfügen. Weitere Informationen finden Sie unter Unify Phone Administration.

Führen Sie die folgenden Schritte aus, um Unify Video zu konfigurieren:

1) Melden Sie sich bei https://service.unifyoffice.com mit einem **Super-Admin-** oder **User-Admin**-Konto an.
2) Um den Benutzern Lizenzen zuzuweisen, wählen Sie unter **Benutzer > Benutzerliste** den zu konfigurierenden Benutzer aus und klicken auf **Lizenzen zuweisen**.
3) Um die Cross-Launch-Funktion zu aktivieren, wählen Sie die Benutzer unter **Mehr > Kontoeinstellungen > Cross-Launch** aus und klicken Sie auf **Cross-Launch einschalten**.

Unter **Benutzer > Benutzerliste** können Sie auch neue Konten hinzufügen, indem Sie auf **Benutzer hinzufügen** oder **Massen-Upload von Benutzern** klicken. Jeder neue Benutzer erhält eine E-Mail-Einladung an die konfigurierte E-Mail-Adresse. Diese E-Mail-Adresse wird für die Zuordnung des Unify Video-Kontos zu einem Unify Phone-Anschluss in OpenScape 4000 verwendet.

16.3.2.2 OpenScape 4000 konfigurieren

Konfigurieren der E-Mail Adresse

Ein Unify Phone-Client wird im OpenScape 4000-System als UFIP-SIP-Gerät registriert, das mit einem Tischgerät verbunden ist. Dieses Tischgerät definiert die E164-Nummer des Unify Phone-Benutzers, aber es ist nicht zwingend erforderlich, dass das Tischgerät in Betrieb ist.

Die E-Mail-Adresse des Unify Phone-Benutzers muss in OpenScape 4000 (am Tischgerät) in der Konfigurationsverwaltung eingerichtet sein. Derzeit ist diese Konfiguration nicht über AMO möglich.

Um die E-Mail-Adresse zu konfigurieren, navigieren Sie zu **Konfigurationsverwaltung > Anschluss** und fügen Sie die E-Mail-Adresse auf der Registerkarte **Basis 3** hinzu.

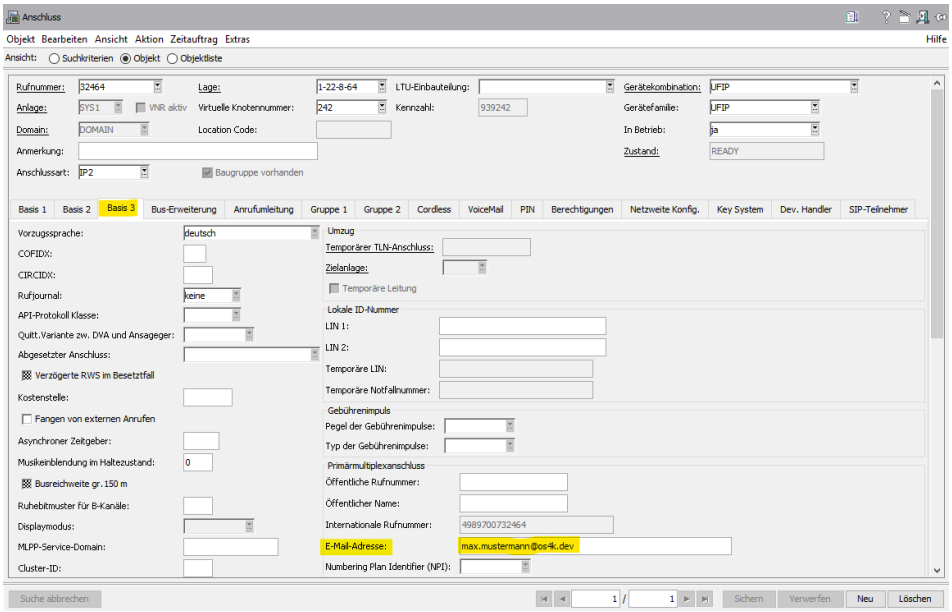


Figure 315: Hinzufügen der E-Mail-Adresse

NOTICE:

Wenn mehrere E-Mail-Adressen konfiguriert werden müssen, verwenden Sie den CSV-Import der Circuit-Massenmigration. Weitere Informationen finden Sie unter Massenmigration aus Circuit.

Konfigurieren eines Zusatzgeräts

Jeder Unify Phone-Client (z. B. OSMO- und Circuit-Clients) wird in OpenScape 4000 als UFIP-SIP-Gerät registriert. Dieses Zusatzgerät muss über den Parameter CLNTDESK mit dem Tischgerät des Benutzers verbunden sein. Außerdem muss es über den Parameter CLNTTYPE=UNIPHONE als Unify Phone-Gerät gekennzeichnet sein.

Zusatzgeräte, die mit CLNTTYPE=UNIPHONE konfiguriert sind, müssen über eine Unify Phone-Lizenz verfügen. Ohne eine solche Lizenz wird jede Registrierung über den Unify Phone-Client abgelehnt.

Das Zusatzgerät kann wie folgt konfiguriert werden:

- Befehl AMO-SBCSU:
  `ADD-SBCSU:STNO=<UFIP_STN>, OPT=OPTI, CONN=IP2, PEN=<X-Y-Z-T>, DVCFIG=UFIP, IPPASSW=..., USERID=..., SECZONE=..., CLNTDESK=<DESK_STN>, CLNTTYPE=UNIPHONE;`
- Mit OpenScape 4000 Assistant oder Manager, indem Sie zu **Konfigurationsverwaltung > Anschluss** > Registerkarte **Bus-Erweiterung** navigieren und den Abschnitt **Universal Feature Access** konfigurieren, wie in der folgenden Abbildung dargestellt:

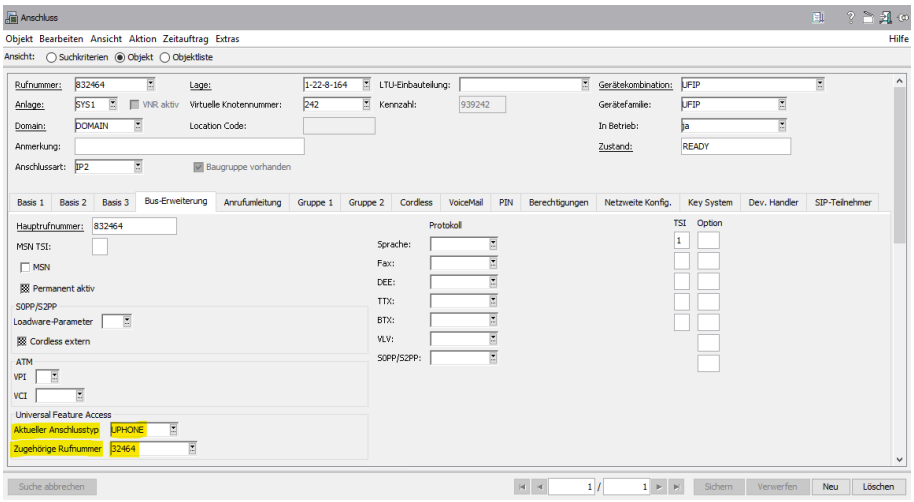


Figure 316: Bus-Erweiterung

Um die Verknüpfung zu überprüfen, verwenden Sie **DIS-SBCSU**:

- DIS-SBCSU for UFIP_STN zeigt DESK=<DESK_STN>
- DIS-SBCSU for DESK_STN zeigt CLIENT=<UFIP_STN>

oder

- Mit dem WBM des Gateways, wobei UFIP_STN unter **Konfiguration > Voice Gateway > Clients > UFIP SIP** konfiguriert wird:
  - In der Spalte **Anschlussnummer** wird <UFIP_STN> angezeigt
  - In der Spalte **ONS-Nummer** wird DESK_STN angezeigt.

Daten zwischen Unify Phone Telephony Connector und OpenScape 4000 synchronisieren

Die Konfiguration in OpenScape 4000 kann periodisch (z.B. alle 5h) mit Unify Phone Telephony Connector synchronisiert werden. Während des Synchronisierungsprozesses ruft OpenScape 4000 Änderungen von der Unify Video-Seite ab (z. B. neue Benutzer) und lädt die Konfigurationsdaten (z. B. Telefonnummer und SIP-Anmeldeinformationen) in den Unify Phone Telephony Connector hoch. Wenn Sie einige neue Unify Phone-Benutzer in OpenScape 4000 eingerichtet haben, können Sie den Synchronisationsprozess auch sofort starten.

Um die Konfiguration zu synchronisieren, navigieren Sie zu **Konfigurationsverwaltung > Unify Phone**, wählen Sie die Hüufigkeit der **Datensynchronisierung** und klicken Sie auf **Daten synchronisieren**

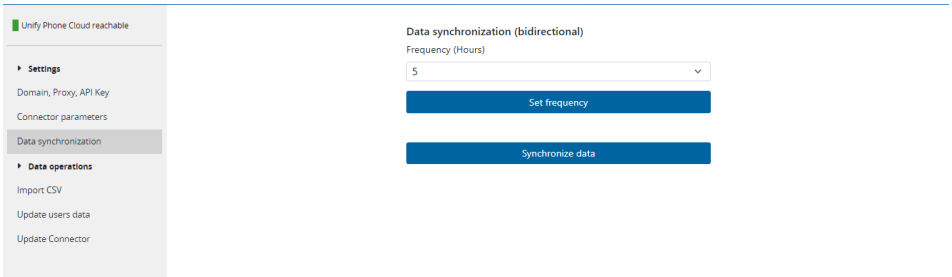


Figure 317: Datensynchronisierung

Sie können die Konfiguration unter dem Abschnitt **Benutzerdaten aktualisieren** überprüfen, wie in der folgenden Abbildung dargestellt.

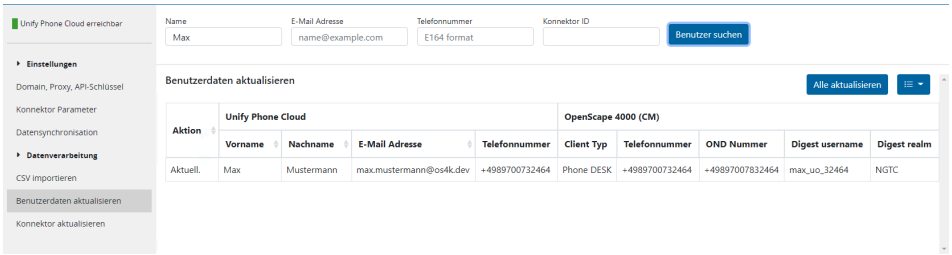


Figure 318: Benutzerdaten aktualisieren

In der Spalte **Aktion** wird der aktuelle Status der Konfiguration und der Synchronisierung angezeigt.

- **Aktuell**: Die Daten sind bereits mit Unify Phone Telephony Connector synchronisiert.
- **Update**: Die Änderungen wurden auf OpenScape 4000 vorgenommen und sind noch nicht synchronisiert. Sie können die Update-Schaltfläche drücken, um sie jetzt zu synchronisieren.
- **E-Mail nicht in OS4K konfiguriert**: Für den Unify Video-Benutzer wurde keine entsprechende E-Mail-Adresse in OpenScape 4000 konfiguriert.

  NOTICE: Diese Meldung wird auch angezeigt, wenn der Benutzer an einer anderen Telefonanlage konfiguriert ist.

- **Unify Phone ist nicht in OS4K konfiguriert**: Für den Unify Video-Benutzer wurde eine E-Mail-Adresse in OpenScape 4000 konfiguriert, aber

das Zusatzgerät ist nicht konfiguriert oder ihm ist der falsche Client-Typ zugewiesen.

16.4 Massenmigration aus dem Kreislauf

Im ersten Schritt müssen alle Circuit-Benutzer zu Unify Video hinzugefügt werden. Dies kann über die **Bulk-Upload-Benutzer** von Unify Video oder über das **Unify Migration Tool**erfolgen. Nachdem Sie die OpenScape-Lizenz mit genügend Unify Phone-Lizenzen hochgeladen haben, kann der Client-Typ aller von Circuit verwendeten Zusatzgeräte mit dem folgenden AMO-Befehl von **OTHER** auf **UNIPHONE** geändert werden:
`CHA-SBCSU:STNO=<UFIP_STN>, OPT=OPTI, CLNTTYPE=UNIPHONE;`

Dies kann auch dann geschehen, wenn der Nutzer noch Circuit verwendet. Die Registrierung eines Circuit-Clients wird nicht abgelehnt, wenn das Zusatzgerät bereits auf UNIPHONE geschaltet ist, aber die Registrierung eines Unify Phone-Clients wird abgelehnt, wenn der CLNTTYPE OTHER ist.

Es ist möglich, alle Benutzer des Circuit-Tenants in eine CSV-Datei zu exportieren. Diese CSV datei kann direkt in OpenScape 4000 importiert werden und hat das folgende format:

```
Name,Vorname,Nachname,Ort,Rolle,Status,Erstellt
 am,Erste Anmeldung,Letzte
 Anmeldung,Datennutzung,Telefonnummer,Paketname
max.mustermann@os4k.dev,Max,Mustermann,,,,,,,,4989700732464,
somewhere.else@os4k.dev,Not,Here,,,,,,,,4989700799999,
...
```

Führen Sie die folgenden Schritte aus, um den Clustermodus zu aktivieren:

1) Navigieren Sie zu **Configuration Management > Unify Phone**.
2) Klicken Sie auf **Datei auswählen** unter **CSV importieren**, wählen Sie Ihre csv-Datei aus und klicken Sie auf **Importieren**.

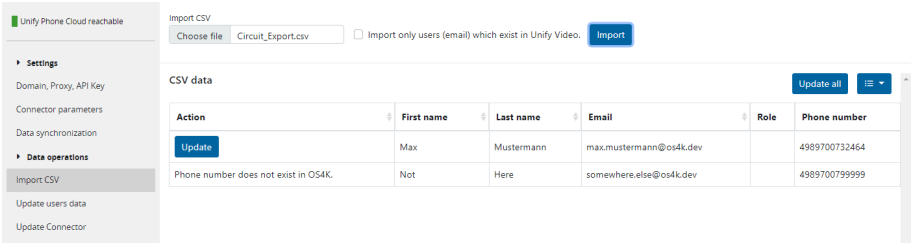


Figure 319: Import einer CSV-Datei

3) Klicken Sie auf **Alle aktualisieren** oder Selektive **Aktualisierung** , um die E-Mail-Adresse anhand der Spalte **Telefonnummer** zu konfigurieren. Wenn eine Telefonnummer (Internationale Nummer in Basic 3) nicht existiert (oder in einer anderen Telefonanlage existiert), dann enthält die entsprechende Zeile die Meldung **Telefonnummer existiert nicht in OS4K**.

NOTICE:

Diese Methode kann auch verwendet werden, wenn die E-Mail-Adressen für viele Schreibtischgeräte konfiguriert werden müssen.

---

4) Nach der Datensynchronisation mit dem Unify Phone Telephony Connector können die Clients verwendet werden.

17 H323-/H323-Annex-Konnektivität

17.1 Überblick

Wichtig: Ab OpenScape 4000 V8 wird H323-Trunking nur noch für Verbindungen zu OpenScape XPressions unterstützt.

Leistungsmerkmale

- CLIP / CLIR / COLP / COLR
- Namensanzeige
- Halten / Wiederaufnehmen / Makeln
- Anrufübergabe (blind, nicht überwacht, überwacht)
- Anrufumleitung
- Rückruf bei besetztem Teilnehmer / Rückruf bei nicht melden
- Message Waiting Anzeige
- Wege-Optimierung
- OpenScape 4000 als Survivability Media Gateway
- Signalisierungs- und Sprachverschlüsselung (TLS / SRTP)
- T.38

Verwendete Baugruppen

- Es wird die Common-Gateway-Baugruppe HG 3500 verwendet. Für Details siehe „Gateways HG 3500 und HG 3575“, Kapitel 3, „Unterstützte Gateways“.
- Das H323 Trunk-Protokoll zu OpenScape Xpressions wird auf der STMIX-Karte und dem SoftGate (vHG3500-Karte) unterstützt.

17.2 MVF-Außerband-Signalisierung

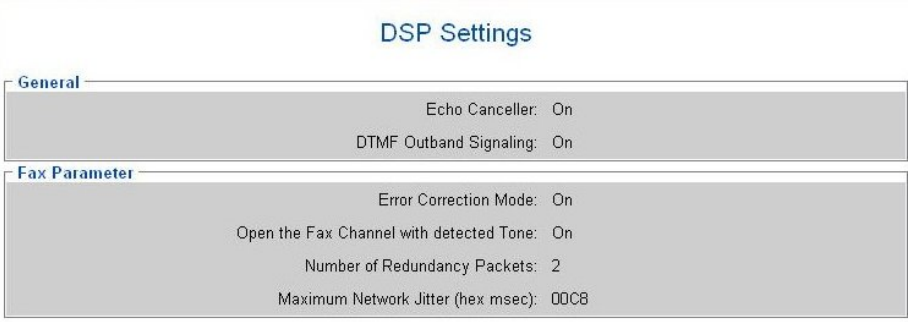
Um auf „MFV Außerband Signalisierung“ umzustellen, muss man die folgenden Schritte ausführen:

1) RFC 2833 mit AMO CGWB ausschalten:
2) `AE-CGWB:MTYP=CGW,LTU=<ltu>,EBT=<ebt>,TYP=ASC,RFCDTMF=NEIN;`

   Zur Aktivierung von H.323 Außerband Signalisierung muss auf beiden Seiten die MFV-Tonübertragung nach RFC 2833 ausgeschaltet werden. RFC 2833 ist entgegen vieler Annahmen keine Außerband Signalisierung, sondern eine Innerband Signalisierung mit einem speziellen Codec.

   Zur Deaktivierung **muss auf beiden Seiten** im AMO CGWB Zweig **ASC** der Parameter **RFCDTMF=NEIN** eingestellt werden.
3) „MFV Außerband Signalisierung“ über WBM aktivieren (Parameter **MFV-Außerband-Signalisierung**)

4) WBM: **Explorer > Payload > HW-Module**



Aktivierung von MFV-Außerband-Signalisierung

17.3 Konfigurationsbeispiel

17.3.1 Konfiguration mit Hilfe von AMOs

17.3.1.1 Trunking-Protokoll

Im AMO CGWB und AMO GKREG müssen immer die selben Protokolle eingestellt werden.

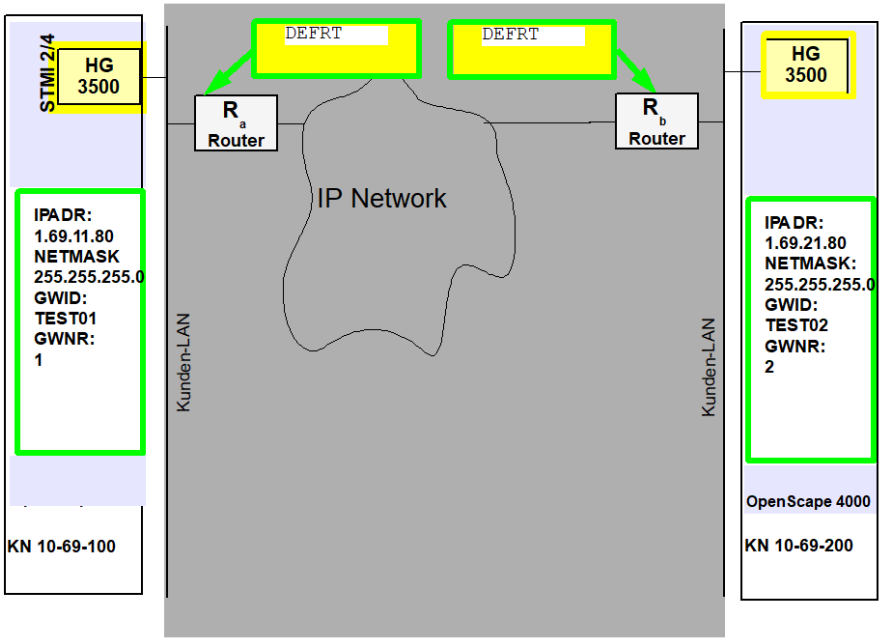
Tabelle 83: Protokolle im AMO CGWB und AMO GKREG

AMO CGWB	AMO GKREG	Protokoll
TRPRH323	H323	native H323
TPRH323A	H323ANN	H323 Annex

Wird im AMO CGWB / AMO GKREG H323 Annex eingestellt, so wird nur dann dieses Protokoll verwendet, wenn auch die Gegenseite dieses Protokoll eingestellt hat bzw. in der Lage ist dieses Protokoll zu verwenden.

17.3.1.2 Einrichten einer (v)HG 3500 als internes Gateway

Die folgende Abbildung zeigt die auf HG 3500 reduzierte Situation bei einem fiktiven Kunden in Frankfurt. Dargestellt sind der Knoten 10-69-100 (Frankfurt-Bockenheim) und der Knoten 10-69-200 (Frankfurt-Sachsenhausen). Beide Anlagen verfügen über je eine Common Gateway-Baugruppe, die als HG 3500 eingerichtet werden soll. Auf beiden Anlagen soll der LEGK laufen (zwei Mal local Gateway). Diese Konstellation ist daher relativ einfach zu erklären, weil dann die beiden Knoten quasi symmetrisch eingerichtet werden können. Im Bild sind alle benötigten Parameter eingetragen. Der Knoten 10-69-100 befindet sich im IP-Netz 1.69.11.0 /24 und der Knoten 10-69-200 liegt im IP-Netz 1.69.21.0 /24. Beide Netze erreichen sich über die Router Ra und Rb.



Einrichtebeispiel: beide Knoten sind LEGK

17.3.1.2.1 Einrichtung in Knoten 10-69-100

Im Knoten 100 beginnt man mit der Einrichtung der Baugruppe als HG 3500. Es empfielt sich, die Baugruppe erst am Ende der Konfiguration zu stecken, um sich mehrere Neustarts zu ersparen.

Schritt 0:

LEGK im Knoten 10-69-100 einrichten.

```
AENDERN-ZANDE:TYP=DATENALL,GATEKPR=JA;
```

Schritt 1:

Die Common Gateway Baugruppe Q2316-X wird als HG 3500 eingrichtet. Die Q2316-X ist die Ausgabe mit 60 B-Kanälen. Sie können die Baugruppe als reine IP-Trunking Baugruppe einrichten oder auch im Mischbetrieb mit IP-Trunking und LAN-Connectivity (WAML) und diversen anderen Leistungsmerkmalen.

Konfiguration der Baugruppe nur für IP-Trunking:

```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3550,ANZSATZ=1,

ANZEINH=3; /* 30 B-Kanäle für HG3550 Funktion (H323
 Trunking,

SIP Trunking, SIP Subscriber)
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=37,SACHNR="Q2316-
X",

FCTID=1,LWVAR="0",FCTBLK=1,BKAN3550=30,ALARMNR=0;
```

oder

IP-Trunking & WAML:

```
EINRICHTEN-BFDAT:FCTBLK=1,FUNCTION=HG3550&WAML,

BGBKAN=BKAN60&BKAN120;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3550,ANZSATZ=1,

ANZEINH=3; /* 30 B-Kanäle für HG3550 Funktion (IP Trunking,
 SIP Trunking, SIP
Subscriber)
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=WAML,ANZSATZ=1; /*
 Baugruppe wird
mit einem Satz, d.h. 10 B-Kanälen für WAML eingerichtet
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=1,EBT=37,SACHNR="Q2316-X
   ",FCTID=1,LW►
VAR="0",FCTBLK=1,BKAN3550=30,BKANWAML=10,ALARMNR=0;
```

Schritt 2:

Die Baugruppe erhält über den AMO CGWB die IP-Adresse im Kunden-LAN (LAN1), die Subnetzmaske und die Protokollvariante (SIP-Q / H323A / KEIN (Baugruppe wird nur für SIP Subscriber konfiguriert)).

Wichtig: Pro Baugruppe kann nur ein Trunking-Protokoll konfiguriert werden! Mischung mit anderen Funktionen ist uneingeschränkt möglich!

```
EINRICHTEN-CGWB:LTU=1,EBT=37,SMODE=NORMAL,IPADR=1.69.11.80,
 NET►
MASK=255.255.255.0,TPRH323A=10; /*10 B-Kanäle für H323A-
Trunking
```

oder

```
EINRICHTEN-CGWB:LTU=1,EBT=37,SMODE=NORMAL,IPADR=1.69.11.80,
 NET►
MASK=255.255.255.0,TRPRH323=10; /*10 B-Kanäle für H323A-
Trunking
```

=> Es bleiben 20 B-Kanäle für andere Funktionen

Schritt 3:

Nun wird der Default Router im Kunden LAN eigestellt:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=GLOBIF,DEFRT=1.69.11.254;
```

Schritt 4:

Die HG 3500 benötigt eine im Netz eindeutige ID. Der Parameter befindet sich im AMO-CGWB und lautet **GWID**:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=GWDATA,GWID1="TEST01";
```

GWID1 und **GWID2** bilden zusammen einen zusammenhängenden Wert aus 128 Zeichen. Groß- Kleinschreibung beachten!

Schritt 5:

Die HG 3500 Baugruppen werden unter einer Gateway-Nummer verwaltet (**GWNR**). Diese muss eindeutig sein.

```
AENDERN-CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=LEGKDATA,GWNR=1;
```

Schritt 6:

Wichtig: Es sind mehrere Baugruppen in einem Bündel erlaubt!

Dieser Schritt umfasst nun mehrere Einrichtekommandos. Es wird das Bündel und der Satz eingerichtet, über den die B-Kanäle zwischen Gateway und OpenScape 4000 geschaltet werden.

Zunächst braucht man ein Bündel:

```
EINRICHTEN-BUEND:BUNUM=50,NAME="IP TRUNK GWID 1   ",
 ANZ=30,ANZFANG=0,PRIO►
NUM=2,TDDRFLAG=ON, GDTRRLG=0, ACDPMGRP=0, ZEICHUM=NEUTRAL;
```

Dann wird ein digitaler Leistungssatz (AMO TDCSU) benötigt. Der Gerätetyp lautet **HG3550IP** (bei H323-/H323A- und native SIP-SIP-Q-Trunking). Möchte man DMC erlauben, so wird **DMCERL=JA** gesetzt. Dies kann aber nur dann gemacht werden, wenn die Partneranlage DMC unterstützt.

```
EINRICHTEN-TDCSU:ART=NEU,LAGE=1-01-037-0,COTNR=36,

COPNR=32,WABE=0,VBZ=0, COS=2,LCOSS=1,LCOSD=1,

SATZNR="SATZ VON GW2",PROTVAR="ECMAV2",SEGMENT=8,
 ISDNIP=00,ISDN►
NP=0,TRACOUNT=31,SATCOUNT=VIELE,

KNNR=1-69-499,ALARMNR=12,
 COTX=36,CCHDL=ASEITE,CLASSMRK=EC&G711,

TCCID="IP TR",BUNR=50,SUCHART=AB,INBETR=J,GER=HG3550IP,

BKANAL=1&&30,BKVER=N,BKGR=1,LWPAR=0,DMCERL=JA;
```

Wenn für die H323-/H323A-Trunkingstrecke DMC aktiviert wurde, sollte auch Voice Activity Detection aktiviert werden. Andernfalls benötigt man auf der Masterverbindung die gleiche Bandbreite wie auf der Slaveverbindung!

```
AENDERN-CGWB:MTYP=CGW,LTU=<ltu>,EBT=<ebt>,TYP=ASC,

PRIO=PRIO1,VAD=JA;
```

Andernfalls benötigt man auf der Masterverbindung die gleiche Bandbreite wie auf der Slaveverbindung.

Wichtig: Es empfiehlt sich ein Rücksetzen der Baugruppe:
`RESET-BSSU:ADRART=LAGE,LTG=1,LTU=1,EBT=37;`

Wichtig: Über das Kommando AENDERN-FUNSU kann das komplette Neuladen der STMI Baugruppe verhindert

werden. Ein Neuladen ist nur bei Loadware-Änderungen erforderlich. AENDERN-FUNSU:PIT=FLASH,SACHNR="Q2316-X ",FCTID=2, ACTION=RESET;

Schritt 7:

Der LEGK muss nun noch im AMO GKREG über die Existenz des HG 3500 Gateways informiert werden. Die **GWNR** hat dem Eintrag aus dem AMO CGWB zu entsprechen. Im Falle eines local Gateways lädt sich der AMO GKREG automatisch die IP-Adresse (**IPADR**) aus dem AMO CGWB. Darüber hinaus sind die Attribute **INTGW** (internes -local- Gateway) und **HG3550V2** (Versionskennung) zu setzen. Der Parameter **REGGW** ist nicht nötig, da sich das Gateway nicht an einem anderen Gateway registrieren muss.
EINRICHTEN-GKREG:**GWNR=1**,GWATTR=**INTGW**&HG3550V2&**H323ANN oder H323**,NUM=0,WABE=0,LBER=1;

Hat man ein local Gateway eingerichtet, wird bei **AB-GKREG;** immer REGISTRIERT=NEIN angezeigt.

Damit ist die HG 3500-Baugruppe im Knoten 10-60-100 funktionsfähig und kommuniziert mit dem LEGK. Es fehlt aber noch das Gateway im Partnerknoten.

17.3.1.2.2 Einrichtung im Knoten 10-69-200

Im Knoten 10-69-200 soll ebenfalls ein LEGK laufen. Die Einrichtung von 10-69-200 ist spiegelbildlich zur Einrichtung im Knoten 10-69-100. Daher werden nur die entsprechenden AMO-Kommandos zu den oben genannten Schritten aufgeführt.

Schritt 0:

AENDERN-ZANDE:TYP=DATENALL,**GATEKPR=JA**;

Schritt 1:

```
EINRICHTEN-
BFDAT:FCTBLK=1,FUNCTION=HG3550,BGBKAN=BKAN60&BKAN120;
AENDERN-
BFDAT:CONFIG=WEITER,FCTBLK=1,FUNCTION=HG3550,ANZSATZ=1,

ANZEINH=3; /* 30 B-Kanäle für HG3550 Funktion (IP Trunking,
 SIP Trunking, SIP
Subscriber)
AENDERN-BFDAT:CONFIG=OK,FCTBLK=1,ANTW=JA; /* Beenden der
 Konfiguration
EINRICHTEN-BCSU:TYP=IPGW,LTG=1,LTU=2,EBT=49,SACHNR="Q2316-X
   ",

FCTID=1,LWVAR="0",FCTBLK=1,BKAN3550=30,ALARMNR=0;
```

Schritt 2:

```
EINR-
CGWB:LTU=2,EBT=49,SMODE=NORMAL,IPADR=1.69.21.80,NETMASK=255.255.255.0,
TPRH323A=10;
```

oder

```
EINR-
CGWB:LTU=2,EBT=49,SMODE=NORMAL,IPADR=1.69.21.80,NETMASK=255.255.255.0,
```

```
PRH323=10;
```

Schritt 3:

```
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=49,TYP=GLOBIF,DEFRT=1.69.21.254;
```

Schritt 4:

```
AENDERN-
CGWB:MTYP=CGW,LTU=2,EBT=49,TYP=GWDATA,GWID1=âTEST02â;
```

Schritt 5:

```
AENDERN-CGWB:MTYP=CGW,LTU=2,EBT=49,TYP=LEGKDATA,GWNR=2;
```

Schritt 6:

```
EINRICHTEN-BUEND:BUNUM=50,NAME="IP TRUNK GWID 2 ",ANZ=30;
EINRICHTEN-TDCSU:ART=NEU,LAGE=1-02-049-0,COTNR=36,

COPNR=32,WABE=0,VBZ=0, COS=2,LCOSS=1,LCOSD=1,

SATZNR="SATZ VON GW2",PROTVAR="ECMAV2",SEGMENT=8,ISDNIP=00,

ISDNNP=0,TRACOUNT=31,SATCOUNT=VIELE,KNNR=1-69-499,

ALARMNR=12,COTX=36,CCHDL=ASEITE,CLASSMRK=EC&G711,TCCID="IP
 TR",

BUNR=50,SUCHART=AB,INBETR=J,GER=HG3550IP,BKANAL=1&&30,
 BKVER=N,BKGR=1,LW►
PAR=0(=Master),DMCERL=JA;
AENDERN-
CGWB:MTYP=CGW,LTU=<ltu>,EBT=<ebt>,TYP=ASC,PRIO=PRIO1,

VAD=JA;
```

Schritt 7:

Der GKREG enthält die Einrichtung für beide HG 3500 Baugruppen. **GWNR=2** ist hier nun im Knoten 10-69-200 das local Gateway mit den Attributen **INTGW**, **HG3550V2** und **H323ANN oder H323**, während das **GWNR=1** (das Partnergateway im Knoten 10-69-100) in dieser Anlage die Attribute **EXTGW**, **HG3550V2** und **H323ANN oder H323** erhält. Der Parameter **REGGW** ist nicht nötig, da sich das Gateway nicht an einem anderen Gateway registrieren muss.

```
EINRICHTEN-GKREG:GWNR=1,GWATTR=EXTGW&HG3550V2&H323ANN oder
 H323,GWIPA►
DR=1.69.11.80,WAPLNUM=0,WABE=0,LBER=1;
EINRICHTEN-GKREG:GWNR=2,GWATTR=INTGW&HG3550V2&H323ANN oder
H323,WAPLNUM=0,WABE=0,LBER=1;
```

17.3.1.2.3 Ergänzung im Knoten 10-69-100

Im Knoten 10-69-100 muss für den LEGK noch die HG 3500 im Knoten 10-69-200 nachgetragen werden (AMO GKREG). Diese HG 3500 (**GWNR=2**) ist für den Knoten 10-69-100 ein externes Gateway (Attribute

EXTGW&HG3550V2&H323ANN oder H323), dass sich im Knoten 10-69-100 nicht registriert.

```
EINRICHTEN-GKREG:GWNR=2,GWATTR=EXTGW&HG3550V2&H323ANN oder
H323,GWIPADR=1.69.21.80,WAPLNUM=0,WABE=0,LBER=1;
```

17.3.1.2.4 Ruf von Knoten 10-69-100 zu Knoten 10-69-200

Exemplarisch soll nun das LCR für den Knoten 10-69-100 so eingerichtet werden, das ein Teilnehmer dieses Knotens über eine offene Nummerierung (**UNKNOWN**) einen Teilnehmer des Knoten 10-69-200 über den IP-Trunk erreicht. Verdeckte Nummerierung oder ISDN-Rufnummernpläne werden ebenso unterstützt und vergleichbar eingerichtet.

Der Teilnehmer des Knotens 10-69-100 erreicht den Knoten 10-69-200 über die Querkennziffer 902.

```
EINRICHTEN-WABE:RNR=902,KZP=QUER;
```

LRTG 520 soll zu Knoten 10-69-200 führen und das Bündel 50 (s.o.) benutzen:

```
EINRICHTEN-RICHT:ART=LRTGNEU,LRTG=520,LDIENST=ALLE,

NAME="IP ZU KN 69 200 ", BUNUM=50,ZKNNR=1-69-499;
```

Eine einfache Wahlregel:

```
EINRICHTEN-LODR:LWR=520,LWREL=ECHOFELD,FELD=2;

EINRICHTEN-LODR:LWR=520,LWREL=ENDE;

EINRICHTEN-LODR:LWR=520,INFO="QUER ZU GW2";
```

In der LRTG 520 trägt man nun unter **GW1=2-0** ein. Die **2** verweist auf den Parameter **GWNR** im AMO GKREG (siehe Abschnitt 3.1.2.3, „Ergänzung im Knoten 10-69-100“). Im AMO GKREG des Knotens 10-69-100 ist die HG 3500 mit **GWNR=2** die IP-Adresse 1.69.21.80. Die **0** steht für die Sektorpfadnummer. Sektorpfad 0 bedeutet, dass für diesen Weg unbegrenzt Bandbreite zur Verfügung steht. Sollte das Zielgateway nicht erreichbar sein, kann man über die Parameter **GW2** bis **GW5** ein Alternativrouting konfigurieren.

```
EINRICHTEN-
LDAT:LRTG=520,LDIENST=ALLE,LWERT=1,BUNUM=50,LWR=520,

LBER=1, GW1=2-0;
```

Wichtig: Im Gegensatz zu S0-/S2-Verbindungen (Punkt zu Punkt) ist eine IP-Verbindung eine Punkt- zu Mehrpunkt-Verbindung, und somit wird im AMO LDAT immer die gleiche Bündelnummer zu unterschiedlichen Zielgateways (**GW1-GW5**) verwendet!

Die Querkennziffer wird in den AMO LDPLN eingetragen. Die Rufnummer wird in den Standardwählplan mit **WAPLNUM=0** eingetragen. Anstelle von LRTG kann auch ein Profilindex verwendet werden (AMO LPROF):

```
EINRICHTEN-LDPLN:LCRCONF=LCRMUST,WAPLNUM=0,LWM="902"-"X",

LRTG=520,LBER=1;
```

Möchte man den Fall einrichten, dass man vom Knoten 10-69-200 den Knoten 10-69-100 erreicht, so ist diese Konfiguration entsprechend durchzuführen. Man verweist dann im AMO-LDAT auf die **GWNR=1**.

17.3.1.3 Backup & Restore der WBM-Konfigurationsdaten

Alle Konfigurationsdaten, die über das WBM der Baugruppe eingerichtet werden, müssen über einen Backup-Server gesichert werden. Andernfalls würden nach einem Baugruppentausch, einem Reset der Baugruppe oder einem Loadware-Upgrade alle Konfigurationsdaten verloren sein und die H323-/H323A-Trunking-Verbindung könnte nicht automatisch wieder hergestellt werden. Dies geschieht über den OpenScape 4000 Assistant > Backup & Restore.

Hierfür ist es wichtig sicherzustellen, dass der Backup-Server immer erreichbar ist. Falls der Backup-Server nicht erreichbar ist, können die Konfigurationsdaten auch im Flash der Baugruppe gesichert werden und von dort geladen werden.

OpenScape 4000 Assistant > Backup & Restore

Verbindung zum OpenScape 4000 Assistant und Backup-Server konfigurieren:

```
AENDERN-CGWB:MTYP=CGW,LTU=1,EBT=37,TYP=MGNTDATA,

MGNTIP=<ip_adresse_assistant>,MGNTPN=<port_nr_assistant>,

BUSIP=<ip_adresse_backup_server>,BUSPN=<port_nr_backup_server>};
```

Wichtig: Hinweis: Nach einem Restart der Baugruppe werden die Werte für **MGNTPN** und **BUSPN** nicht wiederhergestellt. Diese müssen neu konfiguriert werden.

Lokaler Flashspeicher

Wichtig: Es wird empfohlen den Flash ebenfalls als Backup-Medium einzurichten. Wenn der Backup-Server nicht erreichbar sein sollte, so wird auf diesen lokalen Speicher zurückgegriffen.

WBM > Wartung > Aktionen > Automatische Aktionen > Konfigurationsdateien im lokalen Flash speichern

Für mehr Informationen siehe „Gateways HG 3500 und HG 3575“, Kapitel 6, „Konfigurationsdaten im lokalen Flash speichern (local Backup & Restore)“.

Wichtig: Wenn der Restore notwendig ist (z.B. nach einer Hochrüstung der Loadware) und der Backup-Server während der Hochlaufphase nicht erreichbar ist, wird die Baugruppe mit Defaultkonfiguration geladen bzw. in Betrieb genommen. Sollte danach der HBR-Server erreichbar sein, wird der Restore nachträglich gemacht und ein Reboot mit der neuen Konfiguration angestoßen! Ein zusätzlicher Reboot wird ebenfalls während der Hochlaufphase angestoßen, wenn betriebsnotwendige Konfigurationen/Daten durch den Restore zurückgespielt werden (z.B. SPE-Zertifikate).

Wichtig: Um Probleme bei Hochrüstungen/Loadware-Tausch zu vermeiden, sollte nach dem Austausch einer Baugruppe

(Hardware-Tausch) unbedingt ein Backup angestossen werden, da der Backup auch mit der MAC-Adresse verknüpft ist.

17.3.1.4 Abfragen des Linkstatus

Der Linkstatus der LAN-Schnittstelle (Linksignal Ethernet, LAN-Geschwindigkeit und LAN-Schnittstelle) kann mittels AMO SDSU auf den einzelnen Ebenen abgefragt werden, und zwar über die üblichen Kommandos (**PERI1**, **PERI2,** and **PERI3**):

```
ABFRAGEN-SDSU:TYP=LAGE,EBENE=PERI1,LTG=1,LTU=<ltu nr>,

EBT=<ebt nr>;
```

17.3.1.5 Vorgehen bei Erweiterung um weitere HG 3500 Gateways im Netz

Weitere LEGKs können analog zu Knoten 10-69-100 konfiguriert werden. Dann sind AMO BFDAT, AMO BCSU, AMO CGWB, AMO GKREG und AMO LDAT in einem Knoten.

Wichtig: Wichtig ist, der GKREG muss alle im Netz befindlichen (v)HG 3500 Baugruppen kennen.

17.3.1.6 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/Description
BCSU	TYP=IPGW	d	CGW einrichten
	TYPE=IPGW	e	Configure CGW
	BKAN3550	d	Anzahl der B-Kanäle für IP-Trunking
	BCHAN3550	e	Number of b channels for IP trunking
BFDAT	FUNCTION=HG3550	d	CGW mit IP-Trunking
	FUNCTION=HG3550	e	CGW with IP trunking
	BGBKAN	d	Maximale Anzahl der verfügbaren B-Kanäle der Baugruppe (entweder 60 oder 120)
	BRDBCHL	e	Maximum number of available b channels (60 or 120)
	ANZSATZ	d	Anzahl der Sätze für IP-trunking
	LINECNT	e	Number of lines for IP trunking

AMO	Parameter	Sprache/ Language	Beschreibung/Description
	ANZEINH	d	Anzahl der vordefinierten Blöcke mit ausgewählter Funktion pro Satz.
	UNITS	e	Defines the number of predefined blocks with the selected function per line.
CGWB	DEFRT	d	IP-Adresse des Default Routers
	DEFRT	e	IP address of the default router
	GWID1	d	Gateway ID
	GWID1	e	Gateway ID
	VAD	d	Voice Activity Detection
	VAD	e	Voice Activity Detection
GKREG	GWATTR	d	Gateway Attribut
	GWATTR	e	Gateway attribute
	GWNR	d	Gateway ID (muss dem Eintrag im AMO CGWB entsprechen)
	GWNO	e	Gateway ID (must correspond to the vaule in AMO CGWB)
TDCSU	DMCERL=NEIN	d	DMC wird verhindert
	DMCALLWD=NO	e	DMC not allowed
ZANDE	GATEKPR=JA	d	PBX mit Gatekeeper
	GATEKPR=YES	e	PBX with gatekeeper

17.3.2 Konfiguration mit Hilfe des OpenScape 4000 Assistant

17.3.2.1 Gateway HG 3500 konfigurieren

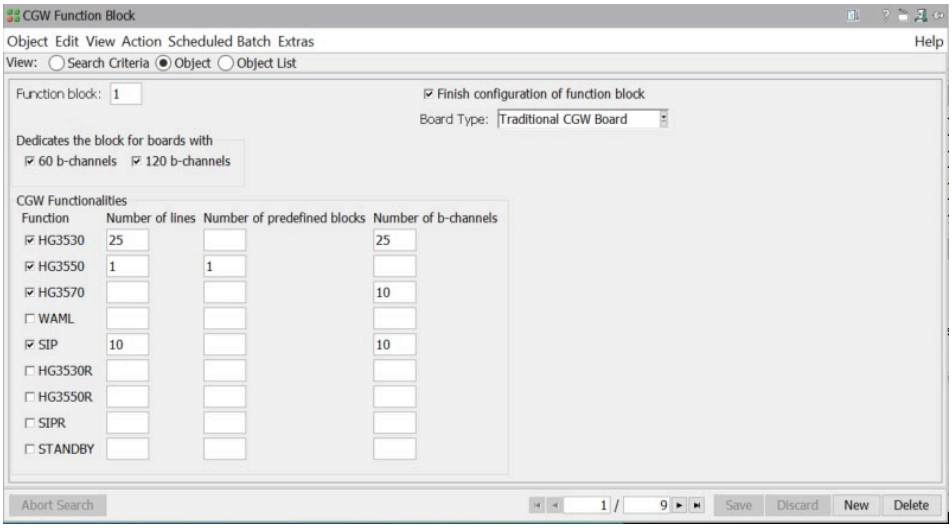
Gehen Sie zum Konfigurieren einer CGW-Baugruppe folgendermaßen vor:

- Schritt 1: Funktionsblock erzeugen
- Schritt 2: Verfügbare Einbauteilung (EBT) suchen
- Schritt 3: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen
- Schritt 4: Neue Baugruppe hinzufügen
- Schritt 5: Maske ausfüllen
- Schritt 6: Dialog STMI2-IGW-Baugruppendaten öffnen und Pflichtfelder ausfüllen

Schritt 1: Funktionsblock erzeugen

Starten Sie **Configuration Management > Anlagendaten > Baugruppe > CGW-Funktionsblock**

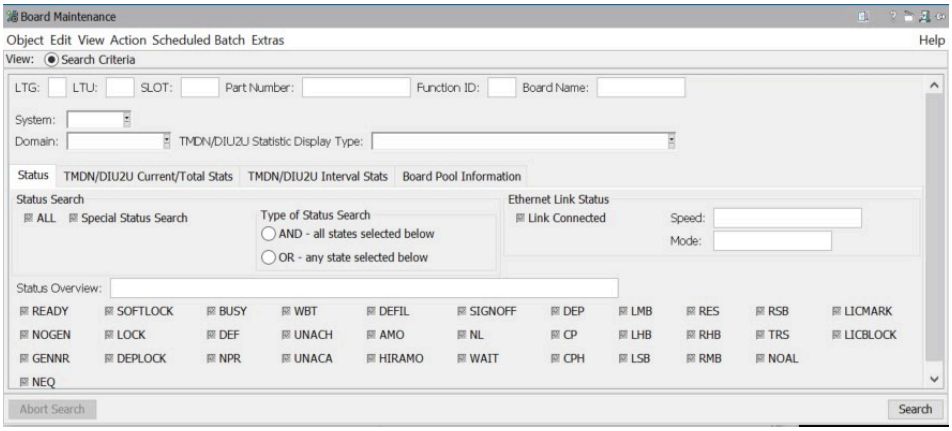
Suchen Sie nach einem freien Funktionsblock mit Hilfe der Schaltfläche **Suchen**. Um einen neuen Funktionsblock zu erzeugen, wählen Sie nun die Schaltfläche **Neu**. Geben Sie die erforderlichen Daten ein und speichern Sie diese mit der Schaltfläche **Sichern**.



Schritt 2: Verfügbare Einbauteilung (EBT) suchen

Vor der Eingabe von LTU- und EBT-Nummer sollten Sie erst prüfen, ob die gewünschte EBT auch verfügbar ist. Dafür bitte **CM > Anlagendaten > Wartung > BG-Wartung** aufrufen.

Nach Abschluss der Suche in der Ansicht Objektliste sind in der Spalte **Zustand Übersicht** freie LTUs und Einbauteilungen mit **NOGEN/NPR/UNACH** gekennzeichnet.



Schritt 3: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 4: Neue Baugruppe hinzufügen

Um die neue Baugruppe hinzuzufügen, klicken Sie auf die Schaltfläche **Neu**.

Schritt 5: Maske ausfüllen

- **Sachnummer**: Q2316-X oder Q2316-X10 oder Q2324-X500 oder Q2324-X510
- **Funktions-ID**: ist immer 1
- **Kategorie**: IPGW
- **BG-Name**: STMI2 oder STMI4
- **CGW-Funktionsblock**: geben Sie den zuvor erzeugten Funktionsblock für Trunking ein (siehe Schritt 1: Funktionsblock erzeugen)
- **LTU** und **EBT**: Wählen Sie eine verfügbare Einbauteilung (siehe Schritt 2: Verfügbare Einbauteilung (EBT) suchen)

Schritt 6: Dialog STMI2-IGW-Baugruppendaten öffnen und Pflichtfelder ausfüllen

IP-Adresse des Kunden-LAN und **Subnetzmaske**.

Amtsprotokoll: Anzahl der B-Kanäle pro Protokoll (z.B. **H323/H323-Annex**: 50).

Wichtig: Pro Baugruppe wird nur ein Amtsprotokoll unterstützt! Eine Kombination von mehreren Amtsprotokollen auf einer Baugruppe ist nicht möglich!

Nach Eingabe der Daten in die entsprechenden Felder bitte die Schaltfläche **Sichern** anklicken.

Die Baugruppe ist nun hinzugefügt und wird unter **Baugruppendialog** und **BG-Wartung** angezeigt.

17.3.2.2 IPGW löschen

Um eine IPGW-Baugruppe zu löschen, gehen Sie bitte folgendermaßen vor:

- Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen
- Schritt 2: Nach IPGW suchen
- Schritt 3: IPGW auswählen und löschen

Schritt 1: Menü Baugruppenkonfiguration in OpenScape 4000 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 2: Nach IPGW suchen

Search Criteria > Kategorie: IPGW

Schritt 3: IPGW auswählen und löschen

Aus der Trefferliste zu löschendes Gateway aussuchen und Schaltfläche **Löschen** wählen. Nachdem die Schaltfläche **Löschen** betätigt wurde, erscheint eine Meldung, die die Entfernung der Baugruppe aus der Anlage bestätigt.

17.3.2.3 IPGW-Baugruppendaten ändern

Um die Daten einer IPGW-Baugruppe zu ändern, gehen Sie bitte folgendermaßen vor:

Schritt 1: Menü Baugruppenkonfiguration in OpenScape 400 Assistant öffnen

CM > Anlagendaten > Baugruppe > Baugruppe

Schritt 2: IPGW auswählen

IPGW in der Liste „Kategorie“ wählen und die Schaltfläche „Suchen“ anklicken.

Schritt 3: Gewünschte Änderungen durchführen

Gewünschte Änderungen (z.B. IP-Adresse) im Baugruppendialog durchführen und durch Anklicken der Schaltfläche Speichern sichern.

Nachdem die Änderungen gespeichert wurden, erscheint eine entsprechende Bestätigungsmeldung.

Schritt 4: Überprüfung der Änderungen

Führen Sie eine erneute Baugruppensuche durch, um zu überprüfen, ob die neuen Daten angenommen wurden.

18 Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))

18.1 Leistungsmerkmalbeschreibung

Das Leistungsmerkmal "Signaling and Payload Encryption" (Signalisierungs- und Sprachverschlüsselung) umfasst die Verschlüsselung der Sprachdaten und der Signalisierungsdaten zwischen OpenScape 4000-Systemen bzw. diesen Systemen und damit verbundenen Endpunkten. Darüber hinaus werden Anrufe in Netzwerken mit HiPath 3000 ab V7 und OpenScape Voice ab V3.1 R2 verschlüsselt übertragen.

Für die Verwendung der Signalisierungs- und Sprachverschlüsselung wird eine PKI (Public Key Infrastructure) benötigt. Weitere Informationen finden Sie in Abschnitt 1.3.1, „PKI (Public Key Infrastructure)“.

Wichtig: T38 Fax-Streams werden für SPE nicht unterstützt.

18.1.1 Verschlüsselte Signalisierungs- und Payload-Verbindungen

Alle über ein IP-Netzwerk übertragenen Signalisierungs- und Payload-Streams können aus Sicherheitsgründen verschlüsselt werden.

Tabelle 84: Signalisierungs- und Sprachverschlüsselung (IP-Umgebung)

OpenScape 4000	STMI-Baugruppe	OpenScape 4000 SoftGate/vHG 3500/ STMIX
Native SIP-Trunk	TLS	TLS + SDES
SIP-Q Trunk	TLS + MIKEY	TLS + MIKEY oder SDES
HFA-Teilnehmer	TLS + MIKEY	TLS + MIKEY
SIP-Teilnehmer	TLS	TLS + SDES

Anmerkung: SIP-Geräte werden für SPE (TLS und SRTP) auf STMIX und SoftGate unterstützt. Bei Geräten, die MTLS nicht unterstützen (z. B. Mediatrix) ist jedoch keine MFS-Funktionalität mit SIPQ-Trunks jedoch nicht möglich, und es wird eine dedizierte SIP-Teilnehmer-Baugruppe empfohlen. Das Problem besteht darin, dass die Aktivierung von SIPQ zur Erzwingung von MTLS führt und SIP-Endgeräte, die TLS verwenden, daher nicht funktionieren.

18.1.2 Szenarien - Überblick

Signalisierungs- und Sprachverschlüsselung wird bei folgenden Szenarien unterstützt:

- IP-Trunking (siehe Abschnitt 3.3.2, „SPE für IP-Trunking“)
- SIP-Teilnehmer (siehe Abschnitt 3.4.2, „SPE bei IP-Endgeräten“
- HFA-Teilnehmer (siehe Abschnitt 3.4.2, „SPE bei IP-Endgeräten“)
- IPDA (siehe Abschnitt 3.5, „Aktivieren/Deaktivieren von SPE bei Access Points“)
- OpenScape 4000 SoftGate (siehe Abschnitt 3.6, „Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate“)
- Analog- und TDM-Terminals (siehe Abschnitt 3.4.1, „SPE bei analogen/TDM-Endpunkten“)
- Analog- und TDM-Trunking-Verbindungen (siehe Abschnitt 3.3.1, „SPE bei analogen / TDM Trunks“)

18.1.3 Lösungskonzepte

18.1.3.1 PKI (Public Key Infrastructure)

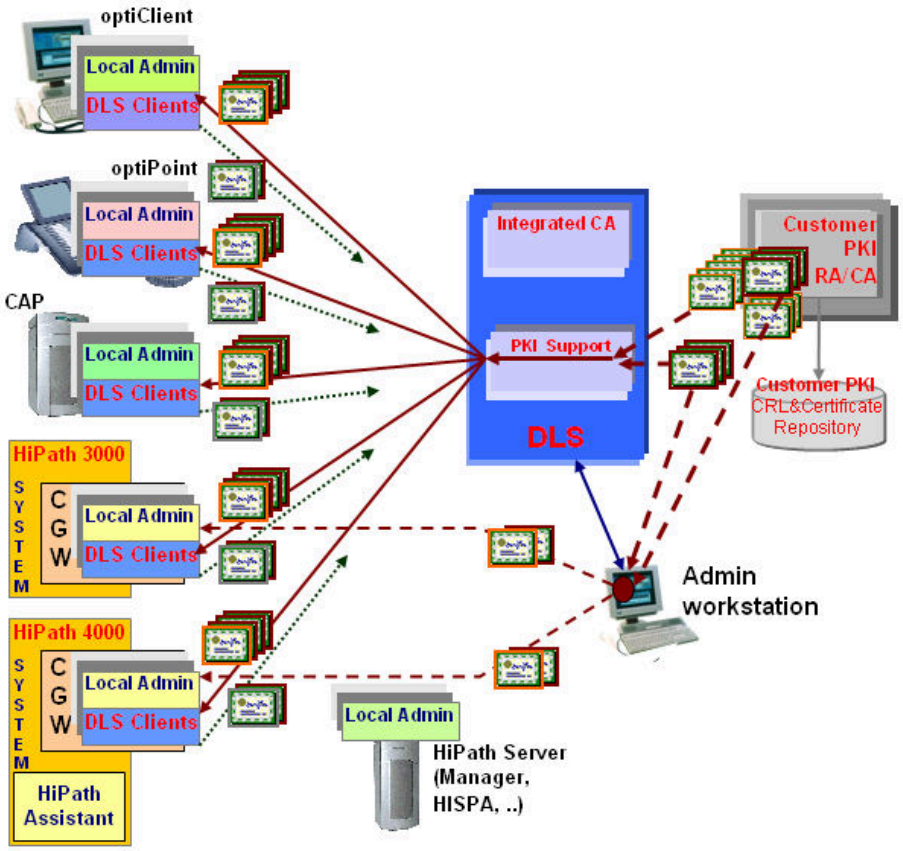


Abbildung 320: Public Key Infrastructure (PKI) am Beispiel von Common Gateways

Zur Verwendung des Leistungsmerkmals „Signalisierungs- und Sprachverschlüsselung“ wird eine PKI (Public Key Infrastruktur) benötigt. Sie können entweder eine vorhandene Kunden-PKI nutzen oder eine neue PKI mit dem Deployment Service DLS (DLS V3 und V7 R1.11.2) einrichten.

Die Verteilung der benötigten Zertifikate an alle OpenScape 4000-Gateways und -Teilnehmer erfolgt zentral über DLS.

Die für OpenScape 4000 in DLS enthaltene PKI bietet Folgendes:

- Einfache PKI-Lösung für Kunden, die über keine PKI verfügen (zur Erstellung von Zertifikaten)
- Unterstützung der Integration einer vorhandenen PKI (Zertifikat-Bereitstellung für Kunden-PKI)
- Automatische Verteilung von Zertifikaten

Kunde mit PKI

Hat der Kunde bereits eine PKI, muss er Folgendes beachten:

- Das vorhandene Zertifikat muss zum Verschlüsseln und Signieren zugelassen sein.
- Das bestehende Zertifikat ist ein RSA- oder ECDSA-Zertifikat.
- Für RSA-Zertifikate muss die Länge des privaten Schlüssels mindestens 512 Bits betragen.
- Für RSA werden die Zertifikatschlüssel-Längen von bis zu 4096 Bits unterstützt. Für STMI2/4 beträgt die maximale Schlüssellänge 2048 Bits.
- Das vorhandene Zertifikat hat das Format PEM bzw. PKCS #12.

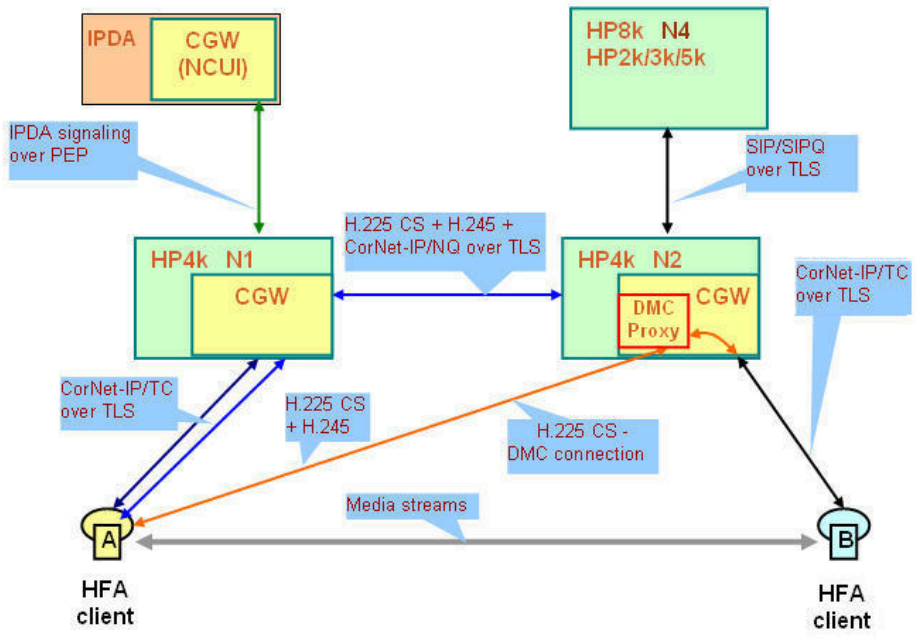
Kunde ohne PKI

Ist beim Kunden noch keine PKI vorhanden, können die benötigten Zertifikate mit DLS erstellt werden. Die **Automatische SPE-Konfigurationsfunktion** im **Administrationsmenü** wird dafür verwendet.

Detailinformationen zu DLS

Weitere Informationen zum Importieren und Verteilen von Zertifikaten finden Sie in Kapitel 7, “Verteilung von Zertifikaten mit dem Bereitstellungsdienst (DLS)”.

18.1.3.2 Signalisierungsverschlüsselung



Signalisierungsverschlüsselung

Das PEP (Proprietary Encryption Protocol) basiert auf dem Master Encyrption Key (MEK). PEP dient zum Schutz der Signalisierung für Verbindungen zwischen einem Hostsystem und den Access Points (IPDA und OpenScape 4000 SoftGate).

Für alle anderen Signalisierungsverbindungen wird das TLS (Transport Layer Security)-Protokoll verwendet (z. B. HFA/SIP-Telefone, IP-Trunking (H.323/ SIP)).

Bei VoIP-Signalisierungspfaden in einem HiPath 4000-/OpenScape 4000-Netzwerk oder zu Partnersystemen (wie OpenScape Voice) werden die einzelnen Verbindungen individuell und unabhängig voneinander verschlüsselt. Hierfür werden TLS/SSL-Verschlüsselungen (SIP/H.323/HFA) und AES-Verschlüsselung auf Preshared-Secrets-Basis (IPDA/DMC) verwendet. Die End-to-End-Verschlüsselung basiert auf einer durchgehend verschlüsselten Kette von Signalisierungs-Teilverbindungen.

- SIP/HFA/H.323-Verbindungen
- Die Signalisierung wird durch die TLS-Verbindung gesichert.
- DMC-Verbindungen
- Die Signalisierung (H.225) der DMC-Verbindungen wird mit H.235.1 (Authentifizierung und Integrität) gesichert. Das benötigte „Shared-Secret“ (Schlüssel) wird dazu von der OpenScape 4000 für jeden Anruf erzeugt und an die DMC Endpunkte verteilt. Das bedeutet, dass DMC-Verbindungen nicht verschlüsselt, sondern lediglich authentifiziert werden.

18.1.3.3 TLS Version

Protokolle TLSv1.2 und höher werden unterstützt. SSLv2, SSLv3 und TLSv1.0 sind aufgrund von Sicherheitsproblemen nicht zulässig.

Die TLS-Version kann für jede Schnittstelle (HFA/SIP/HTTPS) gesondert im WBM-Menü konfiguriert werden:

Konfiguration > Sicherheit > Einzelklick auf TLS-Chiffren für HFA oder SIP oder HTTPS

Die TLS -Version, die Methode zur Schlüsselvereinbarung für HFA und SIP im Falle von TLSv1.2, der Verschlüsselungsalgorithmus sowie der AES-Betriebsmodus können konfiguriert werden. Weitere Informationen zu TLSv1.2 finden Sie unter https://www.ietf.org/rfc/rfc5246.txt.

IMPORTANT: Nach dem Ändern und Speichern der TLS HFA-Einstellungen muss das Gateway neu gestartet werden, damit die Änderungen in Kraft treten.

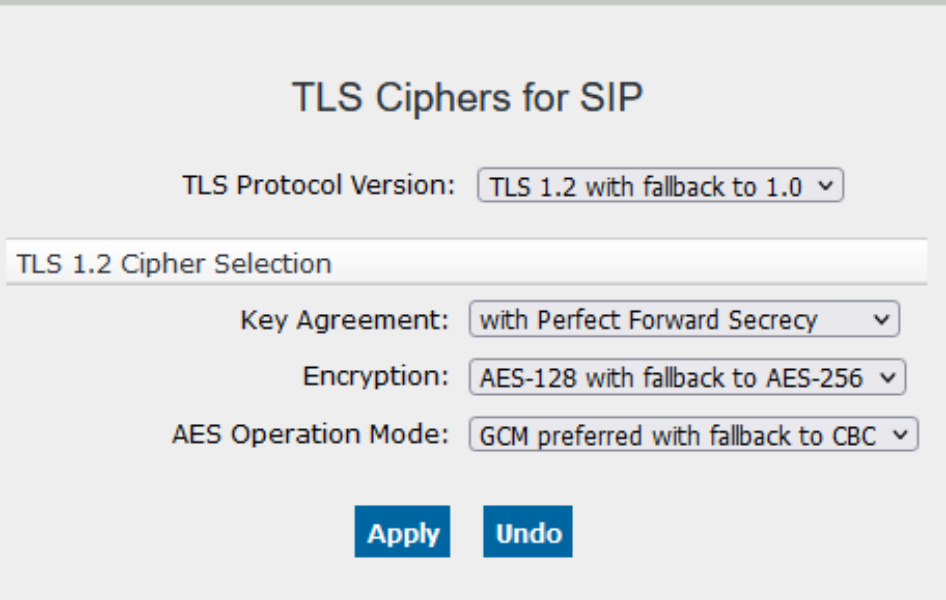


Figure 321: SPE-Konfiguration, TLS-Version

Ab V11R0 wird TLS Version 1.3 auf den VoIP-Schnittstellen (HFA und SIP) unterstützt.

NOTICE: TLS1.3-Chiffren können nicht konfiguriert werden (Einstellungen beheben).

18.1.3.4 Zertifikatsprüfungsstufe

Während des Aufbaus der TLS (Transport Layer Security)-Sitzung muss das Produkt die angegebene Identität (das Zertifikat) der Gegenstelle im Kommunikationskanal überprüfen. Diese Prüfung muss auf der Client-Seite der TLS-Sitzung durchgeführt werden, wenn es um die Identität der Serverseite geht, oder sowohl auf der Client- als auch auf der Server-Seite, wenn MTLS (Mutual TLS) verwendet wird.

Wichtig: Wenn aufseiten des TLS-Servers die Stufe Trusted (Vertrauenswürdig) oder Full (Vollständig) eingestellt ist, wird das Zertifikat des TLS-Clients angefordert (Mutual TLS). Wenn auf dem Gateway Teilnehmer konfiguriert sind, die kein Zertifikat haben, wählen Sie auf dem Gateway (auf dem TLS-Server dieser Schnittstelle) unter Certificate Verification Level (Zertifikatsprüfungsstufe) die Einstellung None, auf der Teilnehmerseite (TLS-Clients) hingegen die Einstellung Trusted (Vertrauenswürdig) oder Full (Vollständig), damit das vom TLS-Server empfangene Zertifikat geprüft wird.

Wichtig: Für SIP-Q-Trunks ist die Certificate Verification Level-Einstellung None nicht zulässig, weil Mutual TLS obligatorisch ist.

Wichtig: Wenn bei Native SIP-Trunks das Gateway über ein Zertifikat verfügt, sollte die Zertifikatsprüfungsstufe nicht auf None eingestellt werden, damit das empfangene Zertifikat geprüft wird.

Wichtig: Die eingestellte Zertifikatsprüfungsstufe gilt für alle SIP-Schnittstellen eines Gateways. Daher ist es nicht möglich, auf einem Gateway SIP-Q-Trunking und zugleich SIP-Teilnehmer ohne Zertifikate zu konfigurieren.

Für die Zertifikatsprüfung sind drei verschiedene Stufen definiert, die ausgewählt werden können:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Certificate Verification Level.

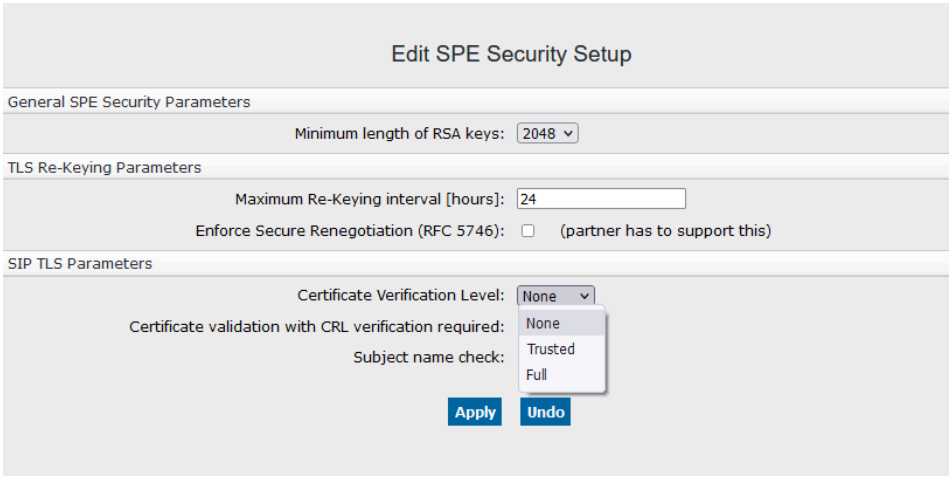


Abbildung 322: SPE-Sicherheit einrichten – Zertifikatsprüfungsstufe

- None – Die Remote-Entity wird nicht authentifiziert.

  Das Zertifikat der Remote-Entity wird nicht angefordert und nicht geprüft.

- Trusted – das von der Remote-Entity vorgelegte Zertifikat (einschließlich Zertifikatskette) wird angefordert und auf seine Integrität geprüft.

  Dies bedeutet, dass die Vertrauenskette für die von der Remote-Entity vorgelegte digitale Signatur in einem der für diese Schnittstelle im Produkt vorkonfigurierten CA-Stammzertifikate endet. Und dass alle Zertifikate in der Kette nicht abgelaufen sind (d. h. das aktuelle Datum und die Uhrzeit liegen innerhalb des angegeben Gültigkeitszeitraums des jeweiligen Zertifikats.
- Full – das von der Remote-Entity vorgelegte Zertifikat (einschließlich Zertifikatskette) wird angefordert und anhand derselben Kriterien wie im Trusted-Modus, zusätzlich jedoch

  auf die korrekte Verwendung aller wichtigen Erweiterungen geprüft (z. B. Grundlegende Einschränkungen, Verwendung des Schlüssels, Verwendung des erweiterten Schlüssels). Wenn eine Erweiterung als kritisch gekennzeichnet ist und nicht erkannt wird, muss das Zertifikat zurückgewiesen werden. Und die korrekte Verwendung bekannter Erweiterungen wird geprüft, die nicht als wichtig gekennzeichnet sind (z. B. Grundlegende Einschränkungen, Verwendung des Schlüssels, Verwendung des erweiterten Schlüssels).

  Es gibt optionale Prüfungen:

  Stufen Trusted und Full:
- Certification validation with CRL verification required:

  Die Zertifikatskette darf keine widerrufenen Zertifikate enthalten. Dieses Verhalten kann per Kontrollkästchen geändert werden:

  Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Certification validation with CRL verification required.

  Stufe Full:
- Subject name check:

  Die Identität der Remote-Entity wird überprüft. Dieses Verhalten kann per Kontrollkästchen geändert werden:

  Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Subject name check.

18.1.3.5 Minimale Länge der RSA-Schlüssel

Legen Sie die minimale Länge des von der Remote-Entity übertragenen RSA-Schlüssels fest.

Die Mindestlänge der RSA-Schlüssel kann im WBM gesetzt werden:

WBM > Konfiguration > Sicherheit > Signalisierung und Nutzlast-Verschlüsselung (SPE) > SPE-Sicherheitsaufbau > Allgemeine SPE-Sicherheitsparameter > Mindestlänge der RSA-Schlüssel

Falls die für SPE verwendeten Zertifikate mit dem RSA-Signaturalgorithmus (auch als "RSA-Zertifikate" bekannt) generiert werden, müssen Sie die Mindestlänge der RSA-Schlüssel der Fernentität definieren.

18.1.3.6 ECDSA-Zertifikate

Ab OpenScape 4000 V11 können Sie die mit dem ECDSA-Signaturalgorithmus generierten SPE-Zertifikate (auch als „ECDSA-Zertifikate“ bekannt), für OpenScape 4000 SoftGate und STMIX/STMIY, für die SIP- und HFA-TLS-Signalisierung verwenden.

Für H.323 Trunking auf OpenScape 4000 SoftGate und STMIX/STMIY werden ECDSA-Zertifikate nicht unterstützt. In diesem Fall müssen herkömmliche RSA-Zertifikate verwendet werden.

HG3500 STMI2/4-Platinen unterstützen keine ECDSA-Zertifikate. In diesem Fall müssen herkömmliche RSA-Zertifikate verwendet werden.

ECDSA hat die folgenden Vorteile gegenüber RSA:

- ECDSA bietet eine wesentlich geringere Ausgabelänge bei gleichem Sicherheitsniveau wie RSA. Eine 3072-Bit-RSA-Signatur bietet beispielsweise das gleiche Maß an Sicherheit wie eine 256-Bit-ECDSA-Signatur.
- ECDSA läuft schneller als RSA.
- ECDSA erfordert deutlich weniger Speicher als RSA.

Sie müssen jedoch sicherstellen, dass der Kommunikationspartner (z. B. die verbundenen HFA- oder SIP-Telefone oder ein Trunking-Partner wie OpenScape Voice oder OpenScape SBC) ECDSA-Zertifikate unterstützt.

Weitere Informationen finden Sie im Versionshinweis.

18.1.3.7 Maximales Intervall für Schlüssel-Neuaushandlung

Die TLS-/SSL-Verbindungen bleiben permanent aktiv und werden in regelmäßigen Zeitabständen erneuert. Das Zeitintervall für die Schlüssel-Neuaushandlung stellen Sie im WBM ein:

1) WBM > Configuration > Security > (rechte Maustaste) Signaling and Payload Encryption (SPE) > Edit Security Configuration > TLS Re-Keying Parameters > Maximum Re-Keying interval [hours]

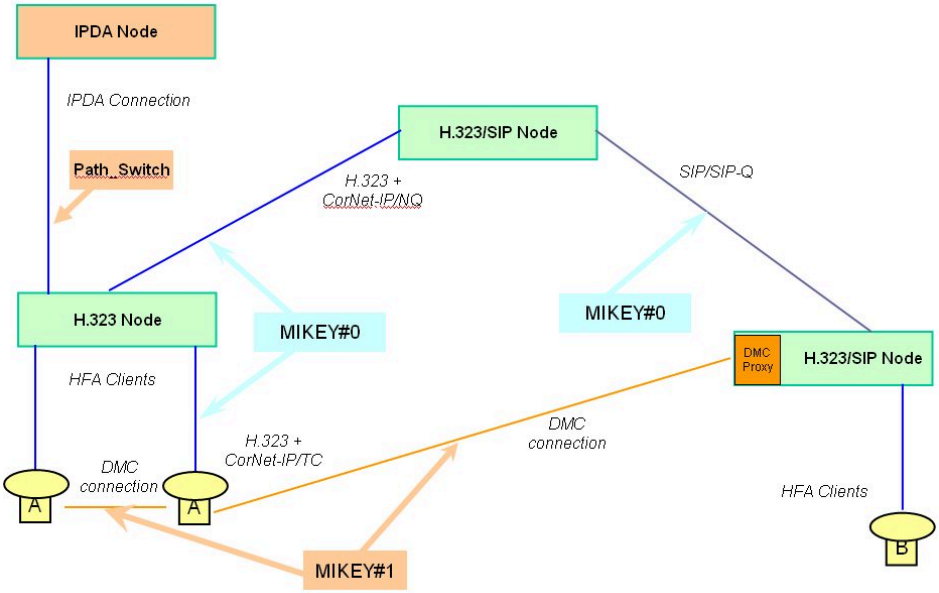
18.1.3.8 Sichere Neuaushandlung erzwingen (RFC 5746)

Wenn alle über TLS verbundenen Remote-Entities die sichere Neuaushandlung (RFC 5746) unterstützen, aktivieren Sie diese Funktion mit dieser Option. Wenn eine Remote-Entity RFC nicht unterstützt, kann in manchen Szenarien sogar der Verbindungsaufbau fehlschlagen und der Anschluss freigegeben werden.

Dieses Verhalten kann per Kontrollkästchen geändert werden:

1) Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > TLS Re-Keying Parameters > Enforce Secure Renegotiation (RFC 5746)

18.1.3.9 Sprachverschlüsselung



Sprachverschlüsselung

SRTP wird für die Sprachverschlüsselung in allen Verbindungen (HFA, SIP, IPDA) verwendet. SRTP basiert auf dem AES-Standard (Advanced Encryption Standard). Je nach Verbindungstyp erfolgt die Verschlüsselung mit dem MIKEY-, SDES- oder MEK-Verfahren.

Die Endpunkte erzeugen zu diesem Zweck (kryptographisch) zufällig 128 Bit lange Schlüssel. Der Schlüsselaustausch zwischen den beteiligten Kommunikationspartnern erfolgt im Rahmen der Signalisierung (siehe Abschnitt 1.3.2, „Signalisierungsverschlüsselung“). Für die Schlüsselerzeugung bzw. für den Austausch kommen dabei je nach Verbindungstyp MIKEY, SDES oder OpenScape 4000 interne Mechanismen zur Anwendung.

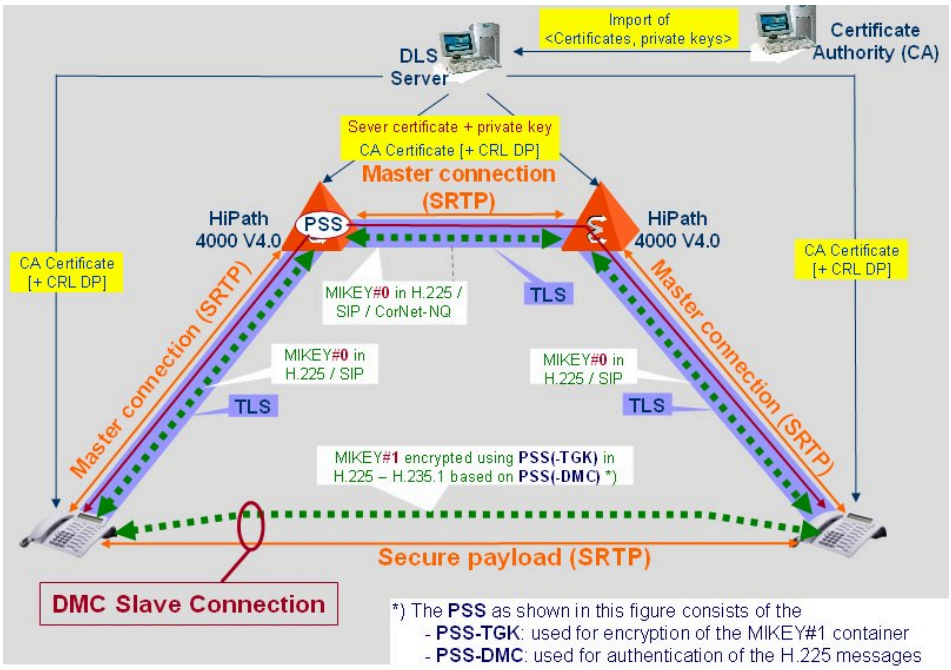
Grundsätzlich werden alle Schlüssel immer nur einmal verwendet, d.h. sie gelten ausschließlich für die Dauer der betreffenden Sprachverbindung. Den Teilnehmer wird in einer Meldung mitgeteilt, ob der Anruf durchgehend verschlüsselt ist.

IPDA

Da für IPDA-Media-Streams keine Signalisierungsverbindungen vorgesehen sind, kann der Schlüssel nicht per MIKEY ausgehandelt werden. Stattdessen wird das folgende Verfahren verwendet:

- DNIL (DB) generiert einen anrufspezifischen SRTP Master Encryption Key sowie einige weitere SRTP-Parameter wie Schlüssellänge und SALT-Key.
- CallProcessing (CP) übermittelt diese SRTP-Parameter in der PATH_SWITCH-Nachricht an die beteiligten Teilnehmer.
- Das entsprechende IP-Gateway (STMIx/NCUIx) generiert anhand der neu hinzugefügten Parameter den ansonsten von MIKEY bereitgestellten Parametersatz und verwendet diesen für die Sprachverschlüsselung.

18.1.4 MIKEY (Multimedia Internet KEYing)



MIKEY

MIKEY beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln sowie weiteren Sicherheitsparametern zwischen den Teilnehmern. In VoIP kann MIKEY für den Austausch des Masterschlüssels und weiterer Sicherheitsparameter benutzt werden, um eine sichere SRTP-Übertragung zwischen den Teilnehmern zu ermöglichen. MIKEY ist in RFC 3830 „MIKEY: Multimedia Internet KEYing“ beschrieben.

18.1.4.1 MIKEY Option 0

MIKEY Option 0 wird verwendet, wenn die Signalisierungsverbindung über TLS gesichert wird (Hop-by-Hop). Dies ist bei allen durchgängigen Payload-Streams für die (DMC)-Master-Verbindung eines OpenScape 4000-Knotens der Fall, in der alle Abschnitte Signalisierungsverschlüsselung unterstützen.

Für MIKEY Option 0 selbst werden daher keine Zertifikate benötigt; allerdings erfordern die OpenScape-4000-Anlagen bzw. deren Gateways ein eigenes (Server-) Zertifikat sowie einen privaten Schlüssel für TLS-Zwecke.

Alle beteiligten Elemente benötigen das Zertifikat der CA(s), die die Zertifikate für die OpenScape-4000-Anlagen / -Gateways ausstellt bzw. ausstellen.

Wenn die Konfiguration Kontrollen der **CRL** (**C**ertificate **R**evocation **L**ist - Zertifikatsperrliste) vorschreibt, wird der **CRL DP** (**CRL D**istribution **P**oint - HTTP/LDAP-URL) von jedem Endpunkt benötigt und muss daher ebenfalls verteilt werden.

18.1.4.2 MIKEY Option 1

MIKEY Option 1 wird nur für DMC-Slave-Verbindungen genutzt, da diese nicht über TLS gesichert werden können.

Der erforderliche symmetrische Verschlüsselungsschlüssel wird daher von der OpenScape-4000-Anlage pro Anruf erzeugt und über gesicherte Netzwerkverbindungen an die DMC-Endpunkte verteilt.

Wichtig: MIKEY Option 1 selbst erfordert keine Zertifikate.

18.1.5 Session Description (SDES)-Protocol

Das „Advanced Encryption Standard (AES)“-Verschlüsselungsverfahren kann zusammen mit dem Verschlüsselungsattribut SDES zur Sprachverschlüsselung für SIP-Verbindungen der vHG3500 verwendet werden. SDES ist in RFC 4568 „Session Description Protocol (SDP) Security Descriptions for Media Streams“ beschrieben.

Die vHG 3500/STMIX unterstützt Kryptographieprogramme mit 80-Bit-Authentifizierung und 32-Bit-Authentifizierung mit SRTP und optionalen M-Leitungen.

Wichtig: SDES wird auf der STMI-Baugruppe nicht unterstützt.

18.1.6 Master Encryption Key (MEK)

Der **MEK** (**M**aster **E**ncryption **K**ey) wird für OpenScape Access/OpenScape 4000 SoftGate Signalisierungsverbindungen verwendet.

18.1.7 Sichere SIP-Verbindungen

Einschränkungen:

- Sicherheit wird nicht für SIP-Teilnehmer unterstützt.
- Sprachverschlüsselung mit SDES wird auf der STMI-Baugruppe nicht unterstützt.

Sprachverschlüsselung mit MIKEY wird nur auf SIP-Q-Trunks unterstützt.Die möglichen Sicherheitseinstellungen sind vom Typ der Verbindung und des Gateways abhängig und in der folgenden Tabelle aufgeführt:

Tabelle 85: Mögliche Verschlüsselung je nach Verbindungsart und Gateway

Sicherheit		STMI-Baugruppe	vHG 3500/ STMIX
SIP-Teilnehmer			
	Signalisierungsverschlüsselung	---	---

Sicherheit	STMI-Baugruppe	vHG 3500/ STMIX
TLS	ok	ok
Sprachverschlüsselung	---	---
SRTP mit MIKEY-Schlüsselmanagement	---	---
SRTP mit SDES-Schlüsselmanagement	---	ok
SIP-Q Trunk		
Signalisierungsverschlüsselung		
TLS	ok	ok
Sprachverschlüsselung		
SRTP mit MIKEY-Schlüsselmanagement	ok	ok
SRTP mit SDES-Schlüsselmanagement	---	ok
Native SIP-Amtsleitung		
Signalisierungsverschlüsselung		
TLS	ok	ok
Sprachverschlüsselung		
SRTP mit MIKEY-Schlüsselmanagement	---	---
SRTP mit SDES-Schlüsselmanagement	---	ok

18.1.7.1 SIP-Q-Trunking

Wenn ein OpenScape 4000-System alle Voraussetzungen für SPE erfüllt (siehe Kapitel 3, „Konfiguration“), versucht das Gateway, eine sichere SIP-Q-Verbindung zum Gateway der Gegenstelle aufzubauen.

Wenn kein SIP-Q-Profil aktiviert ist (siehe „SIP-Konnektivität > Abschnitt , „SIP-Trunking““), erfolgt die Sprachverschlüsselung per MIKEY.

Wenn ein SIP-Q-Profil aktiviert ist, kann die Sprachverschlüsselung auf der vHG3500 konfiguriert werden.

WBM > Configuration> Voice Gateways> SIP-Amtsleitungsprofile > geeignetes SIP-Q-Amtsleitungsprofil auswählen (rechter Mausklick) > Bearbeiten

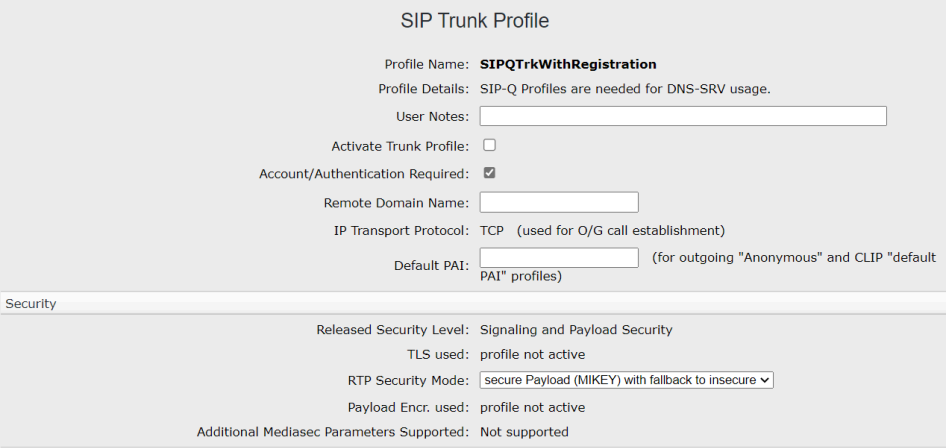


Abbildung 323: RTP-Sicherheitsmodus auf der vHG3500 für eine SIP-Q-Amtsleitung

18.1.7.2 Native SIP-Trunking

Wenn ein OpenScape 4000-System alle Voraussetzungen für SPE erfüllt (siehe Kapitel 3, “Konfiguration”), versucht das Gateway, eine sichere SIP-Verbindung zum Partner-Gateway aufzubauen, wenn dies im SIP-Trunk-Profil konfiguriert ist (siehe SIP-Konnektivität > Abschnitt 3.3, “SIP-Trunk-Profile”).

Für Native SIP-Trunks wird nur der SDES-Sprachverschlüsselungsmodus unterstützt, wenn die Sprachverschlüsselung für den Trunk-Partner freigegeben ist. Der Sprachverschlüsselungsmodus kann nicht konfiguriert werden.

Wenn ein OpenScape 4000-System alle Anforderungen für SPE erfüllt (siehe Kapitel 3, “Konfiguration”) und wenn die Sicherheit für den aktivierten SIP-Trunk-Partner freigegeben wird, versucht das Gateway, eine sichere Verbindung zum Partner-Gateway aufzubauen.

Anmerkung:

Ab der Software-Version V11R0 ist es möglich, native SIP-Trunks mit aktiviertem SPE auszuführen, ohne dass SPE auf dem gesamten OpenScape 4000-System (ZAND und SIPCO) aktiviert werden muss.

Zu diesem Zweck muss SPE über AMO TDCSU aktiviert werden, und die entsprechende Sicherheitskonfiguration muss über das WBM erfolgen.

18.1.7.3 SIP-Teilnehmer

Wenn ein OpenScape 4000-System alle Voraussetzungen für SPE erfüllt und sich ein konfigurierter SIP-Teilnehmer über TLS beim Gateway registriert, ist Payload-Sicherheit möglich, sofern sie von beiden Seiten unterstützt wird. Für SIP-Teilnehmer wird nur der SDES-Sprachverschlüsselungsmodus unterstützt.

Wenn ein SIP-Teilnehmer mit AMO SDAT als Cipher konfiguriert ist,?

(Siehe Abschnitt 3.4.2, „SPE bei IP-Endgeräten“)

18.2 Service-Informationen

18.2.1 Einschränkungen

- Der CSTA-Verkehr ist ein Klartextprotokoll und sollte in einer vertrauenswürdigen Netzwerkumgebung arbeiten. Falls dies nicht möglich ist, verwenden Sie den integrierten VPN-Dienst der OS4K Plattform (siehe OpenScape 4000 V8, Plattform Administration (Portal), Administratordokumentation, Kapitel 2.5, „Integrierter VPN-Dienst“).
- Dieses Leistungsmerkmal ist **nicht** mit der „Signalisierungs- und Sprachverschlüsselung“ in HiPath 4000 V3.0 kompatibel, d. h. im Netzverbund mit HiPath 4000 V3.0 können Signalisierung und Sprache nicht verschlüsselt übertragen werden. Bei einer Vernetzung mit HiPath 4000 V3.0 kann die Trunking-Strecke zwischen den beiden Systemen nicht verschlüsselt werden. Die interne Verschlüsselung von HiPath 4000 V3.0 kann jedoch in HiPath 4000 V3.0 aktiviert werden.
- Wenn Verschlüsselung auf einer STMI2/NCUI2+-Baugruppe aktiviert wurde, muss die Anzahl der konfigurierten Kanäle um 33 % geringer sein als ohne Verschlüsselung.
- Die genaue Anzahl der B-Kanäle finden Sie unter „Gateways HG 3500 und HG 3575“, Abschnitt 2.6, „B-Kanäle“.
- Bis zu 240 HFA- und SIP-Teilnehmer (nativ oder UFIP) können auf dem Common Gateway HG 3500 auf STMI4 mit SPE konfiguriert werden.
- Bis zu 120 HFA-Teilnehmer können auf STMI2 mit SPE konfiguriert werden.
- Bei Nutzung von SPE werden auf STMI2 keine SIP-Teilnehmer-Funktionen (nativ oder UFIP) unterstützt.
- T.38 Fax-Streams werden für SPE nicht unterstützt.

Tabelle 86: Sprachverschlüsselung

Leistungsmerkmal	STMI2	STMI4	SoftGate/STMIX
Native SIP-Trunk	☑*	☑*	☑
SIP-Q Trunk	☑	☑	☑
SIP-Teilnehmer - klassisch	☒	☒	☒
SIP-Teilnehmer - UFIP	☒	☑*	☑
Circuit-Konnektivität (UFIP)	☒	☒	☑
HFA-Teilnehmer	☑**	☑	☑
H323-Trunk	☒	☒	☒
* Nur Signalisierungsverschlüsselung wird unterstützt. SDES wird nur auf SoftGate/STMIx unterstützt.			
** Auf STMI2-Baugruppen werden maximal 120 SPE-Teilnehmer unterstützt.			

Wichtig: Ab V10R0 wird die Unterstützung für STMI2 nicht mehr angeboten. Der Ersatz für STMI2 ist STMIX.

18.2.2 Zertifikate generieren

Mit der Funktion **Automatische SPE Konfiguration** im DLS können Sie Zertifikate erstellen und an die Gateways und Endgeräte verteilen. Dies ist insbesondere dann nützlich, wenn keine Kunden-PKI zur Verfügung steht. Für mehr Informationen siehe Kapitel 8, „AutoSPE-Konfiguration“.

Alternativ ist die Generierung eines Zertifikates auf einer Common Gateway-Baugruppe möglich.

Im Falle von manuell generierten Zertifikaten (PKCS#12 Datei) bei STMI4/NCUI4 Baugruppen, kann der SHA-1 oder SHA-2 (empfohlen) Signatur-Algortihmus verwendet werden.

Der Begriff SHA-2 (SHA2) bezeichnet die gesamte Familie der SHA-2-Algorithmen, d. h. SHA-256, SHA-384, SHA-512 und SHA-224

Wichtig: Die unterstützte Schlüssellänge beträgt 4096 Bit, aber für STMI2/4-Baugruppen ist die maximale Schlüssellänge 2048 Bit.

18.2.3 Unterstützte Zertifikate

Die folgenden Zertifikate (X.509v3) können importiert werden:

- CA-Zertifikate (*.crt, *.cer) von der Certification Authority (=Zertifizierungsstelle)
- Zertifikate im Format **P**ublic **K**ey **C**ryptography **S**tandards #12 (PKCS #12) (*.p12)
- Zertifikate im Format X.509 PEM

Ein abgelaufenes Zertifikat sollte nicht neu eingespielt werden. Wenn ein Zertifikat während des Einsatzes abläuft, wird eine HISTA-Nachricht mit einer Fehlermeldung ausgegeben (F5881 mit Fehlerursache: ZERTIFIKAT ABGELAUFEN). Das System funktioniert dann im sicheren Modus mit der Zertifikatsprüfungsstufe Trusted (Vertrauenswürdig) oder Full (Vollständig) möglicherweise nicht mehr. Telefone können sich nicht bei Baugruppen registrieren und Trunks funktionieren möglicherweise nicht. Die Sicherheit kann deaktiviert werden, bis die Zertifikate erneuert werden (siehe Abschnitt 2.4, "Zertifikate erneuern").

IMPORTANT: Tauschen Sie ein Zertifikat nach Ablauf der Gültigkeit aus!

Das Ketten von Zertifikaten wird unterstützt. CA-Zertifikatsketten können entweder als separate Dateien (eine nach der anderen) importiert werden, oder eine CA-Zertifikatskette kann mit bis zu 3 CA-Zertifikaten im PEM-Format direkt importiert werden. Die Reihenfolge des Imports der CA-Zertifikatskette oder in der PEM-Datei hat keine Auswirkung.

18.2.4 Zertifikate erneuern

Abgelaufene Zertifikate sollten erneuert werden.

Informationen zum Hochladen benutzter Zertifikate beim Austauschen von SPE-Zertifikaten mit OSV finden Sie in der MOP (Vorgehensweise) INF-14-000180:

https://www.g-dms.com/livelink/livelink.exe/view/INF-14-000180

18.2.5 Baugruppentausch

Zertifikate werden bei Verlust (z. B. durch Neuladen der Baugruppe nach einem Baugruppentausch), durch den gewohnten „Backup&Restore“-Vorgang (logischer DATA-Backup) neu geladen. Dasselbe gilt für die MEKs bei der Access Point/OpenScape 4000 SoftGate Verschlüsselung.

Wichtig: Nur ein gültiges Zertifikat sollte auf das Gateway geladen werden.

18.2.6 STMI Standby-Baugruppe

In SPE wird die STMI Standby-Baugruppe unterstützt. Die Unterstützung wird angewendet, wenn ein Backup durch den gewohnten „Backup&Restore“-Vorgang (logisches DATA-Backup) durchgeführt wurde. Dadurch ist sichergestellt, dass die Reserve-Baugruppe dieselben Zertifikate und Konfigurationseinstellung aufweist wie die aktive Baugruppe.

Einschränkung

Nicht unterstützt werden sichere Verbindungen, die mit Hilfe von SIP-Trunk-Profilen konfiguriert werden.

18.2.7 Aktivieren/Deaktivieren des Leistungsmerkmals SPE für Funktionsbereiche in der Anlage

SPE-Funktionsbereiche können ohne Neustart der Anlage deaktiviert – und in manchen Fällen auch wieder reaktiviert – werden. Dadurch kann das Servicepersonal bestimmte SPE-Funktionsbereiche gezielt deaktivieren, um festzustellen, ob ein Problem durch das SPE-Leistungsmerkmal verursacht wird, und die Fehlerursache zu ermitteln. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Abschnitt 3.2, „Aktivieren/Deaktivieren von SPE bei Gateways mit AMO CGWB“
- Abschnitt 3.3, „Aktivieren/Deaktivieren von SPE bei Trunks“
- Abschnitt 3.4, „Aktivieren/Deaktivieren von SPE bei Endgeräten“
- Abschnitt 3.5, „Aktivieren/Deaktivieren von SPE bei Access Points“
- Abschnitt 3.6, „Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate“

18.2.8 Anschließen des Gateways

Es gibt verschiedene Möglichkeiten, ein Gateway anzuschließen.

Tabelle 87: Anschließen von Gateways

Verbindung zum Gateway über ...	STMI	vHG 3500
V24-Verbindung: Mit dieser Verbindung ist es möglich, mit einer Baugruppe zu kommunizieren und ihre Daten zu erfassen, bevor sie vollständig hochgelaufen ist.	ja	nein
SSH: Mit einem SSH-Client (wie TeraTerm, Putty) kann eine Verbindung hergestellt werden, sobald die IP-Kommunikation verfügbar ist.	ja	nein
SSH via HiPath 4000 Assistant unter **Expertenmodus > HG 35xx Telnet / SSH** auf einer aktiven Baugruppe, wenn der HiPath 4000 Assistant über IP-Routing-Zugriff verfügt.	ja	nein
WBM-Verbindung auf einer aktiven Baugruppe, wenn IP-Routing-Zugriff möglich ist.	ja	ja

Wichtig: Mit den ersten drei Verbindungen (1 – 3) ist ein Bootstrap-Reset auf der aktiven STMI-Baugruppen möglich.

18.2.9 SPE in Verbindung mit Mobile HFA

18.2.9.1 Terminologie

SPEcapable Client:	Ein als TRADITIONAL angemeldeter Client, der aber SPE-fähig ist und über alle erforderlichen Berechtigungsnachweise und Konfigurationen verfügt, um sich als **SECURE** oder **CIPHER** Client anmelden zu können.
TRADITIONAL Client:	Ein als TRADITIONAL angemeldeter Client , der **NICHT SPE**-fähig ist (z. B. optiPoint 500).

	**SECURE** und **CIPHER** Client
	**TRADITIONAL** Client

	SPEcapable Client

18.2.9.2 Voraussetzung

Für die Verbindung zum Gateway muss **dasselbe Protokoll** (TCP oder TLS) wie **für** die **Teilnehmeranschlüsse VISITED und HOME** verwendet werden, um zu verhindern, dass ein VISITED-Teilnehmeranschluss, der TCP nutzt, die Verbindung zu einem HOME-Teilnehmeranschluss, der TLS nutzt, trennen kann (DoS-Angriffe).

Ein über TCP verbundener HOME-Teilnehmeranschluss, dessen Verbindung von einem über TLS verbundenen VISITED-Teilnehmeranschluss getrennt wird, kann die Verbindung des VISITED-Teilnehmeranschlusses nicht trennen und daher keine Verbindung mehr zu seinem Gateway herstellen.

18.2.9.3 Szenarien mit homogenem HiPath 4000/OpenScape 4000 Netzwerk bei aktivierter SPE

Wichtig: Gilt ab Hipath 4000 V4!



	Visited		
Home	Secure/Cipher	Traditional	SPEcapable
Secure/Cipher		funktioniert nicht	kritisch[15] [16]
Traditional	keine Probleme[17]	keine Probleme	keine Probleme
SPEcapable	keine Probleme[18]	keine Probleme	keine Probleme

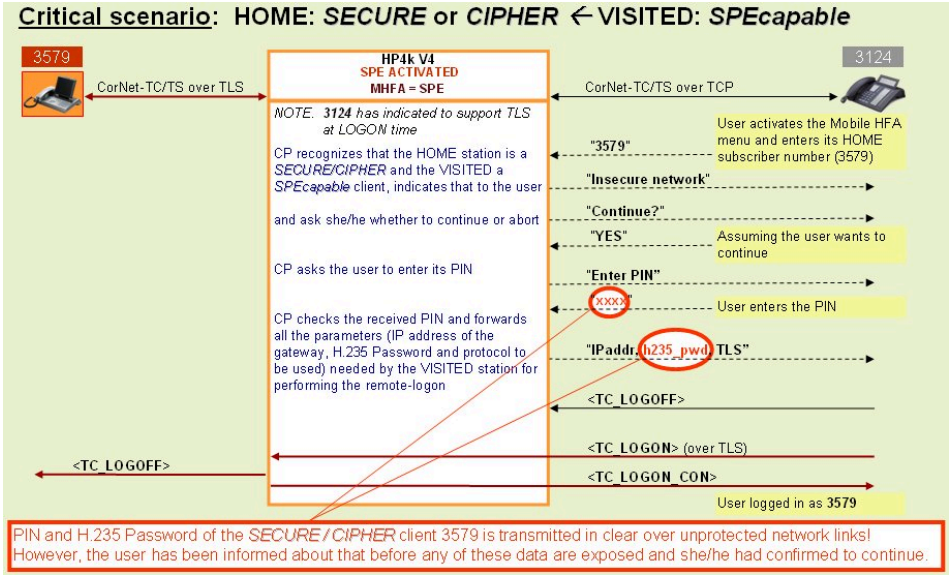
15 SPEcapable-Clients müssen TLS verwenden, wenn sie als VISITED-Teilnehmeranschluss für einen SECURE/CIPHER-Client fungieren.

16 Dieses Szenario ist kritisch, da **PIN und H.235-Passwort über ungesicherte Netzwerkverbindungen übertragen werden**.

17 Secure/Cipher-Clients müssen TCP verwenden, wenn sie als VISITED-Teilnehmeranschlüsse für einen TRADITIONAL-Client fungieren.

18 Secure/Cipher-Clients müssen TCP verwenden, wenn sie als VISITED-Teilnehmeranschlüsse für einen SPEcapable-Client fungieren.

Wichtig: Durch die SPE-/Mobile HFA-Verbindungsflüsse erhält der VISITED-Teilnehmeranschluss bereits das zur Verbindung mit dem HOME-Gateway verwendete Protokoll.



18.2.9.4 Szenarien in einem Netzwerk mit SPE-aktivierten Knoten und SPE-deaktivierten Knoten

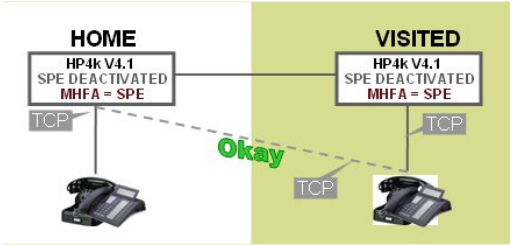
HOME und VISITED. SPE DEACTIVATED und TRADITIONAL/SPEcapable

HOME:

- SPE DEACTIVATED
- Telefone: TRADITIONAL/SPEcapable

VISITED:

- SPE DEACTIVATED
- Telefone: TRADITIONAL/SPEcapable



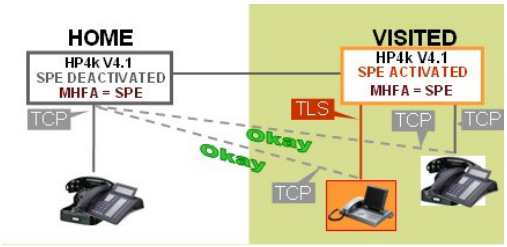
HOME: SPE DEACTIVATED und TRADITIONAL/SPEcapable, VISITED: SPE ACTIVATED und TRADITIONAL/SPEcapable und SECURE/CIPHER

HOME:

- SPE DEACTIVATED
- Telefone: TRADITIONAL/SPEcapable

VISITED:

- SPE ACTIVATED
- Telefone: TRADITIONAL/SPEcapable und SECURE/CIPHER



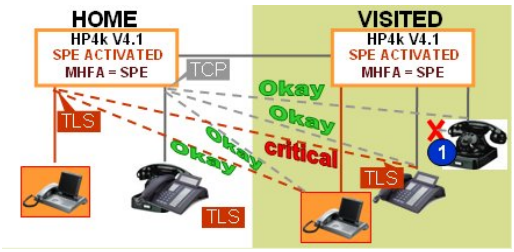
HOME: SPE ACTIVATED und TRADITIONAL/SPEcapable und SECURE/CIPHER, VISITED: SPE ACTIVATED und TRADITIONAL und SPEcapable und SECURE/CIPHER

HOME:

- SPE ACTIVATED
- Telefone: TRADITIONAL/SPEcapable und SECURE/CIPHER

VISITED:

- SPE ACTIVATED
- Telefone: TRADITIONAL und SPEcapable und SECURE/CIPHER



1	Ein **TRADITIONAL**-Client (ohne SPE-Unterstützung) wird nie als VISITED-Teilnehmeranschluss für einen **SECURE**- oder **CIPHER**-Client akzeptiert. Die Anrufverarbeitung auf dem VISITED-Switch erkennt dies und weist den Anmeldeversuch mit der Fehlermeldung „Remote Login not possible“ (Remote-Anmeldung nicht möglich) zurück, noch bevor der Benutzer zur Eingabe seiner PIN aufgefordert wird.

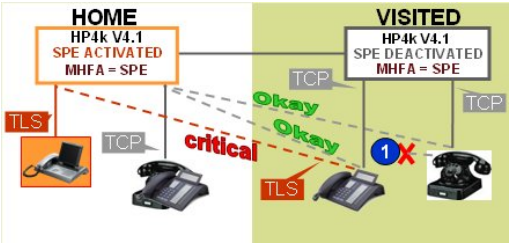
HOME: SPE ACTIVATED und TRADITIONAL/SPEcapable und SECURE/CIPHER, VISITED: SPE ACTIVATED und TRADITIONAL und SPEcapable

HOME:

- SPE ACTIVATED
- Telefone: TRADITIONAL/SPEcapable und SECURE/CIPHER

VISITED:

- SPE ACTIVATED
- Telefone: TRADITIONAL und SPEcapable



1	Ein **TRADITIONAL**-Client (ohne SPE-Unterstützung) wird nie als VISITED-Teilnehmeranschluss für einen **SECURE**- oder **CIPHER**-Client akzeptiert. Die Anrufverarbeitung auf dem VISITED-Switch erkennt dies und weist den Anmeldeversuch mit der Fehlermeldung „Remote Login not possible“ (Remote-Anmeldung nicht möglich) zurück, noch bevor der Benutzer zur Eingabe seiner PIN aufgefordert wird.

18.2.9.5 Netzweite Nutzung von Mobile HFA

Werden **TRADITIONAL** Clients auf einer HiPath 4000 mit aktivierter SPE sowohl als HOME- als auch als VISITED-Teilnehmeranschluss akzeptiert, bedeutet dies eine erhebliche Verbesserung der Nutzung des Leistungsmerkmals Mobile HFA in homogenen HiPath-4000-/OpenScape-4000-Netzwerken[19] (mit oder ohne aktivierter SPE).

Wichtig: Mobile HFA kann **nicht** in Netzwerken verwendet werden in denen HiPath-4000-Systeme (ab Version 4)/ OpenScape 4000 Systemen mit aktiviertem SPE und HiPath 4000 V2.0 / V3.0 vernetzt sind.

18.3 Konfiguration

Bevor Sie das Leistungsmerkmal **Signalisierungs- und Sprachverschlüsselung (SPE)** in einem OpenScape-4000-System konfigurieren, stellen Sie sicher, dass alle Voraussetzungen erfüllt sind (siehe Abschnitt 3.1, „Voraussetzungen“). Anschließend können Sie die einzelnen Funktionen nach Wunsch konfigurieren.

Kurzer Überblick der Vorgehensweise beim Aktivieren/Deaktivieren des SPE-Leistungsmerkmals auf einem OpenScape-4000-System.

1) Aktivieren/Deaktivieren von SPE bei Teilnehmer-Gateways

2) Wenn Sie dieses Leistungsmerkmal aktivieren, wird die Signalisierung/ Payload zwischen Endpunkten (Teilnehmer-Gateways, vHG 3500, HFA/ SIP-Teilnehmer usw.) mit TLS/SRTP verschlüsselt. Die Konfiguration erfolgt mit dem PKI (**P**ublic **K**ey **I**nfrastructure)-Prozess. Das Aktivieren/ Deaktivieren geschieht mit AMO ZANDE. Achten Sie darauf, den korrekten sicheren Port zu verwenden: Parameter TLSP (bei HFA und H323) / PORTTLS1 (bei SIP) unter AMO CGWB. Die Standardwerte lauten

[19] ab HiPath 4000 V4

4061/5061. Weitere Informationen finden Sie in Abschnitt 3.2, „Aktivieren/Deaktivieren von SPE bei Gateways mit AMO CGWB“.

Wichtig: Für Gateways in einem Access Point/OpenScape 4000 SoftGate wird das Schlüsselmaterial für Trunking und HFA über die HSR-Verbindung ausgetauscht. Wenn die HSR-Verbindung nicht verschlüsselt ist, dann wird das Schlüsselmaterial in Klartext dargestellt. Daher muss auch für OpenScape 4000 SoftGate/IPDA Access Points SPE aktiviert werden (siehe Abschnitt 3.5, „Aktivieren/Deaktivieren von SPE bei Access Points“.

---

3) Aktivieren/Deaktivieren von SPE bei Trunks
4) Wenn dieses Leistungsmerkmal aktiviert ist, wird die Signalisierung/Sprache auf dem Trunk verschlüsselt.

   Das Aktivieren/Deaktivieren geschieht durch Ändern des Sicherheitsmodus in AMO TDCSU, AMO GKREG. Weitere Informationen finden Sie in Abschnitt 3.3, „Aktivieren/Deaktivieren von SPE bei Trunks“.
5) Aktivieren/Deaktivieren von SPE bei Endgeräten
6) Aktivieren/Deaktivieren von Teilnehmer-SPE Wenn Sie dieses Leistungsmerkmal aktivieren, wird die Signalisierung/Payload zwischen den Teilnehmern und Gateways verschlüsselt. Das Aktivieren/Deaktivieren geschieht durch Ändern des Sicherheitsmodus der Teilnehmer mit AMO SDAT/WBM. Weitere Informationen finden Sie in Abschnitt 3.4, „Aktivieren/Deaktivieren von SPE bei Endgeräten“.
7) Aktivieren/Deaktivieren von SPE bei Access Points
8) Wenn dieses Leistungsmerkmal aktiviert ist, wird die Signalisierung/Sprache zwischen hergestellten HSR-Verbindungen mit PEP (**P**roprietary **E**ncryption **P**rotocol) / SRTP verschlüsselt. Die Konfiguration erfolgt durch den SPE-Administration Client-Prozess. Das Aktivieren/Deaktivieren auf der Anlage geschieht mit AMO SIPCO. Weitere Informationen finden Sie im Abschnitt 3.5, „Aktivieren/Deaktivieren von SPE bei Access Points“.
9) Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate
10) Wenn dieses Leistungsmerkmal aktiviert ist, wird die Signalisierung/Sprache zwischen hergestellten HSR-Verbindungen mit PEP (**P**roprietary **E**ncryption **P**rotocol) / SRTP verschlüsselt. Die Konfiguration erfolgt durch den MEK Administration Client-Prozess. Weitere Informationen finden Sie im Abschnitt 3.6, „Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate“.

18.3.1 Voraussetzungen

System

Bevor in einem System **SPE** aktiviert werden kann, müssen folgende Voraussetzungen erfüllt sein:

- Je nach Zertifikatsprüfungsstufe können allen (v)HG 3500-Gateways in diesem System SPE-Zertifikate und/oder mindestens ein CA-Zertifikat (siehe Abschnitt 1.3.4, „Zertifikatsprüfungsstufe“).
- Alle NCUI2-Baugruppen müssen durch NCUI2+ oder NCUI4 ersetzt werden.
- Alle (v)NCUI-Baugruppen müssen MEKs (Master Encryption Keys) konfiguriert haben.

- Zeitsynchronisation aller Komponenten über NTP-Server.

Wichtig: Der Assistent kann nicht als NTP-Server für IP-Telefone eingesetzt werden. Er weist nur eine begrenzte Anzahl Puffer auf und ist daher in umfangreicheren Anwendungssystemen nicht ausreichend zuverlässig.

18.3.2 Aktivieren/Deaktivieren von SPE bei Gateways mit AMO CGWB

Wenn SPE auf den Gateways aktiviert ist, wird die Kommunikation zwischen den Endpunkten mit TLS/SRTP verschlüsselt. Informationen zum Verteilen/Aktivieren der Zertifikate auf den Gateways finden Sie im Kapitel 7, „Verteilung von Zertifikaten mit dem WBM des Gateways“.

Wichtig: Für Gateways in einem Access Point/OpenScape 4000 SoftGate wird das Schlüsselmaterial für Trunking und HFA über die HSR-Verbindung ausgetauscht. Wenn die HSR-Verbindung nicht verschlüsselt ist, dann wird das Schlüsselmaterial in Klartext dargestellt. Daher muss auch für Access Points/OpenScape 4000 SoftGate SPE aktiviert werden (siehe Abschnitt 3.5, „Aktivieren/Deaktivieren von SPE bei Access Points“ bzw. Abschnitt 3.6, „Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate“.

Alle Komponenten sollten zeitsynchronisiert werden, da SPE zwischen Komponenten sonst nicht aktiviert werden kann.

Zum besseren Schutz vor Fehlern im Falle des Verlusts von Zertifikaten sollte für jede Baugruppe ein Backup Server konfiguriert und für jedes auf der Baugruppe neu installierte Zertifikat ein Backup durch den gewohnten „Backup&Restore“-Vorgang (logisches DATA-Backup) durchgeführt werden.

Die folgenden Schritte müssen zum Aktivieren der SPE auf einem Gateway ausgeführt werden:

1) Bereitstellen von Zertifikaten für jede zu sichernde Baugruppe. Vor der Bereitstellung der Zertifikate sollte ein Bootstrap durchgeführt werden (falls DLS für die Bereitstellung von Zertifikaten verwendet wird). Weitere Informationen finden Sie in Kapitel 6, „Verteilung von Zertifikaten an Gateways“. Informationen zu Verbindungsmöglichkeiten mit Gateways finden Sie in Abschnitt 2.8, „Anschließen des Gateways“.
2) • Aktivieren von SPE für Trunks und IP-Teilnehmer. Weitere Informationen finden Sie in Kapitel 3, „Aktivieren/Deaktivieren von SPE bei Trunks“ und Kapitel 3, „Aktivieren/Deaktivieren von SPE bei Endgeräten“.

- Aktivieren von SPE bei Gateways mit AMO ZANDE.

Aktivieren/Deaktivieren von SPE bei Gateways:
`AENDERN-ZANDE:TYP=SECURITY,SPESUPP=JA;`

Wenn der Parameter **SPESUPP** auf **JA** eingestellt ist, ist SPE aktiviert!

Parameter:

SPESUPP (JA/ NEIN):	Aktiviert SPE bei diesem System.

Wichtig: Nachdem SPE aktiviert wurde, muss ein Hard-Restart des Systems erfolgen. Vergessen Sie nicht, die Anlage vor dem Neustart EXEC-UPDAT:UNIT=BP,SUSY=ALL; zu aktualisieren. Bei einer Duplexanlage müssen Sie den folgenden Befehl bei beiden Prozessoren gleichzeitig ausführen. Das bedeutet, dass alle LTUs und APs neu gestartet werden! `EXEC-REST:TYP=MODUL,MODUL=BP,RSLEVEL=HARD;`

Ein bei der Konfiguration neuer Trunks oder Teilnehmeranschlüsse zu verwendendes Standard-Security Level kann mittels AMO ZANDE definiert werden:
`CHA-ZANDE:TYPE=SECURITY,SECTDMSB=<sec_level_subs_TDM>,`

`SECTDMTR=<sec_level_trunks TDM>,SECIPSB=<sec_level_ip_subs>,`

`SECIPTR=<sec_level_IP_trunks>;`

Parameter:

SECTDMSB (TRADITIO/SECURE):	Security Level für TDM-Teilnehmer. Standardwert: **TRADITIO**
SECTDMTR (TRADITIO/EXTSECUR):	Security Level für TDM-Trunks Standardwert: **TRADITIO**
SECIPSB (STANDARD/SECURE/CIPHER):	Security Level für IP-Teilnehmer Standardwert: **SECURE**:
SECIPTR (TRADITIO/STANDARD/SECURE/ EXTSECUR):	Security Level für IP-Trunks Standardwert: **SECURE**:
SECLVDSP **JA / NEIN**	Display Sicherheitsterminal Standardwert: **NEIN**

18.3.3 Aktivieren/Deaktivieren von SPE bei Trunks

18.3.3.1 SPE bei analogen / TDM Trunks

Wichtig: Die Aktivierung/Deaktivierung von SPE bei analogen/ TDM Trunks erfordert einen Neustart der Baugruppe.

Wichtig: Die Konfiguration von analogen und TDM Trunks hat keine Auswirkungen auf ihr Verhalten. Der einzige Zweck dieser Konfiguration besteht darin, die Verschlüsselungsendpunkte festzulegen. Die Verbindung wird dann als verschlüsselt behandelt, ist aber nicht verschlüsselt. Die andere Seite des Trunks muss ebenfalls eine OpenScape 4000 sein, die als EXTSECUR konfiguriert ist. Beachten Sie, dass eine Aktivierung von SPE auf Amtsätzen (digital und analog) nicht möglich ist.

1) `AENDERN-TDCSU:PEN=<Teilnehmerlage>, SECLEVEL=<Security_Level>;`

Das Security Level (**SECLEVEL**) kann folgende Werte annehmen:

TRADITIO:	Nichtsicherer Trunk Standardwert für TDM-Trunks
EXTSECUR:	Dieser Trunk wird mit einem anderen Mechanismus als dem dieses Leistungsmerkmals verschlüsselt (z. B. mit VPN). Damit wird dieser Trunk als „voll verschlüsselt“ behandelt, aber nicht von der OpenScape 4000 verschlüsselt. Die andere Seite des Trunks muss ebenfalls eine OpenScape 4000 sein, die als EXTSECUR konfiguriert ist.

18.3.3.2 SPE für IP-Trunking

Wichtig: Abhängig vom Gateway und vom Trunk-Typ sind bei IP-Trunking verschiedene Sprachverschlüsselungen möglich (siehe Tabelle 84: Signalisierungs- und Sprachverschlüsselung (IP-Umgebung) auf Seite 1155).

Wichtig: Die Aktivierung/Deaktivierung von SPE bei IP-Trunking erfordert einen Neustart der Baugruppe.

Folgende Schritte sind auszuführen:

1) Konfiguration des Trunks

Die Basiskonfiguration des Trunks erfolgt über AMO TDCSU:
`AENDERN-TDCSU:PEN=<Teilnehmerlage>,`**`SECLEVEL`**`=<Security_Level>;`

Security Level (**SECLEVEL**) kann folgende Werte annehmen:

TRADITIO:	Nichtsicherer Trunk Standardwert für TDM-Trunks
STANDARD	nur die Signalisierungsverschlüsselung (TLS-secured) wird unterstützt, nicht aber Sprachverschlüsselung (SRTP)
SECURE	Vollständige Verschlüsselung (SRTP + TLS-secured) Standardwert für IP-Trunks
EXTSECUR:	Dieser Trunk wird mit einem anderen Mechanismus als dem dieses Leistungsmerkmals verschlüsselt (z. B. mit VPN). Damit wird dieser Trunk als „voll verschlüsselt“ behandelt, aber nicht von der OpenScape 4000 verschlüsselt. Die andere Seite des Trunks muss ebenfalls eine OpenScape 4000 sein, die als EXTSECUR konfiguriert ist.

Wichtig: Alle Trunks auf einer Baugruppe müssen auf dasselbe Security Level konfiguriert sein.

2) Konfiguration des Gateways

a) Konfiguration des Remote-Gateways (**EXTGW**)

AENDERN-GKREG:GWNR:=<Gateway_rufnum->,**SECLEVEL=<SECURITY_pegel:>**;

Konfiguration des internen (lokalen) Gateways (**INTGW**)

Das Security Level des internen Gateways wird über AMO TDCSU (mit dem Befehl `AENDERN-TDCSU`) festgelegt. Mit der AMO GKREG können Sie das

aktuelle Security Level nur anzeigen, aber nicht ändern. Verwenden Sie zum Ändern des Security Levels die AMO TDCSU.

Sollte für das interne Gateway nicht das über AMO TDCSU konfigurierte Security Level angezeigt werden, gibt es folgende Gründe:

a) SPE ist nicht aktiv (mit AMO ZANDE überprüfen), oder

b) Zertifikate sind nicht vorhanden, fehlerhaft oder abgelaufen (weitere Informationen finden Sie unter WBM/DLS und AMO HISTA, AMO BCSU, AMO SDSU).

AMO BCSU

Detaillierte Informationen finden Sie in der AMO BCSU mit dem Befehl `ABFRAGEN-BCSU:TYP=TBL,LTG=<ltg>,LTU=<ltu>,EBT=<slot>;` im Abschnitt **SECURITY STATUS**.

AMO SDSU

Detaillierte Informationen finden Sie auch in der AMO SDSU mit dem Befehl `DISP-SDSU`. Siehe **SECURITY LEVEL** in der Ausgabe.

```
<DISPLAY-
SDSU:STATUS=ALL,TYPE=PEN,LEVEL=PER3,LTG=1,LTU=1,SLOT=14;
DISPLAY-
SDSU:STATUS=ALL,TYPE=PEN,LEVEL=PER3,LTG=1,LTU=1,SLOT=14;
H500: AMO SDSU STARTED
  LTG1 (PERIPHERY)

  ------

  MOUNTING LOCATION MODULE NAME BDL BD(#=ACT) STATUS
  ------------------- LTG 1 ---------------------
 READY
  -AP370013-----SG 1 LTU 1 ---------------------- READY
  ** .LTG 1.LTU 1.014 STMI4 A Q2324-X510 READY
                       LAN CONN. . . . . . . . . .
 READY
                       LINK SIGNAL ETHERNET . . . .
   PRESENT
                       LAN SPEED . . . . . . . . .
 100 MBIT/S
                       LAN INTERFACE . . . . . . . .
 FDX (FULL DUPLEX)
                       CCT FUNCTION BLOCK
                       0 HG3570_2
                       1 - 2 HG3550_2
                       3 - 12 HG3530_2
 13 - 22 HG3540_2
              CCT LINE STNO SI BUS TYPE
              001 2401 PP NW READY
                MULTLINE
 10 . . . . . . . . . . . . . .READY
                000 NO CONN
                001 NETWORK SUBUNIT. TMD CONN ISDN
 READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . . . . TMD CONN ISDN
 READY
```

```
                002 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                003 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                004 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                005 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                006 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                007 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                008 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                009 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                010 NETWORK SUBUNIT. TMD CONN ISDN
READY
                (ALT_ROUT: N) (HG3550IP)
                  LINE: 2401 STNO: SI:
                    001 . . . . . TMD CONN ISDN
READY
                011 NO CONN
                012 NO CONN
```

```
                013 NO CONN
                014 NO CONN
                015 NO CONN
                016 NO CONN
                017 NO CONN
                018 NO CONN
                019 NO CONN
                020 NO CONN
                021 NO CONN
                022 NO CONN
                023 NO CONN
                024 NO CONN
                025 NO CONN
                026 NO CONN
                027 NO CONN
                028 NO CONN
029 NO CONN
                030 NO CONN
                SECURITY LEVEL . . . . . (CONF.)
"SECURE"
                                         (ACT.)
"SECURE"
           CCT LINE STNO SI BUS TYPE
           002 2402 NOGEN
           003 2403 OPTI ONLY READY
             MULTLINE
8. . . . . .READY
                000 NO CONN
                001 SUBUNIT . . . . . DIGITE MAIN READY
                (ALT_ROUT: N) (OPTIIP )
                  LINE: 2470 STNO: 24054 SI:VCE
                    001 . . . . . DIGITE SUB A
READY
                    002 . . . . . DIGITE SUB A
READY
                    003 . . . . . DIGITE SUB C
READY
                002 NO CONN
                003 NO CONN
                004 NO CONN
                005 NO CONN
                006 NO CONN
                007 NO CONN
008 NO CONN
                SECURITY LEVEL . . . . . (CONF.)
"SECURE"
                                         (ACT.)
"TRADITIO"
           CCT LINE STNO SI BUS TYPE
           004 2404 OPTI ONLY READY
             MULTLINE
8. . . . . .READY
                000 NO CONN
                001 SUBUNIT . . . . . DIGITE MAIN READY
                (ALT_ROUT: N) (OPTIIP )
                  LINE: 2471 STNO: 24055 SI:VCE
```

```
                    001 . . . . . . . . DIGITE SUB A
READY
                    002 . . . . . . . . DIGITE SUB A
READY
                    003 . . . . . . . . DIGITE SUB C
READY
                002 NO CONN
                003 NO CONN
                004 NO CONN
                005 NO CONN
                006 NO CONN
                007 NO CONN
008 NO CONN
                SECURITY LEVEL . . . . . . . (CONF.)
"CIPHER"
                                             (ACT.)
"CIPHER"
              CCT LINE STNO SI BUS TYPE
              005 2405 OPTI ONLY READY
                MULTLINE
8. . . . . . . . . . . . . . .READY
                000 NO CONN
                001 SUBUNIT . . . . . DIGITE MAIN READY
                (ALT_ROUT: N) (OPTIIP )
                  LINE: 2472 STNO: 24056 SI:VCE
                    001 . . . . . . . . DIGITE SUB A
READY
                    002 . . . . . . . . DIGITE SUB A
READY
                    003 . . . . . . . . DIGITE SUB C
READY
                002 NO CONN
                003 NO CONN
                004 NO CONN
                005 NO CONN
                006 NO CONN
                007 NO CONN
008 NO CONN
                SECURITY LEVEL . . . . . . . (CONF.)
"SECURE"
                                             (ACT.)
"SECURE"
              CCT LINE STNO SI BUS TYPE
              006 2406 OPTI ONLY READY
                MULTLINE
8. . . . . . . . . . . . . . .READY
                000 NO CONN
                001 SUBUNIT . . . . . DIGITE MAIN TRS
                (ALT_ROUT: N) (OPTIIP )
                  LINE: 2193 STNO: 24057 SI:VCE
                    001 . . . . . . . . DIGITE SUB A
UNACH
                    002 . . . . . . . . DIGITE SUB A
UNACH
                    003 . . . . . . . . DIGITE SUB C
UNACH
```

```
                002 NO CONN
                003 NO CONN
                004 NO CONN
                005 NO CONN
                006 NO CONN
                007 NO CONN
                008 NO CONN
SECURITY LEVEL . . . . . (CONF.) "SECURE"

                                                (ACT.)
"UNKNOWN"
             CCT LINE STNO SI BUS TYPE
             007 2407 OPTI ONLY READY
               MULTLINE
8. . . . . .READY
                000 NO CONN
                001 SUBUNIT . . . . . DIGITE MAIN TRS
                (ALT_ROUT: N) (OPTIIP )
                  LINE: 2436 STNO: 24058 SI:VCE
                    001 . . . . . DIGITE SUB A
UNACH
                    002 . . . . . DIGITE SUB A
UNACH
                    003 . . . . . DIGITE SUB C
UNACH
                002 NO CONN
                003 NO CONN
                004 NO CONN
                005 NO CONN
                006 NO CONN
                007 NO CONN
                008 NO CONN
SECURITY LEVEL . . . . . (CONF.) "SECURE"

                                                (ACT.)
"UNKNOWN"
             CCT LINE STNO SI BUS TYPE
             008 2408 NOGEN
             009 2409 NOGEN
             010 2410 NOGEN
             011 2411 NOGEN
             012 2412 NOGEN
             013 2413 PP S0 READY
               ELEM DEV. . . . . SB FCT TERM READY
               (ALT_ROUT: N) (S0PP )
                 LINE: 2413 STNO: 24060 SI:VCE
               SECURITY LEVEL . . . . . (CONF.)
"SECURE"
                                                (ACT.)
"TRADITIO"
             CCT LINE STNO SI BUS TYPE
             014 2414 PP S0 READY
               ELEM DEV. . . . . SB FCT TERM READY
               (ALT_ROUT: N) (S0PP )
                 LINE: 2414 STNO: 24061 SI:VCE
```

```
                SECURITY LEVEL . . . . . . . (CONF.)
"SECURE"
                                             (ACT.)
"UNKNOWN"
            CCT LINE STNO SI BUS TYPE
            015 2415 NOGEN
            016 2416 NOGEN
            017 2417 NOGEN
            018 2418 NOGEN
            019 2419 NOGEN
            020 2420 PP S0 READY
              ELEM DEV. . . . . SB FCT TERM READY
              (ALT_ROUT: N) (S0PP )
                LINE: 2420 STNO: 24067 SI:VCE
              SECURITY LEVEL . . . . . . . (CONF.)
"SECURE"
                                             (ACT.)
"UNKNOWN"
            CCT LINE STNO SI BUS TYPE
            021 2421 PP S0 READY
              ELEM DEV. . . . . SB FCT TERM READY
              (ALT_ROUT: N) (S0PP )
                LINE: 2421 STNO: 24068 SI:VCE
              SECURITY LEVEL . . . . . . . (CONF.)
"SECURE"
                                             (ACT.)
"UNKNOWN"
            CCT LINE STNO SI BUS TYPE
            022 2422 NOGEN
```

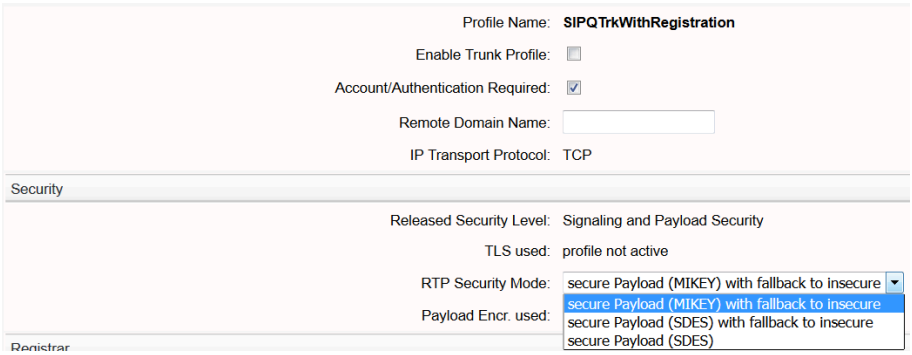
3) Security Parameter des SIP Trunk Profils

Bei SIP-Q-Trunks kann, bei native SIP-Trunks muss ein SIP Trunk Profil aktiviert werden (siehe „SIP-Connectivity > Abschnitt 3.3, „SIP-Trunk Profile““).

- SIP-Q Trunk Profil
- Wird ein SIP-Q Trunk Profil verwendet, dann kann der **RTP Security Mode** im vHG 3500 konfiguriert werden.

  WBM > Configuration > Voice Gateway > SIP Trunk Profiles > Profile selektieren (rechte Maustaste) > Edit

  Der Standardwert ist secure Payload (MIKEY) with fallback to insecure.



  SIP Trunk Profil, SIP-Q, Security-Parameter

- Native SIP Trunk Profil

- Für Native SIP-Trunks wird nur der SDES-Sprachverschlüsselungsmodus unterstützt, wenn die Sprachverschlüsselung für den Trunk-Partner freigegeben ist. Der Sprachverschlüsselungsmodus kann nicht konfiguriert werden. Da SDES auf STMI-Baugruppen nicht unterstützt wird, ist keine Sprachverschlüsselung möglich.

18.3.3.3 Deaktivierung von SPE für SIP-Q/Native SIP-Trunking

SPE deaktivieren

Wichtig: SPE kann ohne Neustart deaktiviert werden.

Das Herabsetzen des Security Levels von **SECURE** auf **TRADITIO** eines Partner-Gateways (**AMO GKREG**, Parameter **SECLEVEL**) hat zur Folge, dass alle darauffolgenden Verbindungen über TCP oder UDP aufgebaut werden. Also ist SPE bei allen Folgeverbindungen zu jenem Partner-Gateway deaktiviert.

Die bestehenden Anrufe bleiben auf TLS, wie auch die TLS-Verbindung bestehen bleibt, auch wenn alle dazugehörigen Anrufe beendet sind. Das Gateway selbst bleibt auch im SecureMode.

Wichtig: Um SPE bei von diesem Partner-Gateway ankommenden Anrufen zu deaktivieren, muss auch an der Partner-Anlage die AMO GKREG (Parameter **SECLEVEL=TRADITIO**) neu konfiguriert werden.

SPE aktivieren

SPE kann ohne Neustart aktiviert werden.

Wie die Deaktivierung erfolgt auch die Aktivierung über AMO GKREG.

Wichtig: Gateway muss bereits im SecureMode sein. Achten Sie bei der Aktivierung auf mögliche Änderungen in der Partner-Anlage (AMO GKREG, **SECLEVEL**=SECURE).

18.3.4 Aktivieren/Deaktivieren von SPE bei Endgeräten

Sowohl die HFA/SIP-Teilnehmer als auch das OpenScape 4000-System müssen für Signalisierungs- und Sprachverschlüsselung konfiguriert werden.

18.3.4.1 SPE bei analogen/TDM-Endpunkten

Wichtig: Die Konfiguration von analogen und TDM-Endpunkten hat keine Auswirkungen auf ihr Verhalten. Der einzige Zweck dieser Konfiguration besteht darin, eine durchgängige

Verschlüsselung festzulegen. Die Verbindung wird dann als verschlüsselt behandelt, ist aber nicht verschlüsselt.

```
AE-
SDAT:STNO=<Teilnehmerrufnummer>,TYP=DATEN1,CLASSSEC=<Security_Level>;
```

Das Security Level (**CLASSSEC**) kann folgende Werte annehmen:

TRADITIO:	Nichtsicherer Endpunkt Standardwert.
SECURE	Vollständige Verschlüsselung (SRTP + TLS-secured) Das Telefon ist durch externe Maßnahmen gesichert, aber nicht durch OpenScape 4000 verschlüsselt. Von der Anrufverarbeitung wird dieses Telefon als voll gesichert behandelt.

18.3.4.2 SPE bei IP-Endgeräten

Wichtig: Damit SIP-Teilnehmer nach dem Aktivieren von SPE (mit AMO ZANDE und/oder AMO SIPCO) weiterhin funktionieren, muss ein Hard-Restart ausgeführt werden. Auf einem Duplex-System sind zwei aufeinander folgende Neustarts erforderlich, um sicherzustellen, dass alle Gateways mit der neuen SPE-Konfiguration neu geladen werden.

Wichtig: Für SIP-Teilnehmer wird nur der SDES-Sprachverschlüsselungsmodus unterstützt. Da SDES auf STMI-Baugruppen nicht unterstützt wird, ist keine Sprachverschlüsselung möglich.

Eine Liste der Teilnehmer, die SPE unterstützen, finden Sie in der Kompatibilitätsmatrix in den Versionshinweisen.

18.3.4.3 Konfiguration

1) Konfigurieren des IP-Teilnehmers.

Die grundlegende Teilnehmerkonfiguration erfolgt über AMO SDAT:

```
CHANGE-
SDAT:STNO=<Teilnehmerrufnummer>,TYPE=DATA1,CLASSSEC=<security
```

_level>;

Das Security Level (**CLASSSEC**) kann folgende Werte annehmen:

SECURE:	Diese Teilnehmer dürfen je nach Teilnehmereinstellungen (WBM/DLS) über TLS oder TCP Verbindungen zum HFA/SIP-Gateway herstellen. Das bedeutet, dass dieser Teilnehmer völlig sicher (SRTP+TLS) oder aber in herkömmlicher Weise unsicher ist, d.h. dass keine Signalisierungs- oder Sprachverschlüsselung erfolgt. Die Einstellung erfolgt über WBM/DLS für den Teilnehmer. Die AMO SDAT-Konfiguration bleibt in beiden Fällen **SECURE** (Einstellung des Teilnehmers sicher oder unsicher). Standardwert.
CIPHER:	Diese Teilnehmer lassen nur vollkommen verschlüsselte Direktverbindungen zu. Das bedeutet, dass die Verbindung zum angemeldeten System und alle DMC-Verbindungen verschlüsselt werden müssen. Diese Einstellung bietet die höchste Sicherheit, kann aber zu einer geringeren Verbindungsqualität führen. Diese Einstellung kann nicht auf SIP-Teilnehmer auf STMI-Baugruppen angewendet werden.

Wichtig: Bei HFA-Teilnehmern sind die Sprach- und die Signalisierungsverschlüsselung nicht getrennt: entweder sind beide aktiv oder beide inaktiv.

Wichtig: HFA/SIP-Teilnehmer können in AMO SDAT nur als SECURE oder CIPHER konfiguriert werden. Zwar sind noch andere Werte in der AMO verfügbar, diese können für HFA/SIP-Teilnehmer jedoch nicht verwendet werden.

2) Konfigurieren von SPE aufseiten des HFA-Teilnehmers

SPE-Einstellungen werden aufseiten des HFA-Teilnehmers entweder mit DLS/WBM oder über den Teilnehmer selbst vorgenommen. Signalisierungs-

und Anzeigeeinstellungen können ebenfalls beim Teilnehmer vorgenommen werden.

OpenStage WBM

(Register) **Administrator Pages > System > Security** (Administratorseiten > System > Sicherheit)

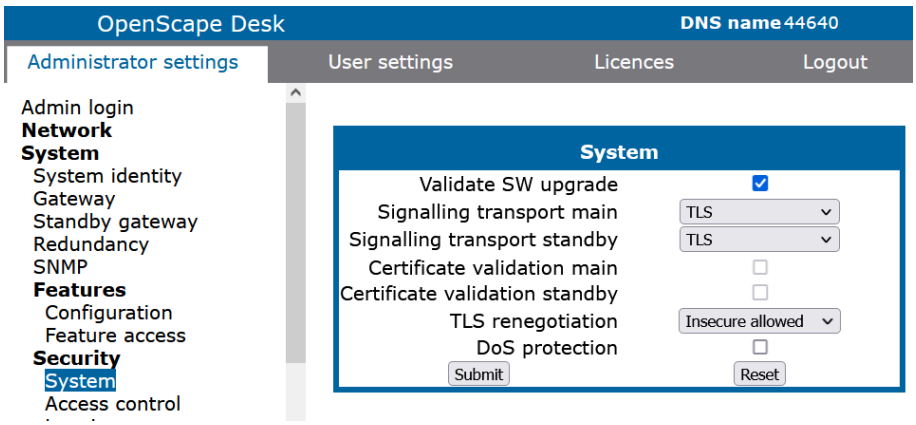


Abbildung 324: optiPoint WBM

In diesem Menü kann angegeben werden, ob TLS oder TCP als **Transportmodus** genutzt wird. Darüber hinaus kann festgelegt werden,

dass das SPE-Zertifkat vom CA-Zertifikat überprüft wird (Kontrollkästchen **Certificate Check**).

Admin > System > Signaling & Payload Encryption (SPE)

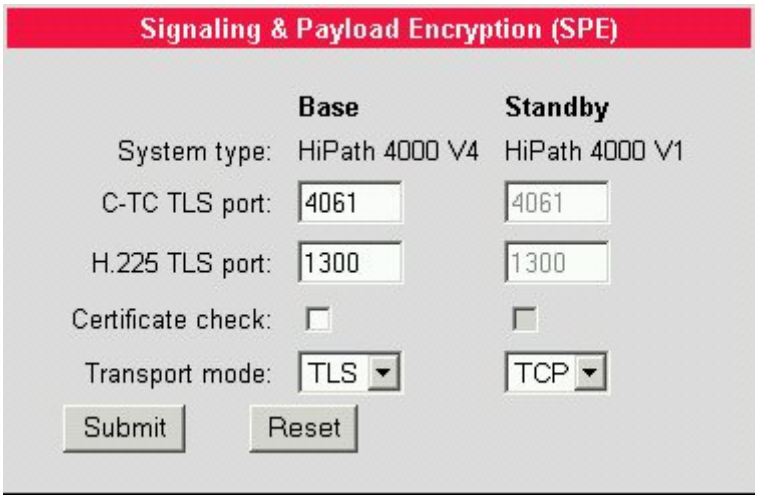


Abbildung 325: DLS

IP Devices > IP Phone Konfiguration > Signaling und Payload Encryption (SPE)

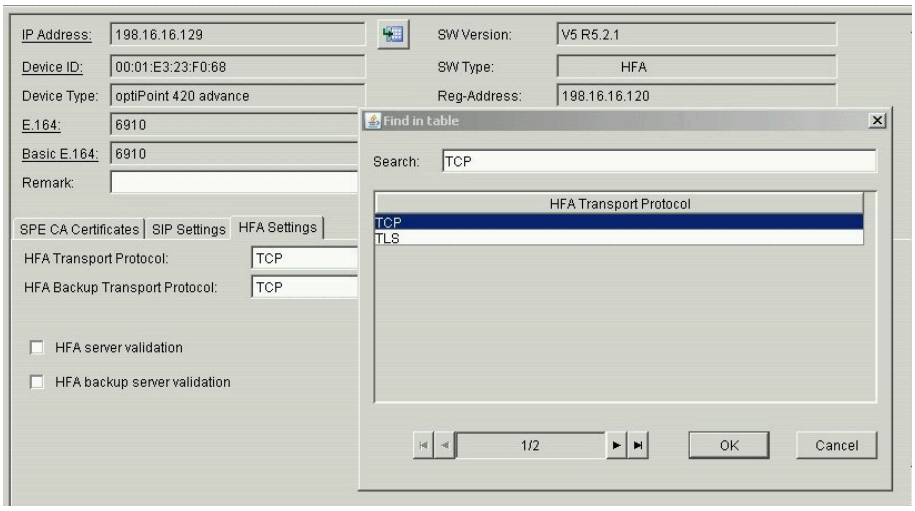


Abbildung 326: Weitere Informationen / Dokumentation

Weitere Informationen finden Sie in der betreffenden Dokumentation:

Deployment Service

http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=OpenScape%20Deployment%20Service&product_version_main=&product_version_sub=&search_term_type=all&

OpenStage HFA-Endgeräte

- OpenStage HFA

http://apps.g-dms.com:8081/edoku/jsp/searchresult_v2.jsp?edokutype=&search_mode=product&product=OpenStage%20HFA&product_version_main=&product_version_sub=&search_term_type=all&ter

optiPoint 410

- optiPoint 410 advance

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B413017619/index.htm

- optiPoint 410 economy/standard

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B412017619/index.htm

- optiPoint 410 entry

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B411017619/index.htm

Betriebsanleitung für optiPoint 420

- optiPoint 420 advance

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B423017619/index.htm

- optiPoint 420 economy/standard

http://apps.g-dms.com:8081/techdoc/en/P31003H8400B422017619/index.htm

optiPoint 410/420 Administratordokumentation

- optiPoint 410/420 Administratordokumentation

http://apps.g-dms.com:8081/techdoc/en/P31003A2056B4150176A9/index.htm

3) SPE aktivieren

4) Alle zuvor beschriebenen Konfigurationen werden erst wirksam, wenn SPE bei diesem System aktiviert wird:
`AENDERN-ZANDE:TYP=SECURITY,SPESUPP=JA;`

Parameter:

SPESUPP (JA/NEIN):	Aktiviert SPE bei diesem System.

Weitere Informationen finden Sie in Kapitel 3, „Aktivieren/Deaktivieren von SPE bei Gateways mit AMO CGWB“

Wichtig: Nachdem SPE aktiviert wurde, muss ein Hard-Restart des Systems erfolgen. Bei einer Duplexanlage müssen Sie den folgenden Befehl bei beiden Prozessoren gleichzeitig ausführen. Das bedeutet, dass alle LTUs und APs neu gestartet werden! `EXEC-REST:TYP=MODUL,MODUL=BP,RSLEVEL=HARD;`

18.3.4.4 Signalisierung auf dem Display

Eine Verbindung wird als „encrypted“ (verschlüsselt) angezeigt, wenn alle Abschnitte (Signalisierung & Payload) und der DMC-Pfad (Signalisierung & Payload) zwischen allen Teilnehmern des Anrufs verschlüsselt werden.

18.3.4.4.1 Anzeige im Gesprächszustand

Wenn auf dem Display eines Teilnehmers angezeigt werden soll, ob eine Verbindung verschlüsselt ist, müssen Sie zunächst den Parameter **SECLVDSP** in der AMO ZANDE systemweit aktivieren.
`CHANGE-ZANDE:TYPE=SECURITY,SECLVDSP=YES;`

Außerdem muss das Attribut **SECLVDSP** in der AMO SDAT bei den Teilnehmern aktiviert werden, an deren Geräten die Anzeige erscheinen soll.
`CHA-SDAT:STNO=<Teilnehmerrufnummer>,TYPE=ATTRIBUT,AATTR=SECLVDSP;`

Wichtig: Wenn Sie eine Anzeige wünschen, muss der Parameter **SECLVDSP** sowohl in der AMO ZANDE als auch in der AMO SDAT aktiviert werden. Beim erstmaligen Aktivieren des Parameters in ZANDE muss für jeden Teilnehmer von Hand ein RES-DSSU:PEN,â¦ ausgeführt werden (wenn der Parameter LAUFEND auf ja eingestellt ist, wird der Neustart des Telefon für alle betreffenden Teilnehmer automatisch ausgeführt).

Über AMO SDAT, Parameter **EMERK=SECLVTON**, kann zusätzlich konfiguriert werden, dass der sichere Teilnehmeranschluss einen Hinweiston erhält, wenn das Gespräch nicht verschlüsselt ist.
`CHANGE-SDAT:STNO=<Teilnehmerrufnummer>,TYPE=ATTRIBUT,AATTR=SECLVTON;`

18.3.4.4.2 Anzeige im Ruhezustand

Am Display eines Teilnehmers im Ruhezustand (ohne aktive Verbindung) wird nicht angezeigt, ob das Endgerät sicher ist oder nicht.

Anzeige per Tastendruck

Hierfür kann in der AMO TAPRO eine Taste konfiguriert werden, die den Status des Teilnehmeranschlusses zur Anzeige bringt:

Beispiel: `AENDERN-TAPRO:TLNNU=<teilnehmernummer>,TD09=SECURE;`

Bitte beachten Sie, dass bei den OpenStage-Teilnehmern die ersten acht Tasten vorbelegt sind.

Anzeige über SPE-Eintrag im Menü

Sie können den Sicherheitsstatus eines Teilnehmers im Ruhezustand auch über das Menü des Teilnehmers überprüfen.

- **Sprachverschlüsselung nicht aktiviert**
- – Der Teilnehmer ist über TLS mit dem Switch verbunden, aber SPE ist bei diesem Teilnehmer nicht aktiviert, oder
  – Der Teilnehmer ist über TCP mit dem Switch verbunden. In diesem Fall ist die Konfiguration des Teilnehmers am Switch ohne Bedeutung.

  In diesem Fall ist die Verschlüsselung immer deaktiviert (**Voice encryption not enabled**).
- **Voice encryption enabled** (Sprachverschlüsselung aktiviert)
- Der Teilnehmer ist über TLS mit dem Switch verbunden und als **SECURE**-Client konfiguriert.

  In diesem Fall ist die Verschlüsselung aktiviert (**Voice encryption enabled**).
- **Voice encryption always active** (Sprachverschlüsselung immer aktiviert)

- Der Teilnehmer ist über TLS mit dem Switch verbunden und als **CIPHER**-Client konfiguriert.
  - Eine Anmeldung über TCP ist nicht möglich.
  - Alle Mediaströme werden verschlüsselt (zumindest zum Gateway).

  In diesem Fall ist die Verschlüsselung immer aktiviert (**Voice encryption always active**).

18.3.4.4.3 Szenarien

- Client A - Standard-Client
- Der Teilnehmer ist über TLS mit dem Switch verbunden, aber SPE ist bei diesem Teilnehmer nicht aktiviert, oder der Teilnehmer ist über TCP mit dem Switch verbunden (Konfiguration des Teilnehmers am Switch ohne Bedeutung).
- Client B - SECURE-Client
- Der Teilnehmer ist über TLS mit dem Switch verbunden und im System als **SECURE**-Client konfiguriert.
- Client C - CIPHER-Client
- Der Teilnehmer ist über TLS mit dem Switch verbunden und im System als **CIPHER**-Client konfiguriert.

Sichere Verbindung: B ruft C an

Beide Teilnehmer haben eine sichere Verbindung zum Gateway. Somit ist die DMC-Verbindung ebenfalls sicher. Auf den Displays beider Teilnehmer wird **encrypted call** (Verschlüsselter Anruf) eingeblendet. Während der Verbindung können beide Teilnehmer den Sicherheitsstatus in ihren Menüs überprüfen.

Unsichere Verbindung: A ruft B an

Die Verbindung von A zum Gateway ist unsicher. Nur die Verbindung vom Gateway zum Client B ist sicher. Somit ist die DMC-Verbindung unsicher. Auf den Displays beider Teilnehmer wird **call not encrypted** (Unverschlüsselter Anruf) eingeblendet. Während der Verbindung können beide Teilnehmer den Sicherheitsstatus in ihren Menüs überprüfen.

Unsichere Verbindung: A ruft C an

Die Verbindung von A zum Gateway ist unsicher. Nur die Verbindung vom Gateway zum Client C ist sicher. Wenn eine DMC-Verbindung hergestellt wird, ist diese unsicher. Die DMC-Verbindung endet bei der OpenScape 4000, da alle Verbindungen zum Client C (CIPHER) sicher sein müssen. Auf den Displays beider Teilnehmer wird **call not encrypted** (Unverschlüsselter Anruf) eingeblendet. Während der Verbindung können beide Teilnehmer den Sicherheitsstatus in ihren Menüs überprüfen.

18.3.4.5 Deaktivieren von SPE bei Endgeräten

Mit DLS/WBM kann SPE für alle HFA/SIP-Teilnehmer deaktiviert werden. Dies führt dazu, dass alle Teilnehmer abgemeldet und anschließend über TCP wieder angemeldet werden.

Die Gateways selbst bleiben im sicheren Modus, es werden jedoch **keine** Verschlüsselungsmethoden verwendet, solange alle Clients über TCP verbunden sind.

CIPHER-Clients funktionieren erst dann fehlerfrei, wenn sie in AMO SDAT in **SECURE** geändert wurden.

SPE aktivieren

Verwenden Sie wie beim Deaktivieren DLS/WBM.

Beim Deaktivieren oder Aktivieren von SPE werden die Teilnehmer ab- und wieder angemeldet.

Wichtig: Die Gateways müssen sich bei der Anmeldung der Clients über TLS bereits im sicheren Modus befinden.

18.3.5 Aktivieren/Deaktivieren von SPE bei Access Points

Einschalten

Folgende Schritte sind auszuführen, um SPE bei Access Points zu aktivieren.

1) Verteilen Sie den **M**aster **E**ncryption **K**ey (**MEK**) über OpenScape 4000 Assistant an **alle** im System konfigurierten APs (Status **Ready** (bereit), **NPR** (nicht präsent) sowie **UNACH** (hierarchisch gesperrt)).

   Damit wird

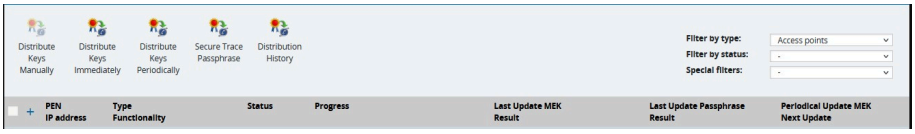
   - in RMX der MEK bei allen Access Points ungeachtet ihres Zustands konfiguriert, und
   - der MEK an alle Access Points mit dem Status **Ready** gesendet.

   Der **M**aster **E**ncryption **K**ey (MEK) wird zum Verschlüsseln der Signalisierungsdaten zwischen dem Hostsystem und einem IPDA-Access Point genutzt.

   Der MEK muss für neue Access Points zuerst auf den NCUI-Baugruppen und dann im Hostsystem konfiguriert werden. Weitere Informationen finden Sie in Abschnitt 3.5.1, „Neuer Access Point in einem aktiven SPE-System“.

   Der MEK wird über den OpenScape 4000 Assistant konfiguriert:

   Experten Modus > Signaling & Payload Encryption > Administration > Bereiche **Konfiguration Automatische MEK Verteilung** und **Manuelle MEK Verteilung**

   Weitere Informationen über die MEK-Verwaltung finden Sie im Administratorhandbuch„OpenScape 4000 Assistant V, MEK Administration“ (http://apps.g-dms.com:8081/techdoc/de/P31003H340M1440100A9/index.htm).

2) Überprüfen Sie das Protokoll des MEK-Clients auf etwaige AP-Fehler.

   Experten Modus > Signaling & Payload Encryption > Administration > Bereich **MEK / Passphrase Verteilung Protokoll**

3) Bei Access Points im Zustand **NPR** und **UNACH** müssen Sie den MEK manuell über die CLI am Access Point eingeben, indem Sie den Befehl `Set new MEK XXXXXXXXXXXXXXXX` (Neuen MEK XXXXXXXXXXXXXXXX festlegen) verwenden.

4) Nachdem bei allen Access Points erfolgreich MEKs konfiguriert wurde, kann SPE aktiviert werden.

   Die Access Point Verschlüsselung wird über AMO SIPCO, Parameter **IPDAENCR**, aktiviert:
   `AENDERN-SIPCO:TYP=SECURITY,IPDAENCR=JA;`

IPDAENCR (JA/ NEIN):	Signalisierungs- und Sprachverschlüsselung für IPDA-Verbindungen.

   Wurden nicht für alle Access Points MEKs konfiguriert, schlägt die SPE-Aktivierung bei den Access Points fehl (siehe Punkt 1 bis 3).

5) Nach der Aktivierung von Security im AMO SIPCO muss ein Hard-Restart des Systems erfolgen.

Wichtig: Bei einer Duplexanlage müssen Sie den Befehl zum Hard-Restart bei beiden Prozessoren gleichzeitig ausführen. Das bedeutet, dass alle LTUs und APs neu gestartet werden!
`EXEC-REST:TYP=MODUL,MODUL=BP,RSLEVEL=HARD;`

---

1) **Ausnahme**

   Ein Soft-Restart ist ausreichend, wenn

   - keine Common Gateways im Access Point vorhanden sind
   - im Zugangspunkt keine HFA-Teilnehmer existieren
   - nur TDM-Endgeräte im Access Point vorhanden sind
   - Common Gateways im Access Point keine Verschlüsselung benötigen
   - HFA-Teilnehmer im Access Point keine Verschlüsselung benötigen

   Beispiel: Soft-Restart des aktiven BP
   `EXEC-REST:TYP=MODUL,MODUL=BP,RSLEVEL=SOFT;`

2) Wenn Sie Common Gateway-Baugruppen und HFA-Teilnehmer im Zugangspunkt haben und diese im sicheren Modus genutzt werden sollen, müssen Sie alle Schritte ausführen, die erforderlich wären, wenn sich die Common Gateway-Baugruppe und die HFA-Teilnehmer auf dem Host-System befänden (SPE mit AMO ZANDE-Parameter **SPESUPP** aktivieren, Zertifikate importieren etc).

3) Verwandte Themen:

   - Aktivieren/Deaktivieren von SPE bei Trunks
   - Aktivieren/Deaktivieren von SPE bei Endgeräten
   - Verteilung von Zertifikaten an Gateways
   - Verteilung von Zertifikaten mit dem WBM des Gateways
   - Verteilung von Zertifikaten an Teilnehmer

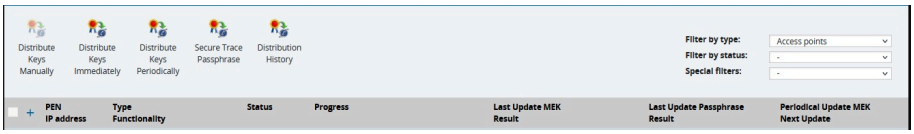
Deaktivierung

Möchte ein Kunde SPE bei den Access Points und den darin befindlichen Common Gateways vollständig deaktivieren, ist hierfür ein Hard-Restart erforderlich.

18.3.5.1 Neuer Access Point in einem aktiven SPE-System

Wenn Sie einen neuen Access Point bei bereits aktivierter Access Point Verschlüsselung hinzufügen müssen, sind folgende Schritte auszuführen:

- Konfigurieren Sie den Access Point im System wie üblich mit AMO UCSU, AMO APRT.
- Schließen Sie den Access Point noch nicht an; dies würde fehlschlagen.
- Verwenden Sie die **SPE-Administration** im OpenScape 4000 Assistant und aktualisieren Sie die Baugruppenliste, um zu überprüfen, ob Ihr neuer Access Point aufgeführt ist.
- **Gateway Manager > SPE >** Abschnitte **Automatische MEK-Verteilung konfigurieren** und **Manual MEK Distribution**



  - Konfigurieren Sie einen MEK für diesen Access Point manuell. Damit wird der MEK an das RMX gesendet.
  - Nutzen Sie die CLI, um denselben MEK auf der NCUI zu konfigurieren.
  - Nun können Sie die Verbindung zwischen Access Point und LAN herstellen und die Verbindung zum System über `EXEC-USSU:MODE=CONFAP,LTU=<ltu_nummer>`; aktivieren.

18.3.5.2 Deaktivieren von SPE bei Access Points mit Soft-Restart

Die Deaktivierung der Access Point-Verschlüsselung (Signalisierung und Payload) erfolgt über AMO SIPCO mit anschließendem Soft-Restart. Bei einer Duplexanlage muss ebenfalls nur **ein** Soft-Restart am aktiven CC durchgeführt werden.

Wichtig: Das Deaktivieren der Access Point-Verschlüsselung führt dazu, dass jeder Ruf und die entsprechenden DMC-Verbindungen mit Access Point-Bezug (Teilnehmer oder Trunk im AP-Shelf) aus Ende-zu-Ende-Sicht als Standard-Ruf ausgeführt und signalisiert wird. Die Verbindungen zwischen der STMI-Baugruppe im AP-Shelf und den HFA-Teilnehmern oder dem Partner-Gateway bleiben jedoch verschlüsselt, d.h. TLS-Teilnehmer werden weiterhin auf TLS in AP-Shelves ausgeführt und Trunking-Gateways mit bereits hergestellter TLS-Verbindung nutzen weiterhin TLS-Verbindungen.

SPE aktivieren

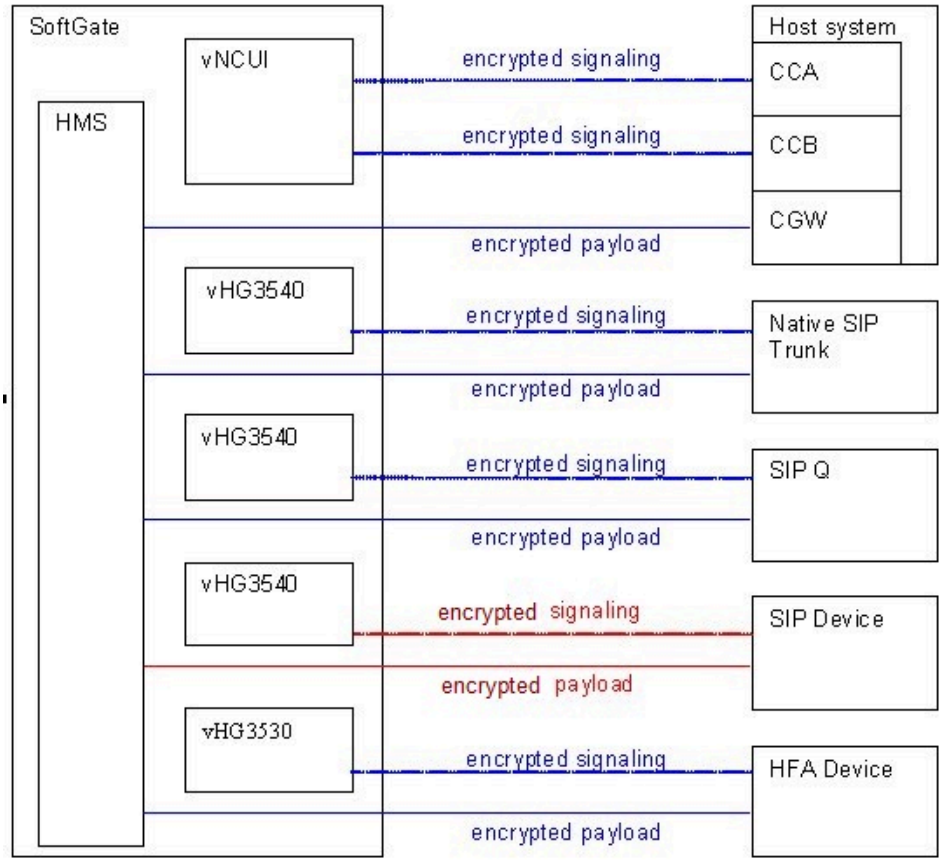
Analog zur Deaktivierung, AMO SIPCO und Soft-Restart.

Hinweis

Beim Ein-/Ausschalten von SPE fordert der AMO SIPCO den Administrator auf, einen Hard-Restart einzuleiten. Dieser Hinweis wird aus den folgenden Gründen nicht abgeändert:

- Wenn SPE im System bereits bei HFA-Endgeräten und IP-Trunking aktiviert ist und die Access Point-Verschlüsselung erstmals aktiviert wird, muss ein Hard-Restart durchgeführt werden, damit das Leistungsmerkmal korrekt funktioniert.
- Möchte ein Kunde SPE bei Access Point und den darin befindlichen Common Gateways vollständig deaktivieren, ist hierfür ein Hard-Restart erforderlich.

18.3.6 Aktivieren/Deaktivieren von SPE bei OpenScape 4000 SoftGate



OpenScape 4000 SoftGate und SPE - Überblick

18.3.6.1 Leistungsmerkmale

- Die Signalisierungsverbindung zwischen OpenScape 4000 SoftGate und zentraler Steuerung im Hostsystem ist verschlüsselt.
- Sprachverbindungen vom OpenScape 4000 SoftGate zur HG 3570 im Hostsystem oder zu einem anderen OpenScape 4000 SoftGate oder zu AP-Shelves sind verschlüsselt.
- Eine Signalisierungs- und Sprachverschlüsselung wird auch für SIP-Trunking- und HFA/SIP-Teilnehmer unterstützt.

18.3.6.2 Einschränkungen

- Ist im Hostsystem SPE aktiviert und dem OpenScape 4000 SoftGate ist kein Default-MEK zugewiesen, geht das OpenScape 4000 SoftGate nicht in Betrieb.
- Das Tracen von HFA-Signalisierung ist am OpenScape 4000 SoftGate nicht möglich!

18.3.6.3 Konfiguration

Um am OpenScape 4000 SoftGate Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption = **SPE**) verwenden zu können, muss wie beim herkömmlichen Access Point (AP) der **M**aster **E**ncryption **K**ey (**MEK**) konfiguriert werden. Bei einem herkömmlichen Access Point erfolgt dies über das **C**ommand **L**ine **I**nterface (**CLI**). Da das OpenScape 4000 SoftGate kein CLI besitzt, ist hier das Vorgehen etwas anders.

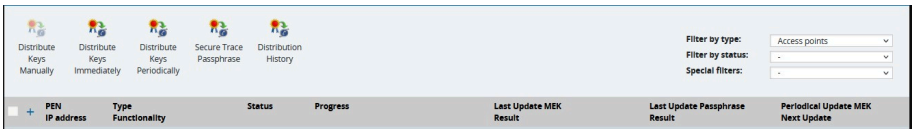
18.3.6.3.1 Szenario 1: OpenScape 4000 SoftGate soll an einem Hostsystem mit bereits aktiviertem SPE angeschaltet werden

Wichtig: Reihenfolge beachten!

Wichtig: Schalten Sie das OpenScape 4000 SoftGate noch nicht an. Dies würde fehlschlagen!

1) Verwenden Sie die SPE-Verwaltung in OpenScape 4000 Assistant und aktualisieren Sie die Baugruppenliste, um zu überprüfen, ob Ihr OpenScape 4000 SoftGate aufgeführt ist.

   Gateway Manager > SPE > Abschnitte **Automatische MEK-Verteilung konfigurieren** und **Manual MEK Distribution**



2) Konfigurieren Sie einen MEK für dieses OpenScape 4000 SoftGate **manuell**. Damit wird der MEK an das RMX gesendet.

   Experten Modus > Signaling & Payload Encryption > Administration > Bereiche **Konfiguration Automatische MEK Verteilung** und **Manuelle MEK Verteilung**

   Weitere Informationen über die MEK-Administration finden Sie im Administratorhandbuch „OpenScape 4000 Assistant V, Signaling & Payload Encryption“ (http://apps.g-dms.com:8081/techdoc/en/P31003H340M1440176A9/index.htm).

3) Nutzen Sie die „OpenScape 4000 Plattform Aministration (Portal)“ um den MEK zu konfigurieren.

   Wichtig: Wenn SPE im System bereits aktiviert ist, kann sich das OpenScape 4000 SoftGate erst dann verbinden, wenn es den korrekten MEK besitzt. WBM (für die Verteilung des MEK)

kann erst dann benutzt werden, wenn sich das OpenScape 4000 SoftGate erfolgreich mit dem Hostsystem verbunden hat.

---

1) Nun kann das OpenScape 4000 SoftGate eingeschaltet werden.

18.3.6.3.2 Szenario 2: OpenScape 4000 SoftGate und Hostsystem haben SPE noch nicht aktiviert

Folgende Schritte sind auszuführen, um SPE beim OpenScape 4000 SoftGate zu aktivieren.

Wichtig: Reihenfolge beachten!

---

1) Reihenfolge beachten! Schalten Sie das Hostsystem an und schalten Sie alle im System befindlichen OpenScape 4000 SoftGates an.

2) Verteilen Sie den **M**aster **E**ncryption **K**ey (**MEK**) über OpenScape 4000 Assistant an **alle** im System konfigurierten OpenScape 4000 SoftGates. Damit wird

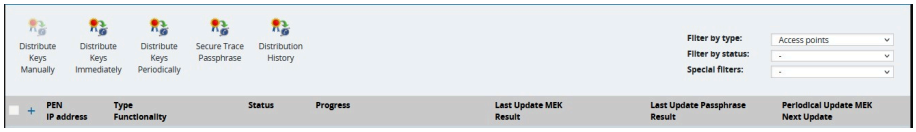
Damit wird

- in RMX der MEK bei allen OpenScape 4000 SoftGate konfiguriert, und
- der MEK an alle OpenScape 4000 SoftGates gesendet.

Der MEK muss zuerst auf den vNCUI-Baugruppen und dann im Hostsystem konfiguriert werden.

Der MEK wird über den OpenScape 4000 Assistant konfiguriert:

Gateway Manager > SPE > Abschnitte **Automatische MEK-Verteilung konfigurieren** und **Manual MEK Distribution**



Weitere Informationen über die MEK-Administration finden Sie im Administratorhandbuch „OpenScape 4000 Assistant V, Signaling & Payload Encryption“ (http://apps.g-dms.com:8081/techdoc/en/P31003H340M1440176A9/index.htm).

3) Überprüfen Sie das Protokoll des MEK-Clients auf etwaige OpenScape 4000 SoftGate-Fehler.

Experten Modus > Signaling & Payload Encryption > Administration > MEK- / Passphrase Verteilung Protokoll

4) Nachdem bei allen OpenScape 4000 SoftGates erfolgreich MEKs konfiguriert wurden, können Sie SPE aktivieren.

Die IPDA-Verschlüsselung wird über AMO SIPCO, Parameter **IPDAENCR**, aktiviert:
`AENDERN-SIPCO:TYP=SECURITY,IPDAENCR=JA;`

IPDAENCR (JA/ NEIN):	Signalisierungs- und Sprachverschlüsselung für IPDA-Verbindungen.

Wichtig: Wurden nicht für alle OpenScape 4000 SoftGates MEKs konfiguriert (siehe Punkt 1 bis 3), schlägt die SPE-Aktivierung bei OpenScape 4000 SoftGate fehl.

18.4 Generieren von SPE-Zertifikaten mit OpenScape 4000 Assistant

Der Bereich SPE SSL Certificate Management des OpenScape 4000 Assistant beinhaltet die Funktionen zur Verwaltung der SSL-Sicherheitszertifikate für die Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)). Er enthält die Werkzeuge zum Generieren des SSL Root-Zertifikats (CA) und des PKCS#12-Zertifikats, das durch das für die SPE-Funktion geeignete Root-Zertifikat signiert wird.

Zum Starten der Anwendung wählen Sie im OpenScape 4000 Assistant die Option **Expert Mode > Signaling & Payload Encryption**.

18.4.1 SPE Root-Zertifikat

Mit dieser Funktion können Sie Ihr eigenes Root-Zertifikat erstellen, das dazu dient, alle von der SPE-Zertifikatfunktion generierten SPE-Zertifikate zu signieren und direkt von der Benutzeroberfläche aus herunterzuladen.

Der Zweck dieser Funktion ist es, alle SPE-Zertifikate in einem HiPath 4000-/ OpenScape 4000-Netzwerk von nur einem Root-Zertifikat (CA) signieren zu lassen.

Ein Root-Zertifikat ist ein spezieller selbstsignierter Zertifikatstyp.

Der Unterschied zwischen einem selbstsignierten Zertifikat und einem Root-Zertifikat besteht darin, dass Sie bei einem selbstsignierten Zertifikat den Servernamen, beim Root-Zertifikat hingegen einen Namen für das Root-Zertifikat (CA) angeben müssen. Der Name des Root-Zertifikats verweist nicht auf einen bestimmten Server.

Der Hauptunterschied besteht darin, dass ein Stammzertifikat ein CA-Zertifikat ist, mit dem andere Zertifikate signiert werden können.

18.4.1.1 Öffnen des Dialogs „SPE Root Certificate“

Wählen Sie auf der Startseite des OpenScape 4000 Assistant die Option **Expert Mode > Signaling and Payload Encryption > SPE Root Certificate**. Der Dialog „SPE Root Certificate“ wird geöffnet.

Zwei Fälle sind möglich:

- Das Root-Zertifikat existiert noch nicht.
- Wenn noch kein Root-Zertifikat erstellt wurde, enthält der Root Certificate-Dialog keine Einträge.
- Das Root-Zertifikat existiert bereits.
- Wenn auf diesem Server bereits ein Root-Zertifikat erstellt wurde, werden die Daten des vorhandenen Zertifikats zusammen mit einem entsprechenden Hinweis im Dialog „Root Certificate“ des Browsers angezeigt.

18.4.1.2 Neues Stammzertifikat erzeugen

Navigieren Sie in der OpenScape 4000 Assistant-Startseite zum **Expertenmodus > Signalisierung und Nutzlast-Verschlüsselung > SPE-Stammzertifikat**. Das Dialogfeld SPE-Stammzertifikat wird geöffnet.

Es gibt zwei Fälle, die unterschieden werden müssen:

- Kein SPE-Stammzertifikat existiert
- Wenn noch kein SPE-Stammzertifikat erstellt wurde, wird das Dialogfeld zum Erstellen eines SPE-Stammzertifikats mit leeren Feldern angezeigt.

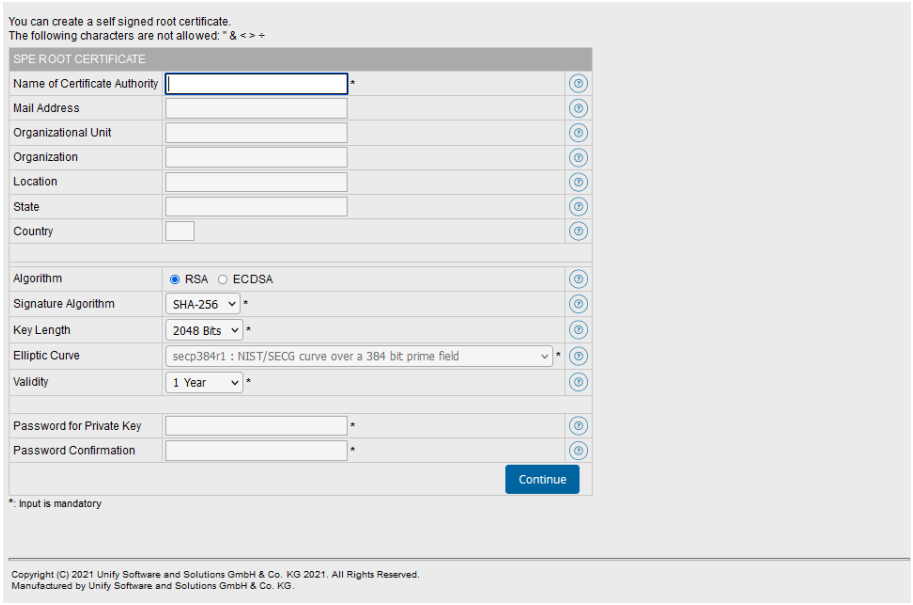


Abbildung 327: Generierung von SPE-Stammzertifikaten (kein SPE-Stammzertifikat existiert)

- Ein SPE-Stammzertifikat bereits existiert
- Wenn bereits ein SPE-Stammzertifikat erstellt wurde, klicken Sie auf die Schaltfläche **Neues Stammzertifikat**, um ein neues SPE-Stammzertifikat zu erstellen. Es öffnet sich ein neues Dialogfeld. Die Daten des bestehenden SPE-Stammzertifikats werden in den Eingabefeldern angezeigt und können für das neue SPE-Stammzertifikat entsprechend geändert werden.

Wichtig: Wenn Sie ein neues SPE-Stammzertifikat erstellen, obwohl für diesen Server bereits ein SPE-

Stammzertifikat existiert, wird das bestehende SPE-Stammzertifikat überschrieben.

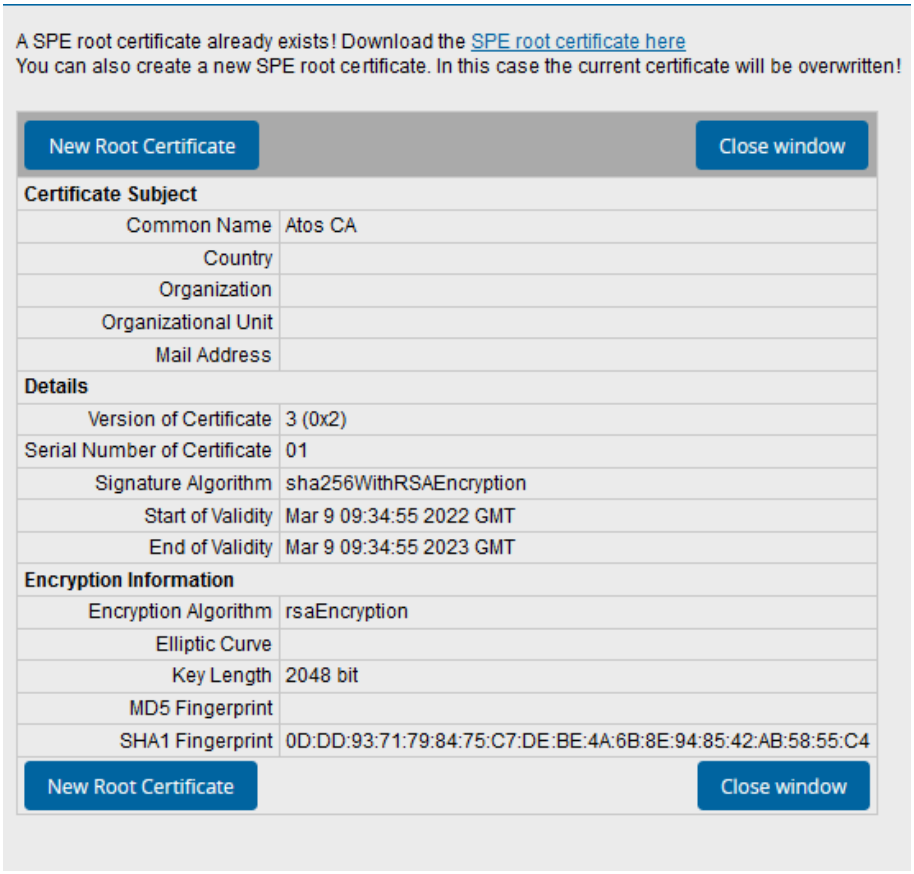


Abbildung 328: Generierung von SPE-Stammzertifikaten mit bestehendem SPE-Stammzertifikat

Prozedur

1) Geben Sie alle erforderlichen Daten ein. Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet. Die folgenden Zeichen sind in den Eingabefeldern nicht zulässig: " & < > ÷ sowie Akzent- und Sonderzeichen.
2) Um zusätzliche Kontextinformationen zu den einzelnen Eingabefeldern zu erhalten, klicken Sie auf das Symbol **?** rechts neben dem jeweiligen Eingabefeld. Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.
3) Klicken Sie auf **Weiter**. Das SPE-Stammzertifikat wird generiert. Nach der Erstellung des Zertifikats wird dieses angezeigt und kann über einen Link heruntergeladen werden.
4) Wenn Sie ein SPE-Zertifikat basierend auf dem ECDSA-Signaturalgorithmus erstellen, stellen Sie bitte sicher, dass alle Endpunkte ECDSA unterstützen.

   Beispielsweise unterstützen HG3500- und STMI2/4-Platinen sie nicht.

18.4.1.3 Anzeigen/Herunterladen des neuen SPE Root-Zertifikats

Wählen Sie auf der Startseite des OpenScape 4000 Assistant die Option **Expert Mode > Signaling and Payload Encryption > SPE Root Certificate**. Der Dialog „SPE Root Certificate“ wird geöffnet.

Wenn bereits ein SPE Root-Zertifikat existiert, wird es angezeigt und kann durch Klicken auf den Link **SPE Root Certificate here** heruntergeladen werden.

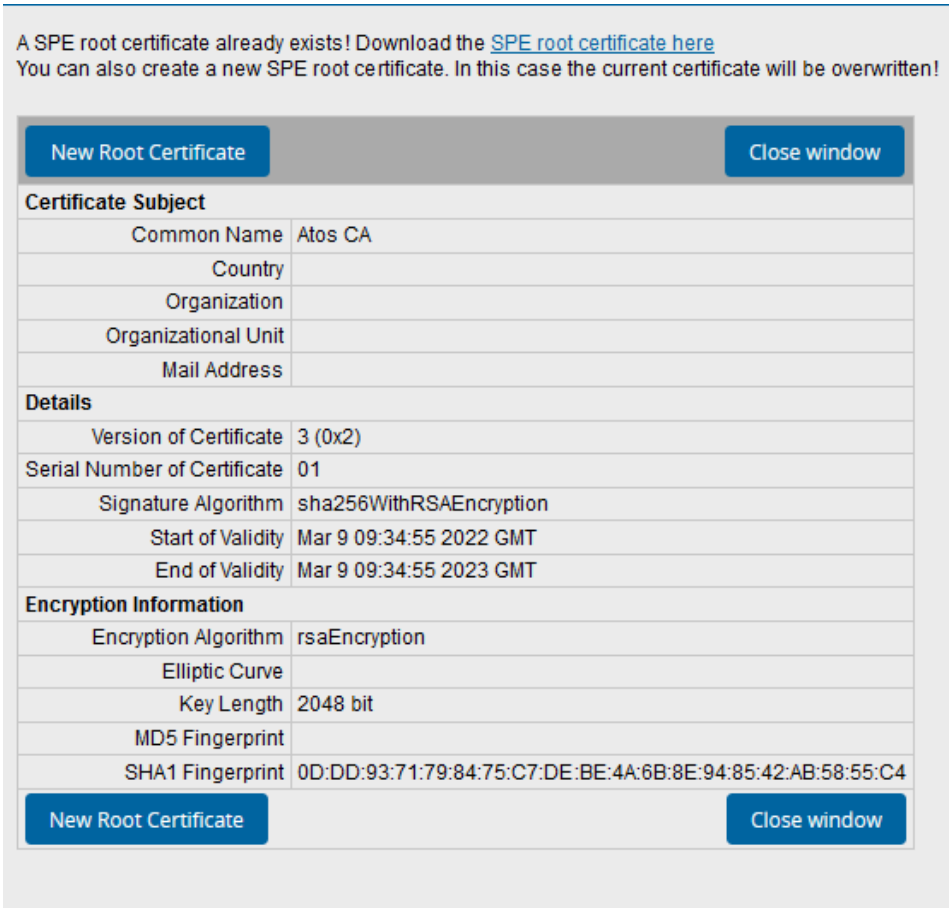


Abbildung 329: SPE Root-Zertifikat herunterladen

18.4.2 SPE-Zertifikat

Die Funktion **SPE Certificate** stellt die Methode zum Erstellen eines neuen SSL-Zertifikats und zum Signieren dieses Zertifikats durch das SPE Root-Zertifikat bereit. Die mit dieser Funktion erstellten Zertifikate werden immer durch das im Dialog **SPE Root Certificate** erstellte Zertifikat signiert (siehe Abschnitt 5.1, „SPE Root-Zertifikat“).

18.4.2.1 Öffnen des Dialogs „SPE Certificate“

Wählen Sie auf der Startseite des OpenScape 4000 Assistant die Option **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. Der Dialog „SPE Certificate“ wird geöffnet.

Drei Fälle sind möglich:

- Das Zertifikat existiert noch nicht.
- Wenn noch kein Zertifikat erstellt wurde, enthält der Certificate-Dialog keine Einträge.
- Das Zertifikat existiert bereits.
- Wenn auf diesem Server bereits ein Zertifikat erstellt wurde, werden die Daten des vorhandenen Zertifikats zusammen mit einem entsprechenden Hinweis im Dialog „Certificate“ des Browsers angezeigt.
- Das Root-Zertifikat existiert noch nicht.
- Wenn noch kein Root-Zertifikat erstellt wurde, wird der Benutzer aufgefordert, zuerst das Root-Zertifikat zu erstellen.

18.4.2.2 Erstellen eines neuen SPE-Zertifikats

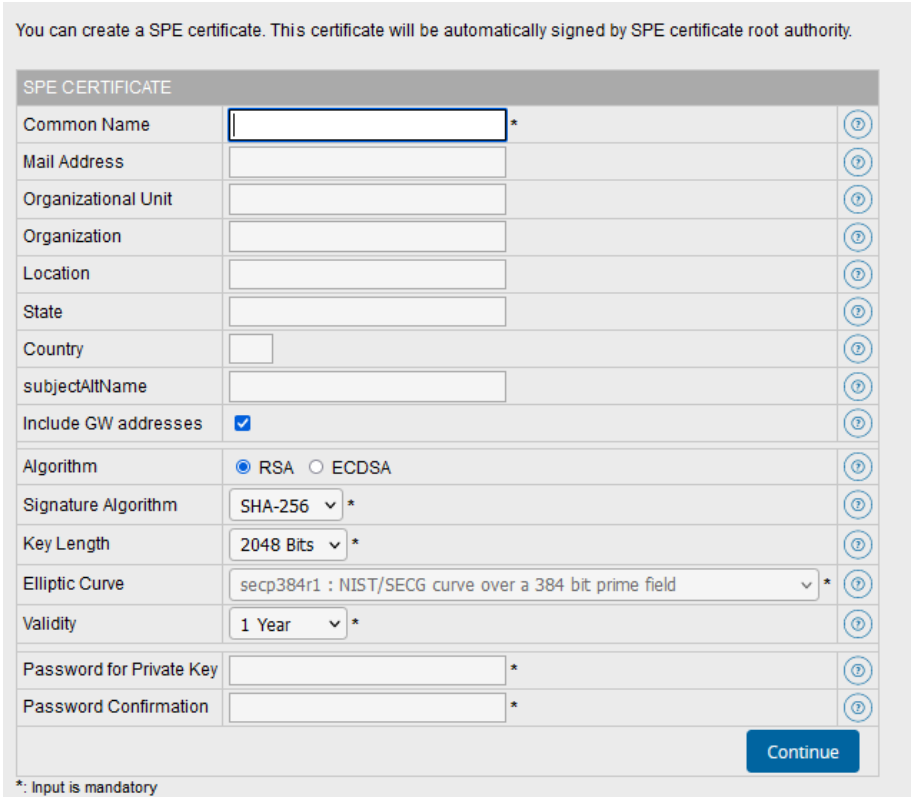
Wählen Sie auf der Startseite des OpenScape 4000 Assistant die Option **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. Der Dialog „SPE Certificate“ wird geöffnet.

Es sind zwei Fälle zu unterscheiden:

- Es existiert kein SPE-Zertifikat.

- Wenn noch kein SPE-Zertifikat erstellt wurde, wird der Dialog zum Erstellen des SPE-Zertifikats mit leeren Feldern angezeigt.

  Abbildung 330: SPE-Zertifikat generieren (es existiert kein SPE-Zertifikat)



- Es existiert bereits ein SPE-Zertifikat.

  Wenn bereits ein SPE-Zertifikat erstellt wurde, klicken Sie auf die Schaltfläche **New SPE Certificate**, um ein neues SPE-Zertifikat zu erstellen. Ein neuer Dialog wird geöffnet. Die Daten des vorhandenen SPE-Zertifikats

werden in den Eingabefeldern angezeigt und können entsprechend dem neuen SPE-Zertifikat geändert werden.

Wichtig: Wenn Sie ein neues SPE-Zertifikat erstellen, obwohl auf diesem Server bereits ein SPE-Zertifikat existiert, wird das vorhandene SPE-Zertifikat überschrieben.

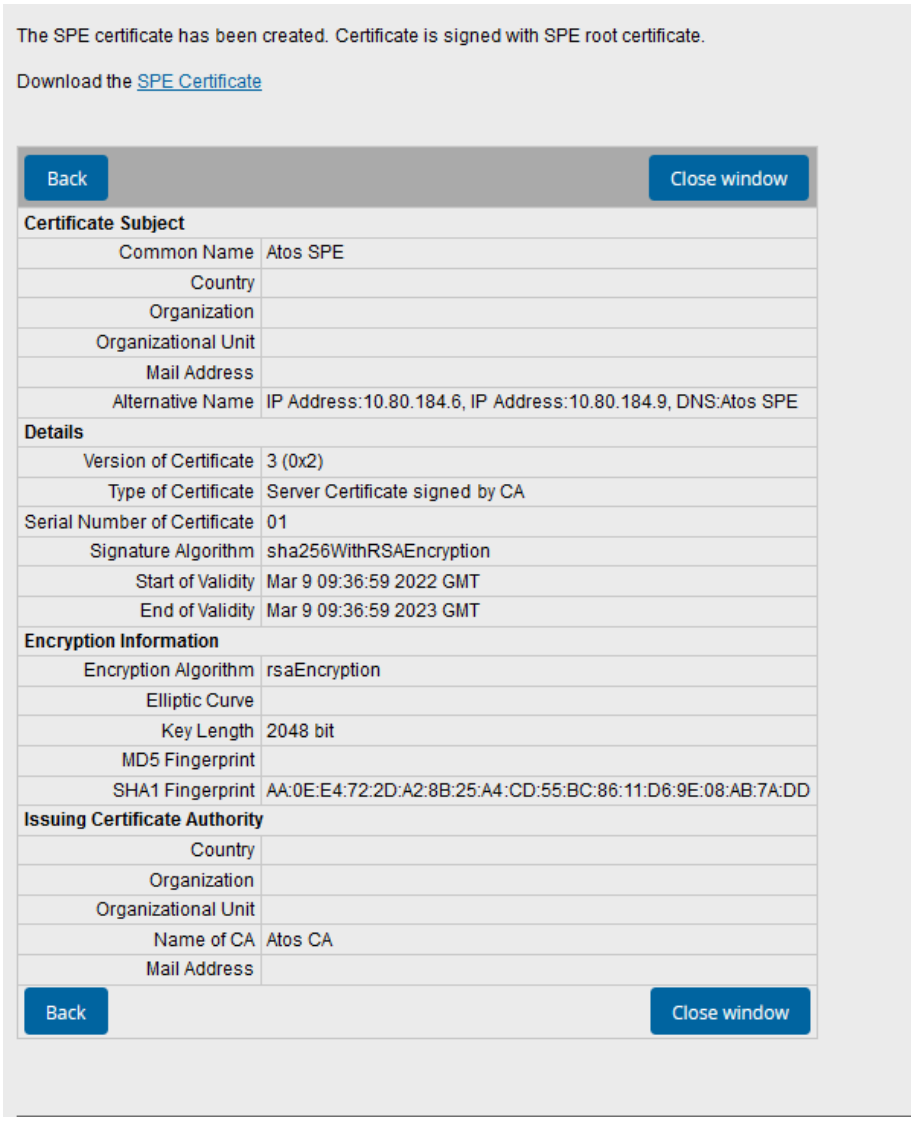


Abbildung 331: SPE-Zertifikat generieren (es existiert bereits ein SPE-Zertifikat)

Vorgehensweise

1) Geben Sie alle benötigten Daten ein. Erforderliche Felder sind mit einem roten Stern (*) gekennzeichnet. Folgende Zeichen sind in den Eingabefeldern nicht zulässig: " & < > Ã· sowie Sonderzeichen und Akzentbuchstaben.
2) Wenn Sie weitere Kontextinformationen zu einem der Eingabefelder benötigen, klicken Sie auf das Fragezeichensymbol (?) rechts neben dem betreffenden Feld. Die kontextspezifischen Informationen zu diesem Feld werden als Tooltip im Browser angezeigt.

3) Klicken Sie auf **Continue**. Das SPE-Zertifikat wird generiert. Das erzeugte Zertifikat wird angezeigt und kann über einen Link heruntergeladen werden.

18.4.2.3 Anzeigen/Herunterladen des neuen SPE-Zertifikats

Wählen Sie auf der Startseite des OpenScape 4000 Assistant die Option **Expert Mode > Signaling and Payload Encryption > SPE Certificate**. Der Dialog „SPE Certificate" wird geöffnet.

Wenn bereits ein SPE-Zertifikat existiert, wird es angezeigt und kann durch Klicken auf den Link **SPE Certificate** heruntergeladen werden.

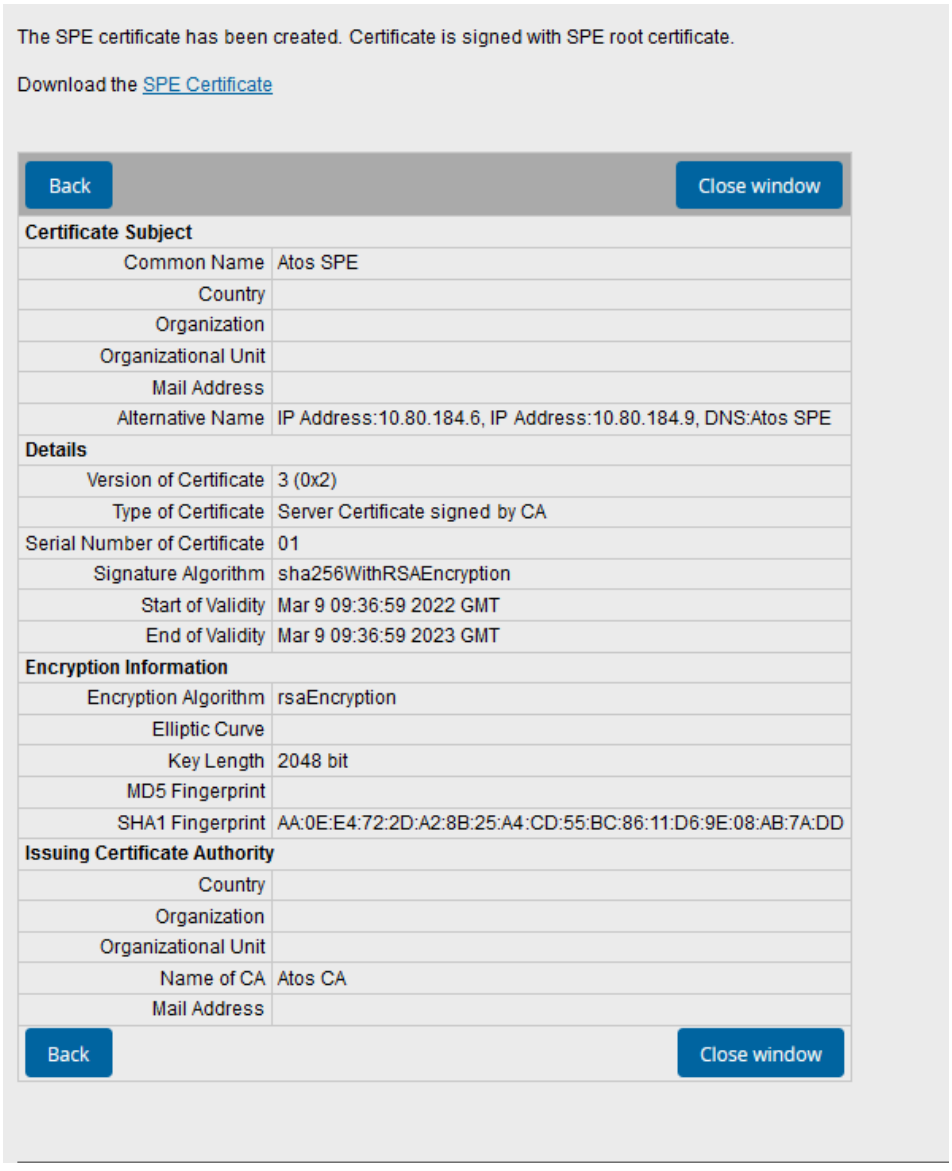


Abbildung 332: SPE-Zertifikat anzeigen/herunterladen

18.5 Verteilung von Zertifikaten mit dem WBM des Gateways

Dieses Kapitel soll lediglich einen kurzen Überblick über die notwendigen Schritte im WBM vermitteln.

Eine genaue Beschreibung finden Sie im Administratorhandbuch des WBM.

- HG 3500 (und HG 3575)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1000176A9/index.htm
- vHG 3500 HFA (für HFA-Teilnehmer)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1020176A9/index.htm
- vHG 3500 SIP (für SIP-Trunking und SIP-Teilnehmer)
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1030176A9/index.htm
- vHG 3575
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1030176A9/index.htm
- HG 3500 auf STMIX
- http://apps.g-dms.com:8081/techdoc/en/P31003H3180M1050176A9/index.htm

  Certificates can be imported directly via WBM (Web-Based Management) on the gateway in any case, even if DLS is not available in the customer network.

  WBM ist über HiPath 4000 Assistant zugänglich: **Expertenmodus | Gateway Dashboard**

18.5.1 SPE CA-Zertifikat für SIP-Trunking importieren

Configuration > **Security** > **Signaling- und Payload-Encryption (SPE) > SPE CA-Zertifikate** > **Vertrauenswürdiges CA-Zertifikat importieren (PEM oder binär)**

Der Dialog **Laden eines SPE CA-Zertifikats über HTTP** wird angezeigt. Suchen Sie das Zertifikat. Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**. Importieren Sie das Zertifikat nun, indem Sie auf die Schaltfläche **Zertifikat aus Datei importieren** klicken.

War der Importvorgang erfolgreich, wird eine entsprechende Meldung ausgegeben.

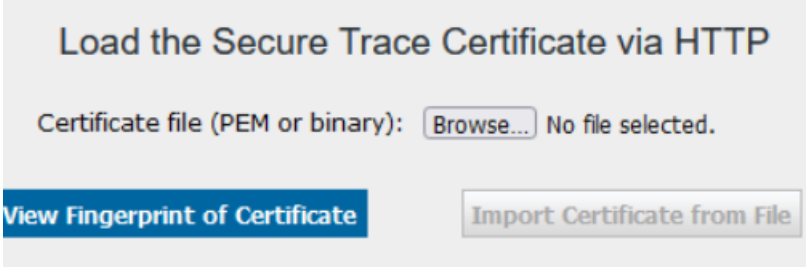


Abbildung 333: Importieren eines SPE CA-Zertifikats auf einem Gateway

18.5.2 Importieren eines SPE-Zertifikats auf einem Gateway

Wichtig: Hinweis zu vHG3500 HFA finden Sie unter Abschnitt 7.3, „Importieren eines SPE-Zertifikats auf einem vHG3500 HFA“**.**

Configuration > Security > Signaling- und Payload-Encryption (SPE) > SPE Zertifikat > Vertrauenswürdiges SPE-Zertifikat importieren (PEM bzw. PKCS#12)

Der Dialog **Laden eines SPE-Schlüsselzertifikates über HTTP** wird angezeigt. Geben Sie die Passphrase (vertrauliches Kennwort (siehe Abschnitt 4.3, „Konfiguration“)) ein, und suchen Sie dann das Zertifikat. Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**. Importieren Sie das Zertifikat nun, indem Sie auf die Schaltfläche **Zertifikat aus Datei importieren** klicken.

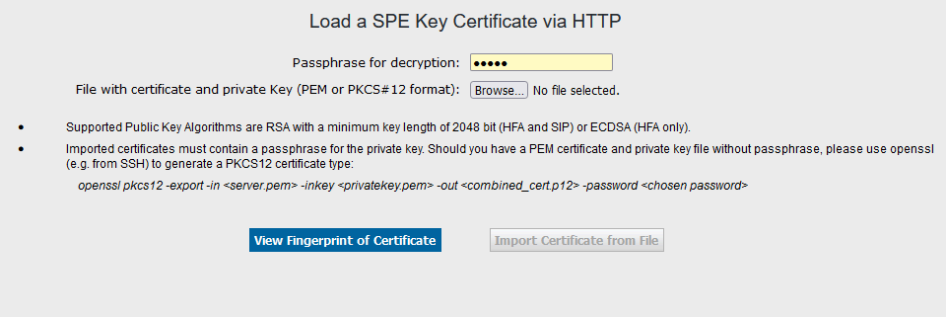


Abbildung 334: Importieren eines SPE-Zertifikats auf einem Gateway

18.5.3 Importieren eines SPE-Zertifikats auf einem vHG3500 HFA

Wichtig: Nur möglich für vHG 3500 HFA!

Konfiguration > SPE > Keycert importieren

Der Dialog **Laden eines SPE-Key-Zertifikats über HTTP** wird angezeigt:

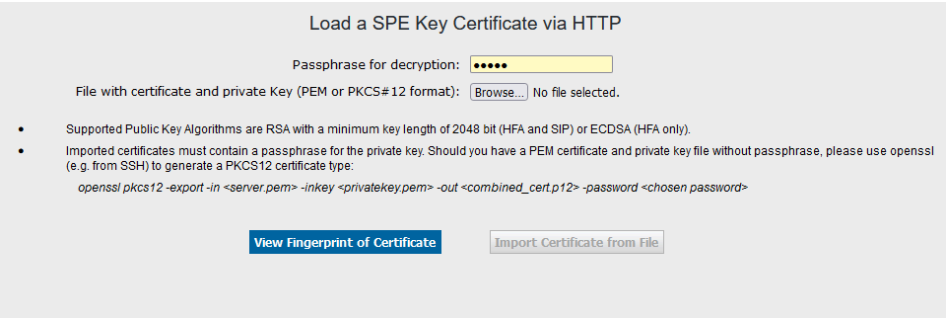


Abbildung 335: Importieren eines SPE-Zertifikats für HFA-Teilnehmer auf einem vHG 3500

In diesem Dialog kann nach Eingabe des Entschlüsselungspassworts und des Dateinamens ein SPE-Schlüsselzertifikat importiert werden. Die Datei mit dem Zertifikat stammt von einer vom Kunden festgelegten PKI-Zertifizierungsstelle

(RA/CA) oder der internen Zertifizierungsstelle des DLS-Servers (CA) und muss im PEM- oder PKCS#12-Format vorliegen.

18.5.4 Zertifikate und Sicherheit an vHFA- und WAN-Schnittstellen

vHFA

Das mit dem vHFA WBM konfigurierte SPE-Zertifikat wird für die TLS-Verbindung zu seiner IP-Adresse verwendet.

- TLS -Ports auf vHFA werden nur geöffnet, wenn SPE aktiviert und Zertifikate geladen sind (alles auf vHFA funktioniert wie vor der WAN-Einführung)
- Das SPE-Zertifikat auf vHFA wird nur für „lokale“ Verbindungen verwendet.
- Wenn SPE deaktiviert ist oder TLS für lokale Verbindungen nicht benötigt wird, ist auf vHFA kein SPE-Zertifikat erforderlich.

WAN-Schnittstelle

Das mit dem OpenScape 4000 SoftGate WBM konfigurierte SPE-Zertifikat wird für die TLS-Verbindung zu seiner WAN IP-Adresse verwendet.

- Für WAN-Verbindungen wird unabhängig von den Sicherheitseinstellungen grundsätzlich SRTP verwendet
- Unabhängig davon, ob SPE aktiviert ist, sind TLS WAN-Ports geöffnet, wenn das Zertifikat konfiguriert ist.
- Die WAN-Schnittstelle erfordert ein SPE-Zertifikat, da im WAN nur TLS zulässig ist.
- Die WAN-Schnittstelle verwendet unabhängig von den SPE-Einstellungen immer TLS und SRTP.
- Wenn SPE aktiviert ist, wird das Telefon im WAN dem System gegenüber als TLS-gesicherter Apparat ausgewiesen.
- Wenn SPE deaktiviert ist, wird das Telefon im WAN dem System gegenüber als nicht TLS-gesicherter Apparat ausgewiesen (unabhängig davon, ob es TLS verwendet).
- Wenn SPE deaktiviert ist, arbeitet die mobile HFA zwischen dem WAN und lokalen Schnittstellen mit TCP auf lokalen Verbindungen und TLS auf WAN-Verbindungen.
- Wenn SPE aktiviert und die mobile HFA für einen bestimmten Teilnehmer erforderlich ist, muss dieser Teilnehmer auch auf der lokalen Verbindung TLS verwenden (andernfalls kann die mobile HFA vom WAN auf dem lokalen Telefon nicht abgebrochen werden, weil TCP TLS nicht außer Kraft setzen kann).

18.6 Deployment Service (DLS)

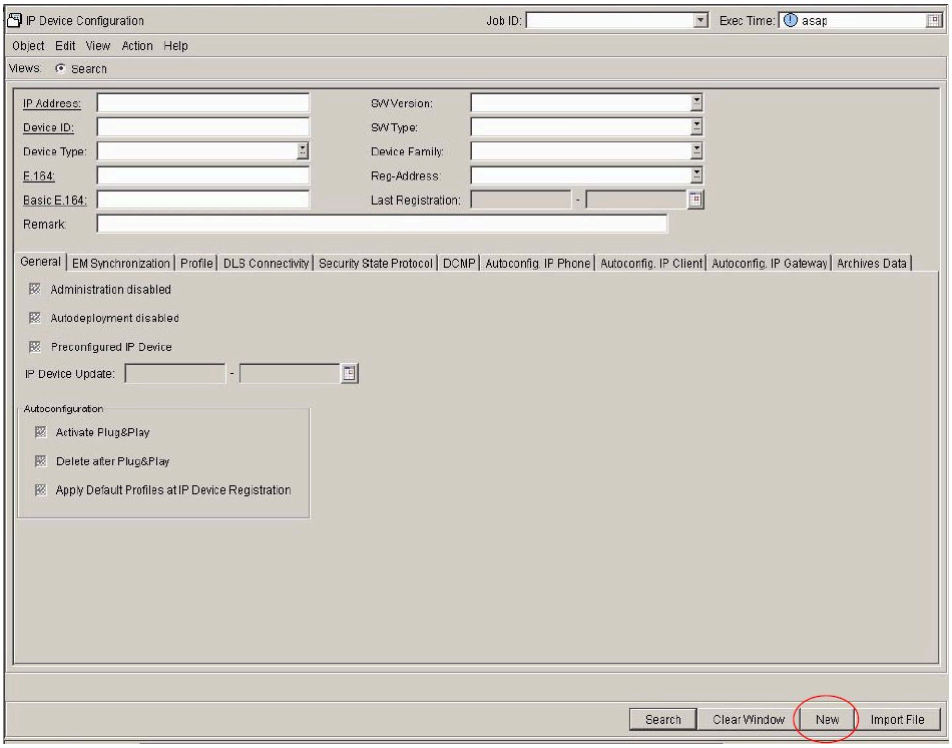
Wichtig: Dieses Kapitel soll nur einen kurzen Überblick über die notwendigen Schritte im Deployment Service (DLS) vermitteln. Eine ausführliche Beschreibung finden Sie im entsprechenden DLS Administrator Handbuch.

18.6.1 Verteilung von Zertifikaten an Gateways

18.6.1.1 Erzeugen eines virtuellen IP Device

IP Devices > IP Device Verwaltung > IP Device Konfiguration

Klicken Sie auf **Neu**, um ein neues virtuelles IP-Gerät zu erzeugen.



Im Bereich allgemeine Daten geben Sie die **Device ID** (IP-Adresse des Gateways) ein und wählen Sie bei **Gerätefamilie** aus der Klappliste **IP-Gateway** aus.

Wählen Sie nun das Register **DLS Verbindung** aus.

Im Abschnitt **DLS Verbindung** geben Sie die **DLS-Server-Adresse** (IP-Adresse des DLS) und den **DLS-Port** (18443) ein.

Diese Angaben müssen mit denen im System konfigurierten Daten übereinstimmen.

Stellen Sie sicher, dass der DLS-Port und die IP-Adresse im System korrekt konfiguriert sind:

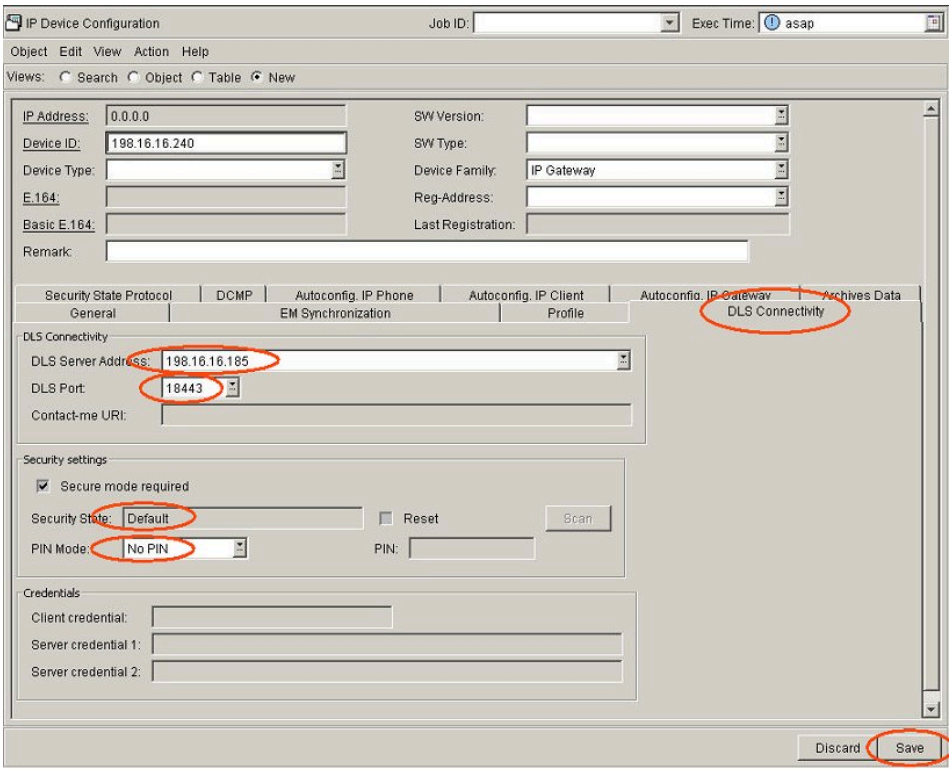
```
AENDERN-
ZANDE:TYP=DLS,DLSIPADR=198.16.16.185,DLSPORT=18443;
```

Stellen Sie außerdem sicher, dass AMO CGWB für die einzelnen Gateways korrekt konfiguriert ist:

```
AENDERN-
CGWB:MTYP=CGW,LTU=1,EBT=4,TYP=DLSDATA,DLSIPADR=198.16.16.185,DL►
SPORT=18443;
```

Im Abschnitt **Security Settings** (Sicherheitseinstellungen) muss das Kontrollkästchen Secure mode required (Sicherer Modus erforderlich) aktiviert

werden. Momentan ist der Sicherheitsstatus im Feld **Security State** auf **Default** (Standard) eingestellt.



Die Kommunikation zwischen DLS und den IP-Geräten (Gateways) ist eine sichere TLS-Verbindung mit den für alle DLS und Gateways festgelegten Standardzertifikaten.

Im Menü **Pin Mode** (Pin-Modus) können Sie zwischen verschiedenen Sicherheitseinstellungen wählen:

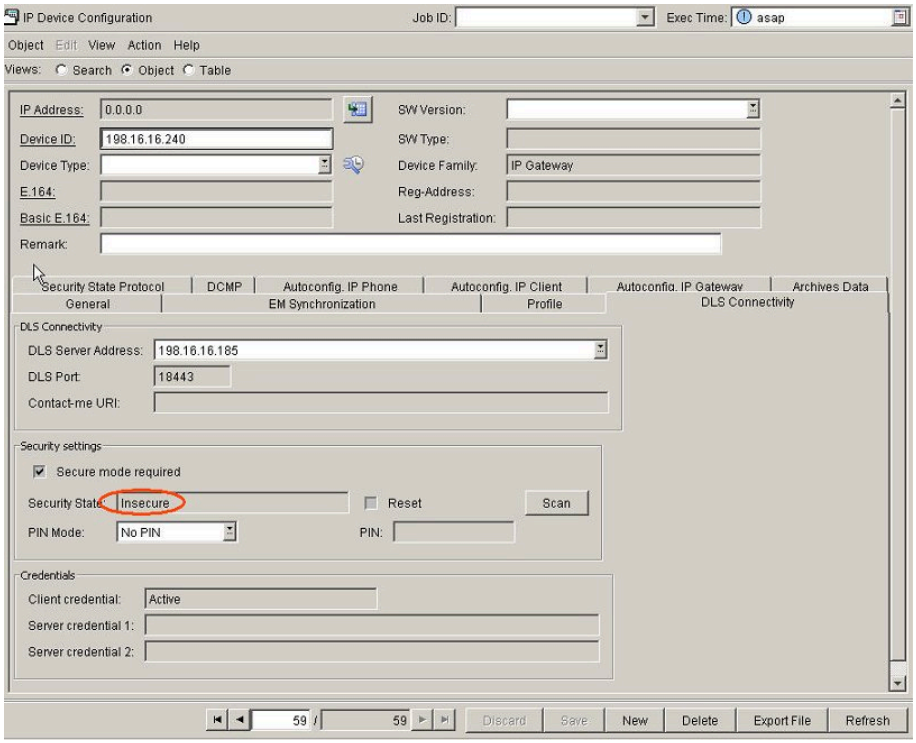
1) Keine PIN

2) Die Zugangsdaten werden mit einem fest codierten Kennwort verschlüsselt an das IP-Gerät gesendet.

   Dieser Modus kann nur verwendet werden, wenn der Parameter **DLSACPAS = NEIN** ist. Überprüfen Sie das mit dem AMO CGWB und ändern Sie wenn nötig.

   ```
   AENDERN-
   CGWB:MTYP=CGW,LTU=1,EBT=14,TYP=DLSDATA,DLSACPAS=NEIN;
   ```

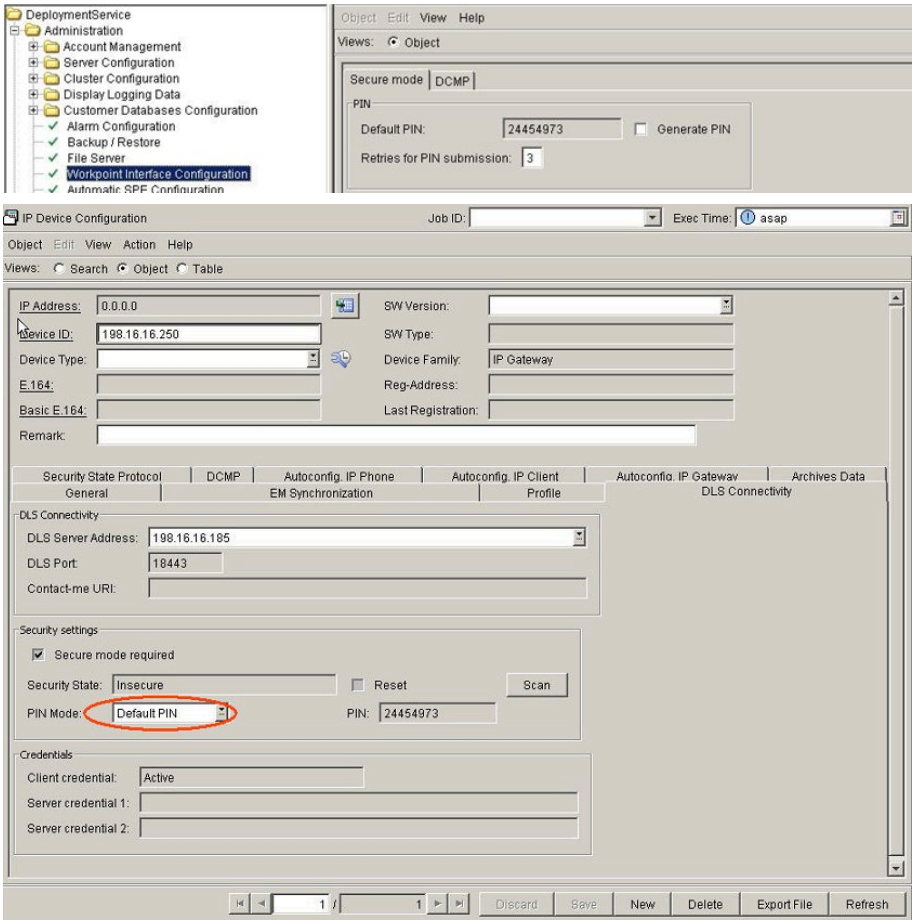
   Nach dem Speichern wird die Einstellung des **Security Status** von **Standard** in **Unsicher** geändert.



3) **Standard-PIN**
4) Diese TLS-Verbindung lässt sich zusätzlich sichern, indem der Inhalt der TLS-Kommunikation außerdem noch mit einer PIN verschlüsselt wird.

   Die Einstellung „Standard-PIN“ bewirkt, dass für jedes Gatewy dieselbe PIN verwendet wird. Unter **Administration > Workpoint Interface**

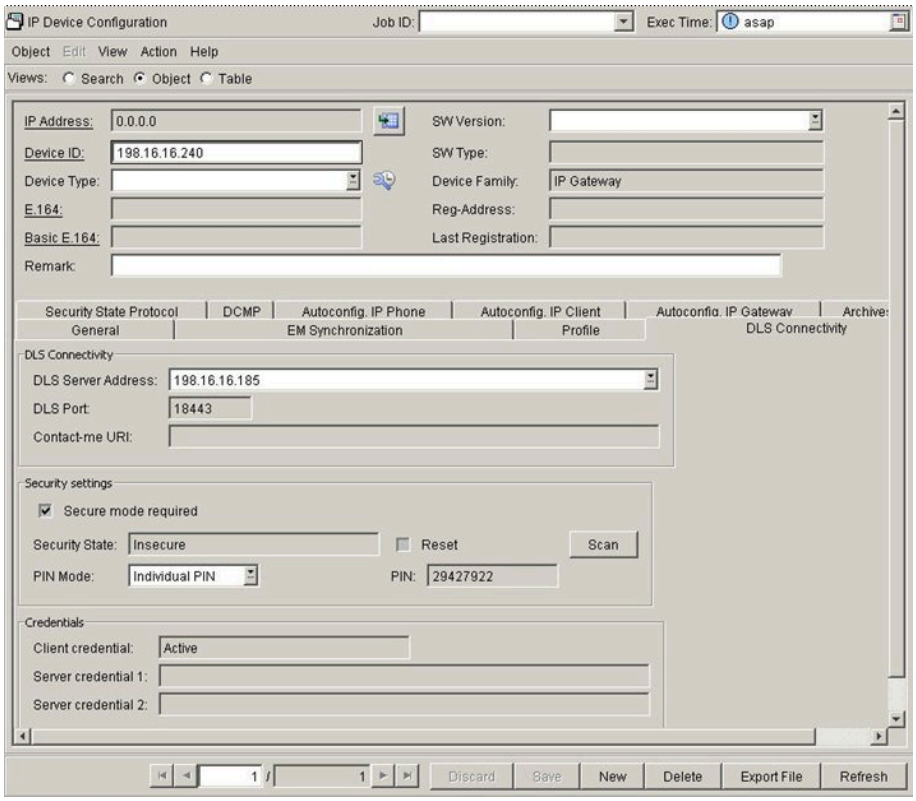
Konfiguration können Sie im Register Secure Modus eine vorhandene, zufällig generierte PIN anzeigen sowie eine neue zufällige PIN generieren.



Nach dem Klicken auf die Schaltfläche **Speichern** können Sie die Standard-PIN anzeigen.

5) **Individuelle PIN**

6) Die Einstellung Individuelle PIN bewirkt, dass für jedes Gateway eine andere PIN verwendet wird.



Wenn Sie auf die Schaltfläche **Speichern** klicken, generiert DLS automatisch zufällige PINs.

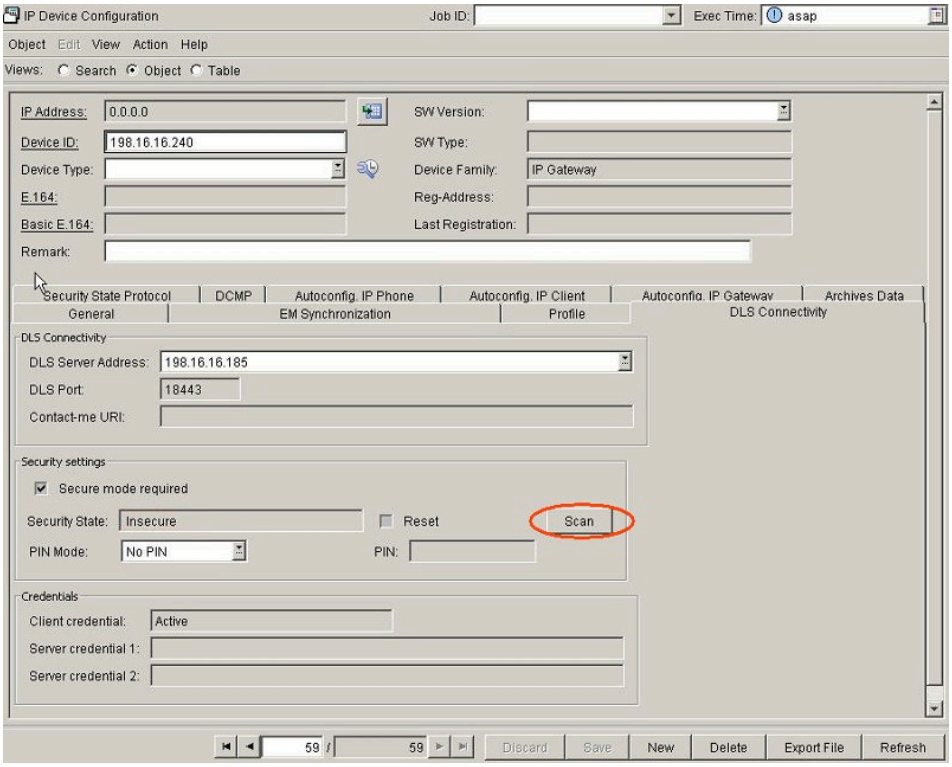
18.6.1.2 Scannen der IP Devices (IP-Gateways)

Bootstrapping: Durch Scannen der IP Devices (Gateways) sendet DLS ein Zertifikat an das Gateway, um eine sichere Verbindung zum Importieren der Kunden-Zertifikate (CA und Zertifikat) vorzubereiten.

Der Scanvorgang ist bei allen verwendeten Modi (Keine PIN, Standard-PIN oder Individuelle PIN) derselbe.

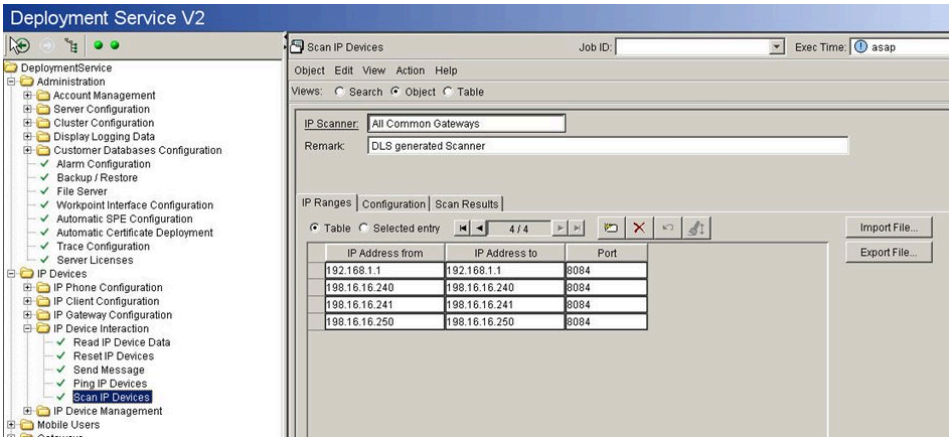
Es gibt 2 Möglichkeiten, den SCAN durchzuführen.

1) Scannen der einzelnen Gateways nacheinander



1) Nachdem Sie auf die Schaltfläche Speichern geklickt haben, um die Konfiguration zu speichern können Sie mit der **Scan**-Schaltfläche den Scanvorgang des konfigurierten Gateway starten.

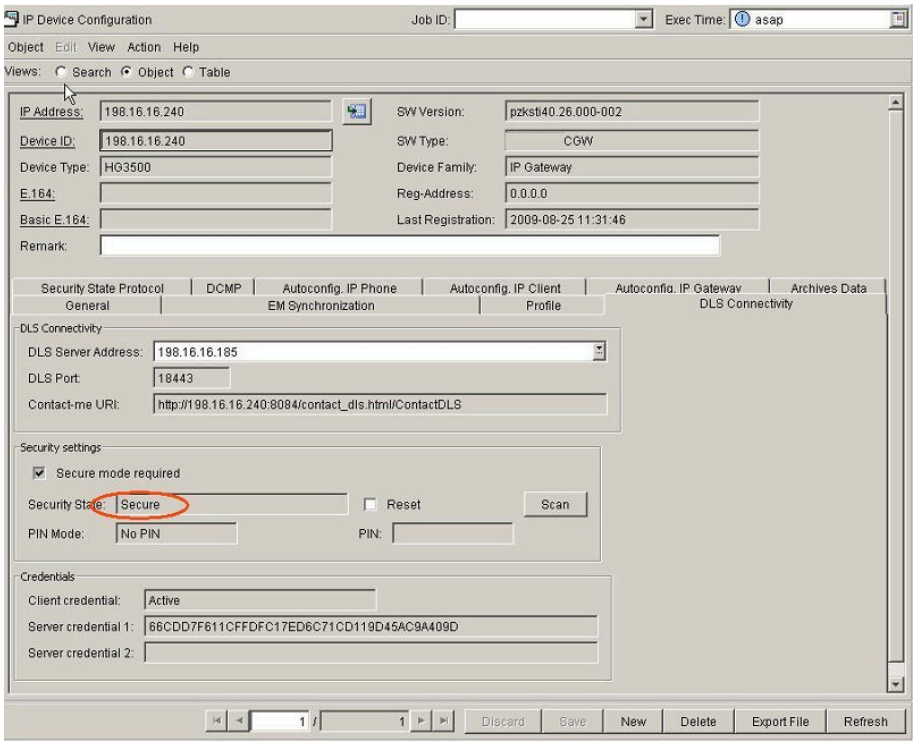
2) Scannen einer Gruppe von Gateways in einem Arbeitsgang



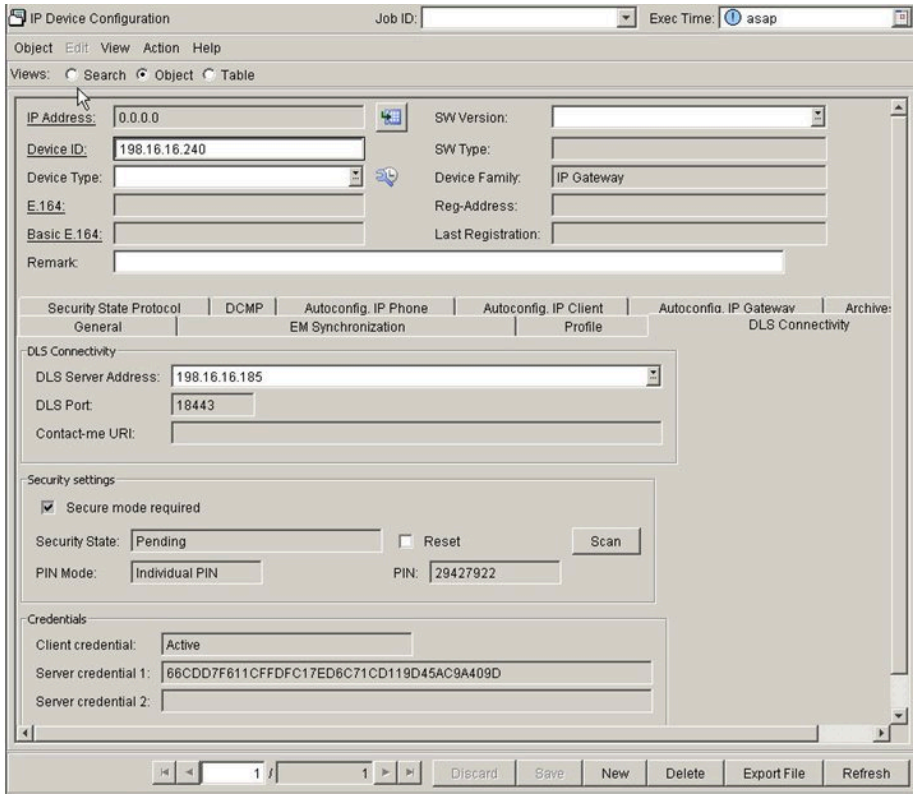
1) Nach Abschluss des Scanvorgangs hängt der nächste Schritt von dem verwendeten Sicherheitsmodus ab:

a) Im **NO PIN**-Modus wird unter **IP Device Configuration** > **DLS Connectivity** > **Security State** der Sicherheitsstatus **Secure** (Sicher) angezeigt. Nun ist das Bootstrapping für diesen Modus beendet und Sie können mit der Verteilung des SPE CA-Zertifikats und der SPE-Zertifikate

beginnen (siehe Abschnitt 6.1.3, „Verteilung eines SPE-Zertifikats“ und Abschnitt 6.1.4, „Verteilung eines SPE-Zertifikats“).



Im Sicherheitsmodus Standard-PIN oder Individuelle PIN wird nach dem scannen als **Sicherheitsstatus Pending** angezeigt.



Die PIN muss über CLI am Gateway eingegeben werden.

CLI-Befehl:

vxTarget> activate dls pin 29427922

activate dls pin - args: 29427922.

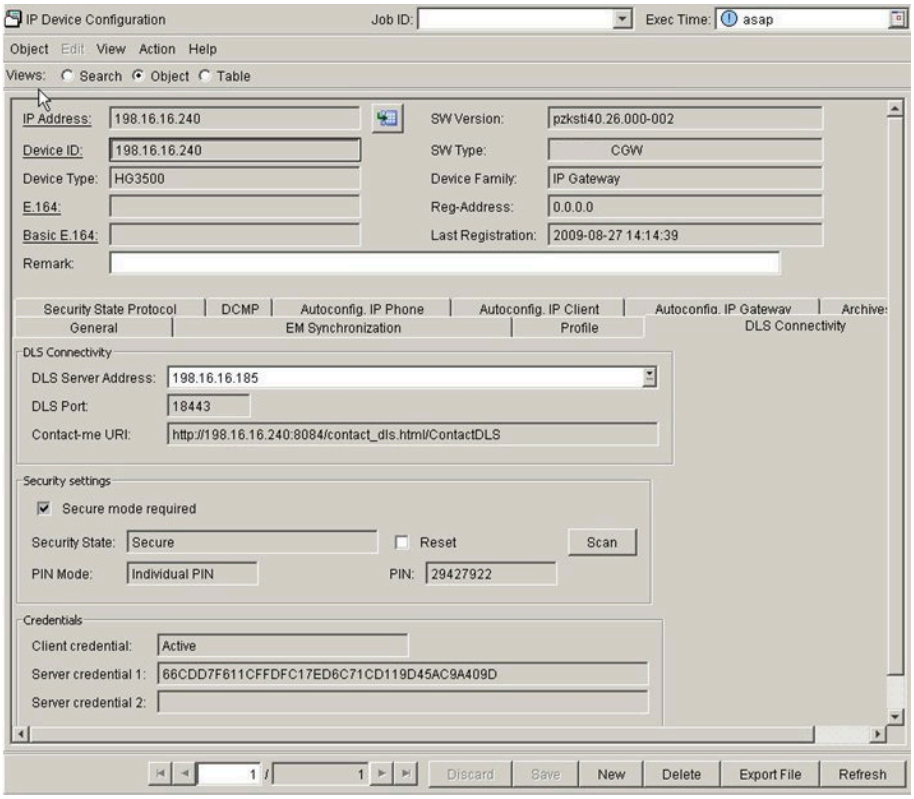
Bootstrapping succeeded.

OK

vxTarget>

Bei virtuellen Gateways gibt es kein CLI. Daher ist die PIN auf einer WBM Maske einzugeben.

Wenn Sie nun zu DLS DLS Konnektivität > **Sicherheitsstatus** zurückkehren zeigt der Gateway **Secure** an. Das Bootstrapping ist abgeschlossen, und Sie können mit der Verteilung von CA- und SPE-Zertifikaten fortfahren (siehe Abschnitt 6.1.3, „Verteilung eines SPE-Zertifikats“ und Abschnitt 6.1.4, „Verteilung eines SPE-Zertifikats“).



Bootstrapping Endprüfung in Gateway WBM:

Im WBM der HG 3500/3575 V4 und neuer können Sie überprüfen, ob das Importieren und Aktivieren der Zertifikate funktioniert hat. Der Zugriff erfolgt mit HiPath 4000 Assistant.

Menü: **Expert Access** > HiPath **4000** > **HG35xx Web Based Management**

Im WBM können Sie die Zertifikate im folgenden Verzeichnis anzeigen:

Configuration > **Security** > **Deployment and Licensing Client (DLSC)**

Hier müsste es nun zwei Einträge geben:

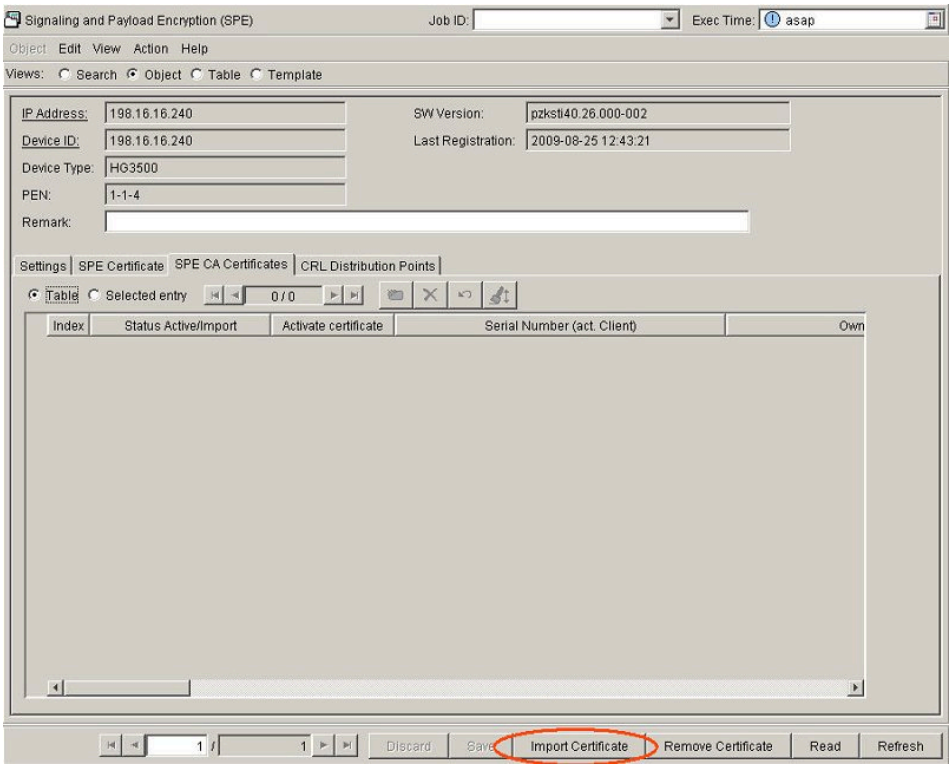
a) DLSC Client Certificate
b) • DLSC CA Certificate

18.6.1.3 Verteilung eines SPE-Zertifikats

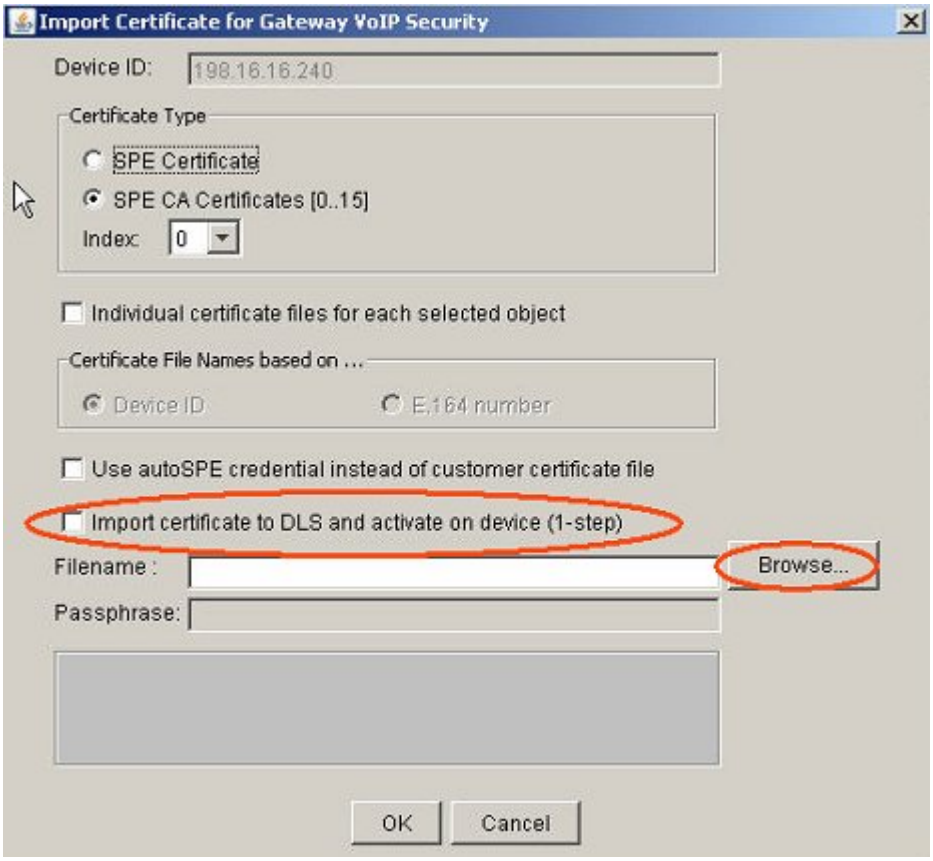
CA-Zertifikat importieren: **IP Devices** > **IP Gateway Configuration** > **Signaling und Payload Encryption (SPE)**

Nach dem Bootstrapping lassen sich alle betreffenden Baugruppen (siehe Abschnitt 6.1.2, „Scannen der IP Devices (IP-Gateways)“) mit der Optionsschaltfläche **Suchen** anzeigen.

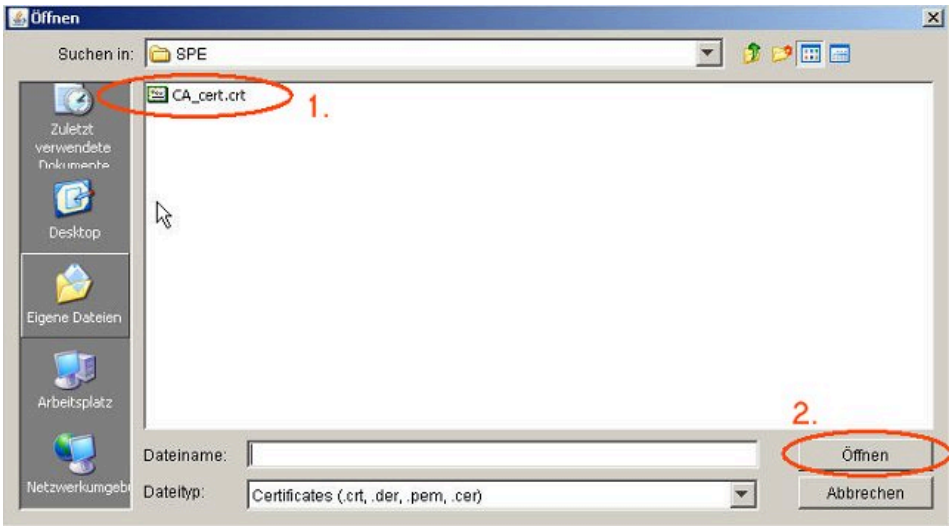
Klicken Sie auf die Schaltfläche **Zertifikat importieren**.



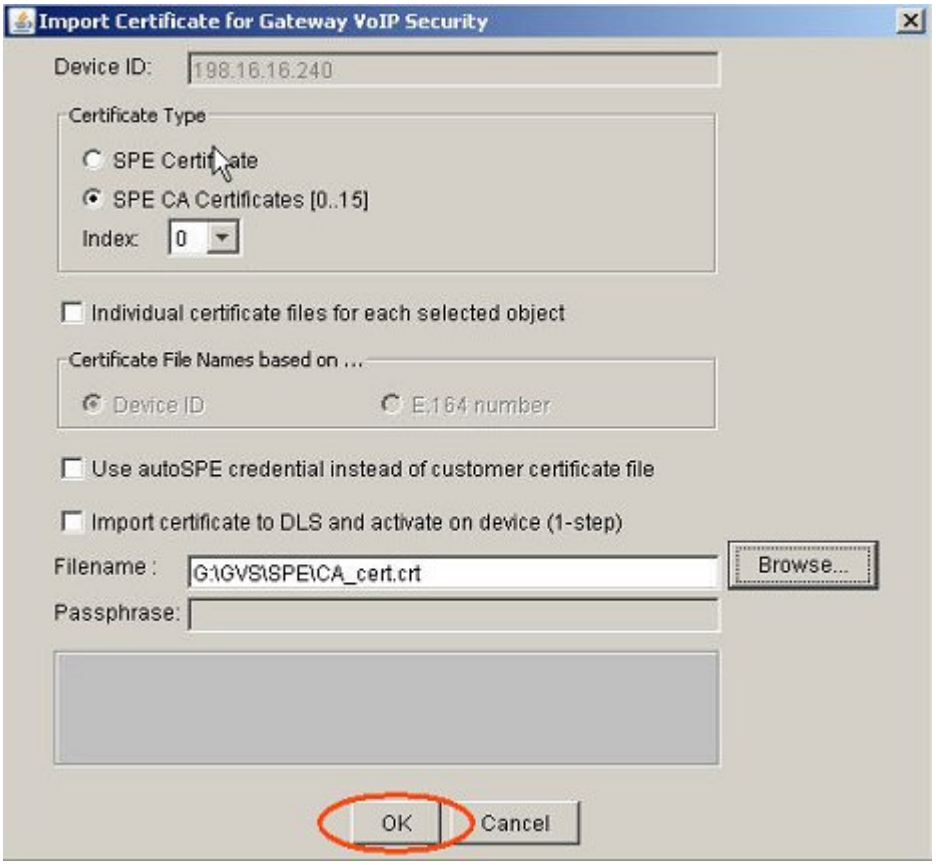
Ein neues Fenster wird angezeigt, in dem Sie nach dem CA-Zertifikat suchen können. Es können bis zu 16 CA Zertifikate importiert werden. Die CA-Zertifikate können in einem Arbeitsgang importiert und aktiviert werden.



CA-Zertifikat auswählen

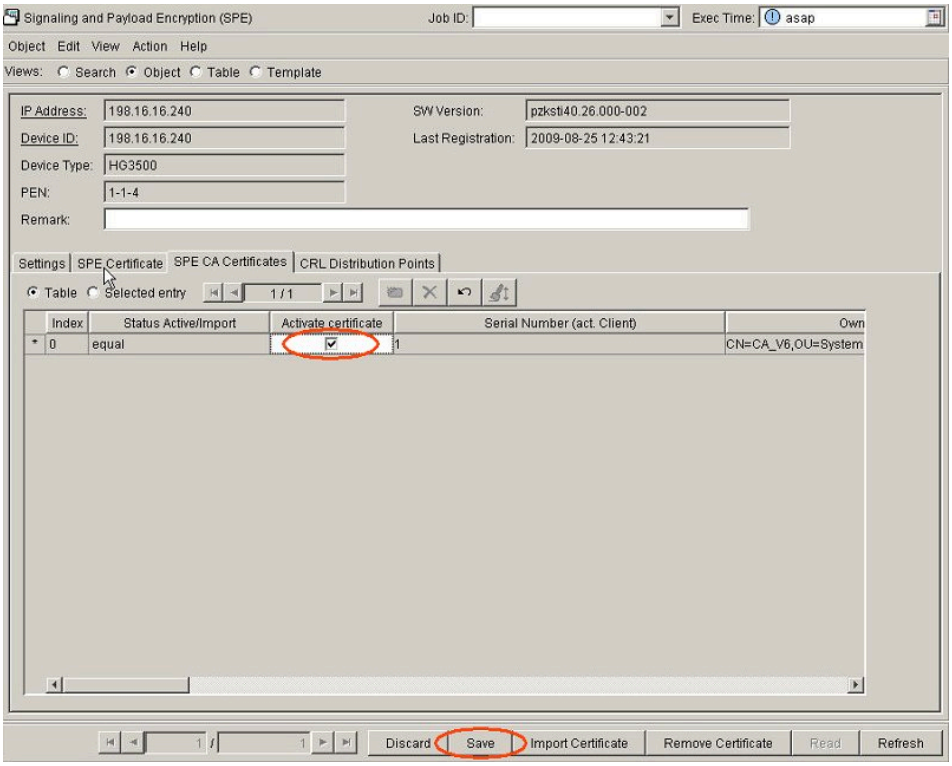


Bestätigen Sie Ihre Auswahl.



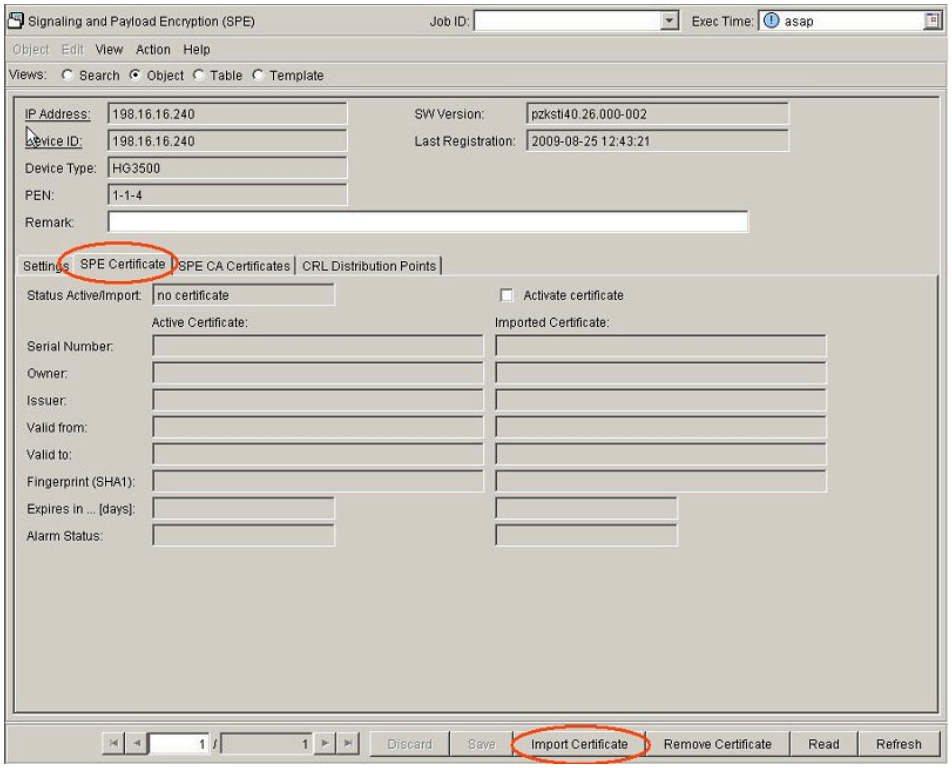
Aktivieren Sie das CA-Zertifikat.

Wenn Sie das Kontrollkästchen **Zertifikat aktivieren** aktivieren und auf **Speichern** klicken, wird das Zertifikat aktiviert. Ist das Zertifikat gültig, wechselt der Status des importierten Zertifikates von **kein aktives Zertifikat** zu **gleich**. Außerdem werden einige Daten vom DLS gelesen, z. B. CN, OU.



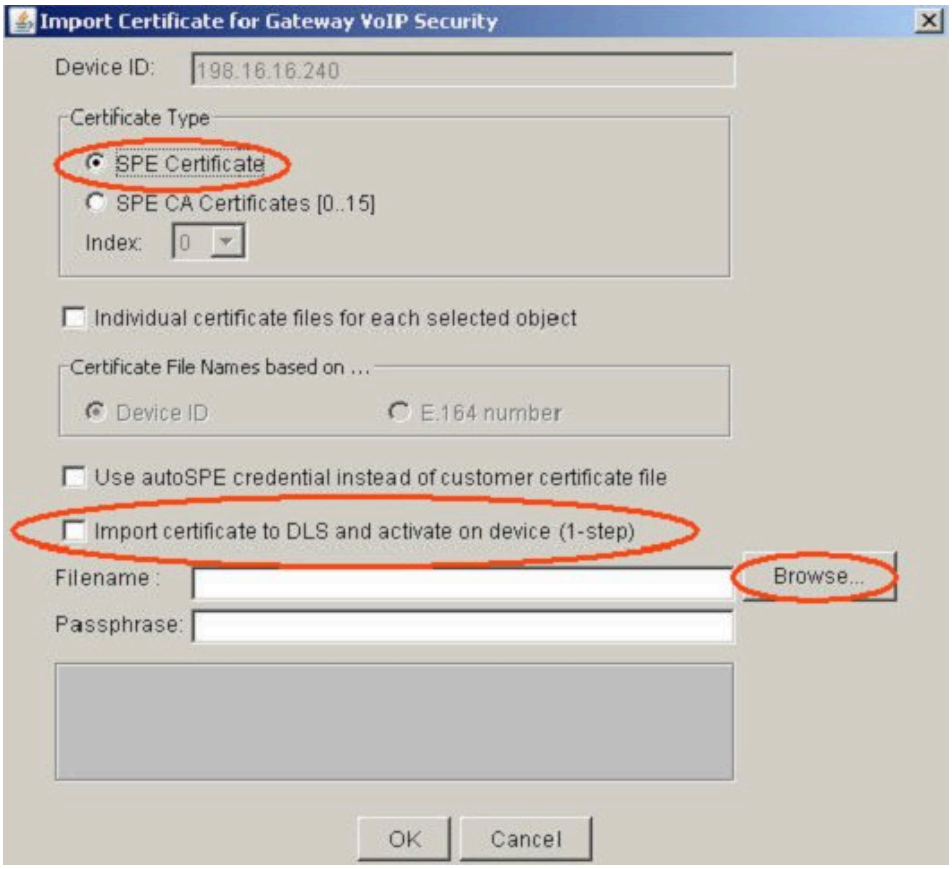
18.6.1.4 Verteilung eines SPE-Zertifikats

SPE-Zertifkat importieren: **IP Devices** > **IP Gateway Konfiguration** > **VoIP Security** > Register **Credentials**

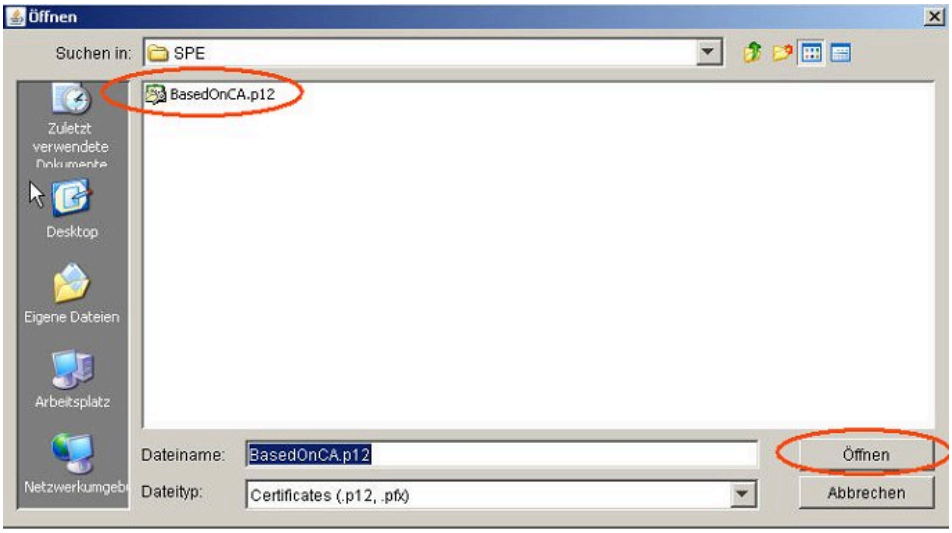


Suchen Sie das Zertifikat.

Das Zertifikat kann in einem Arbeitsgang importiert und aktiviert werden.

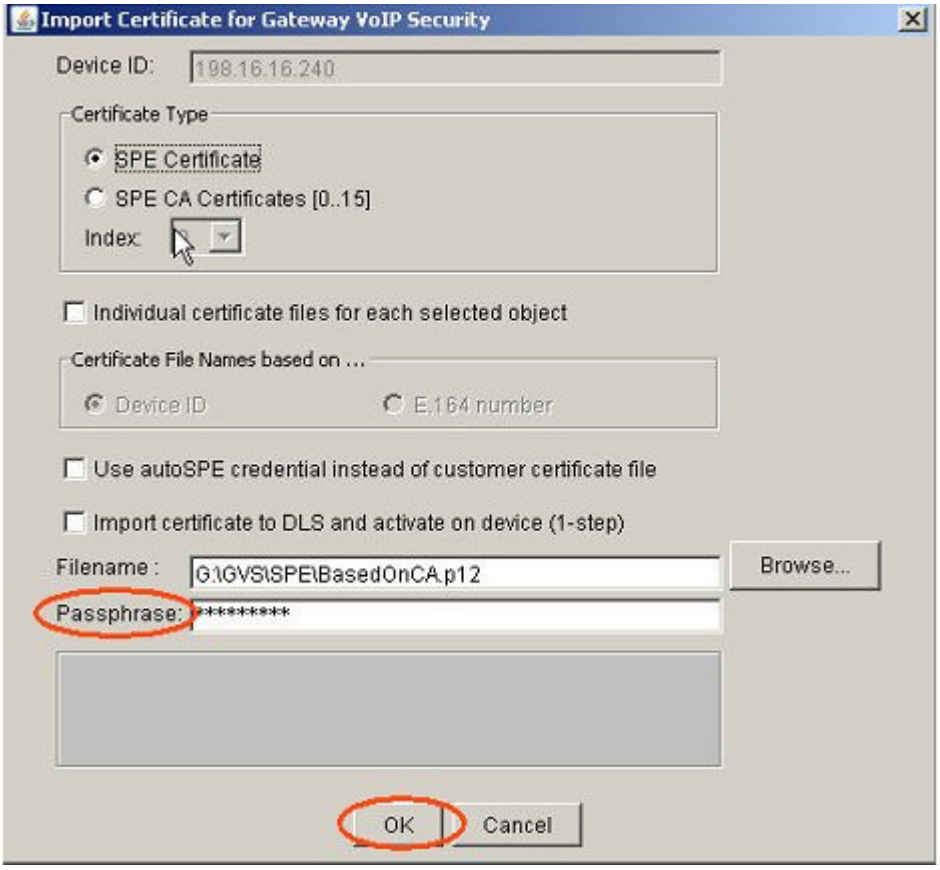


Wählen Sie das Zertifikat aus.



Passphrase ist das für die Verschlüsselung des Inhalts der p12-Datei verwendeten Passwort. Es wird beim Erstellen der p12-Datei erzeugt.

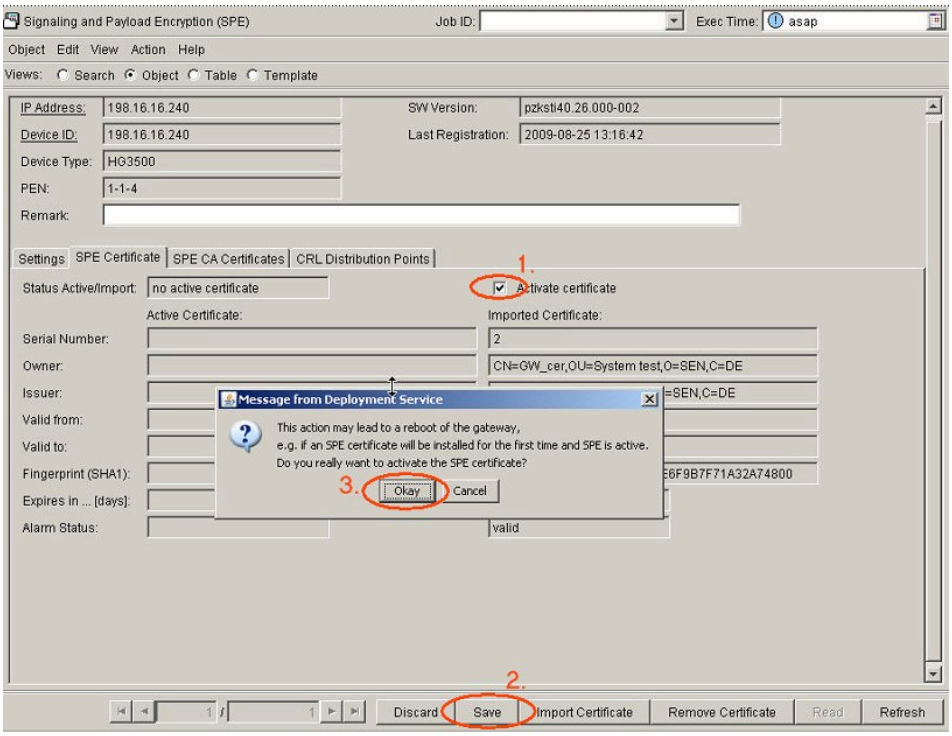
Wichtig: Diese Passphrase ist nicht mit der im Assistant konfigurierten Passphrase für die Aktivierung von Secure Trace zu verwechseln. Diese beiden Passphrase haben nichts miteinander zu tun.



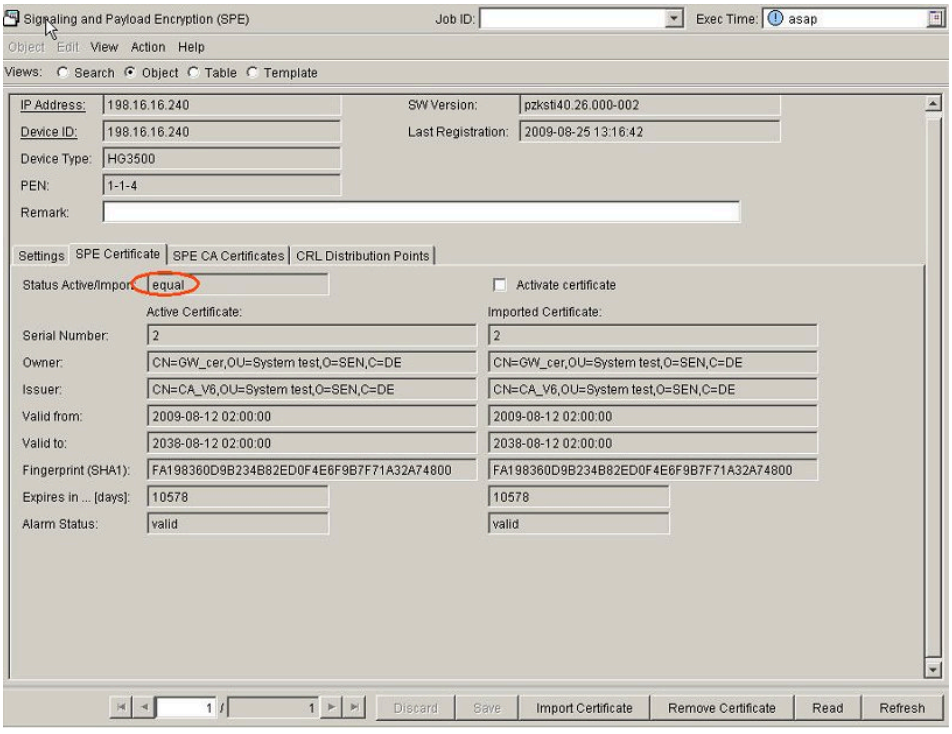
Das Zertifikat wurde erfolgreich importiert.



Aktivieren Sie das Zertifikat.



Das Zertifikat ist aktiv. Der Status (**Status Aktiv/Import**) ist **gleich**.



Im WBM der HG 3500/3575 V4 und neuer können Sie überprüfen, ob das Importieren und Aktivieren der Zertifikate funktioniert hat. Der Zugriff erfolgt mit HiPath 4000 Assistant.

Menü: **Expert Access** > HiPath **4000** > **HG35xx Web Based Management**

Im WBM können Sie die Zertifikate im folgenden Verzeichnis anzeigen:

1) **Configuration> Security > Signaling und Payload Encryption (SPE)**

Hier müsste es nun zwei Einträge geben:

- SPE-Zertifikat
- SPE CA Zertifikat



18.6.1.5 Bootstrap-Reset

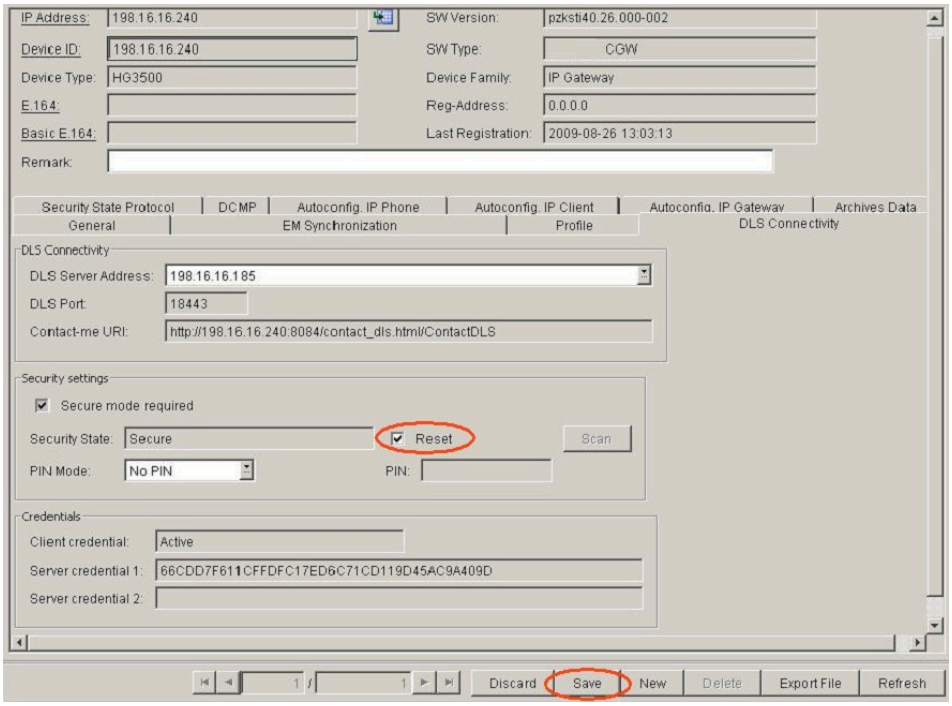
Sollte es zu dem Fall kommen, dass der DLS und das Gateway nicht mehr miteinander kommunizieren können, dann muss das Bootstrapping zwischen dem DLS und dem Gateway zurückgesetzt werden.

18.6.1.5.1 DLS-Bootstrap-Reset

Funktionsweise der Reset-Option:

Wenn dieses Kontrollkästchen aktiviert ist, lässt sich der Sicherheitsmodus durch Klicken auf die Schaltfläche „Speichern“ auf „Unsicher“ zurücksetzen.

Der DLS muss dann eine neue Sicherheitskonfiguration an das IP Device senden, der Bootstrap-Vorgang also wiederholt werden.



18.6.1.5.2 Gateway-Bootstrap-Reset

CLI-Befehl:

```
reset dls bootstrapping
```

Wichtig: Auf virtuellen Gateways gibt es kein CLI. Reset Bootstrapping ist dort per WBM durchzuführen.

18.6.2 Verteilung von Zertifikaten an Teilnehmer

18.6.2.1 Verteilen eines CA-Zertifikats

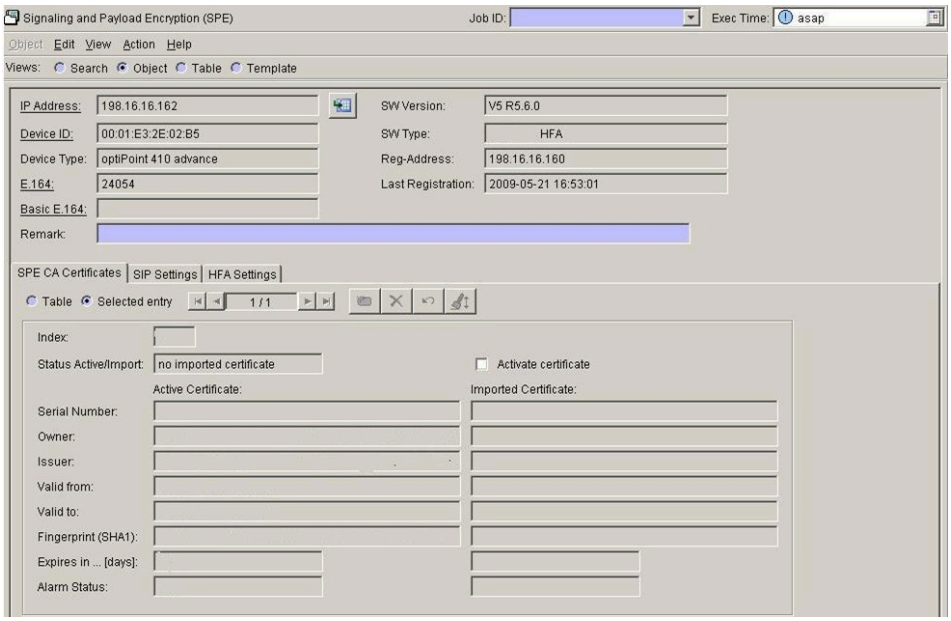
Beim Teilnehmer kann das Transportprotokoll auf TCP oder TLS eingestellt werden (Menü, WBM des Teilnehmers oder DLS). Wenn **Verschlüsselung** verwendet wird, muss für den Teilnehmer das **TLS**-Protokoll genutzt werden.

Ein IP-Teilnehmer erhält nur ein CA-Zertifikat. Das SPE-Zertifikat wird direkt vom Gateway an den IP-Teilnehmer gesendet, wenn der Teilnehmer mit dem TLS-Protokoll arbeitet.

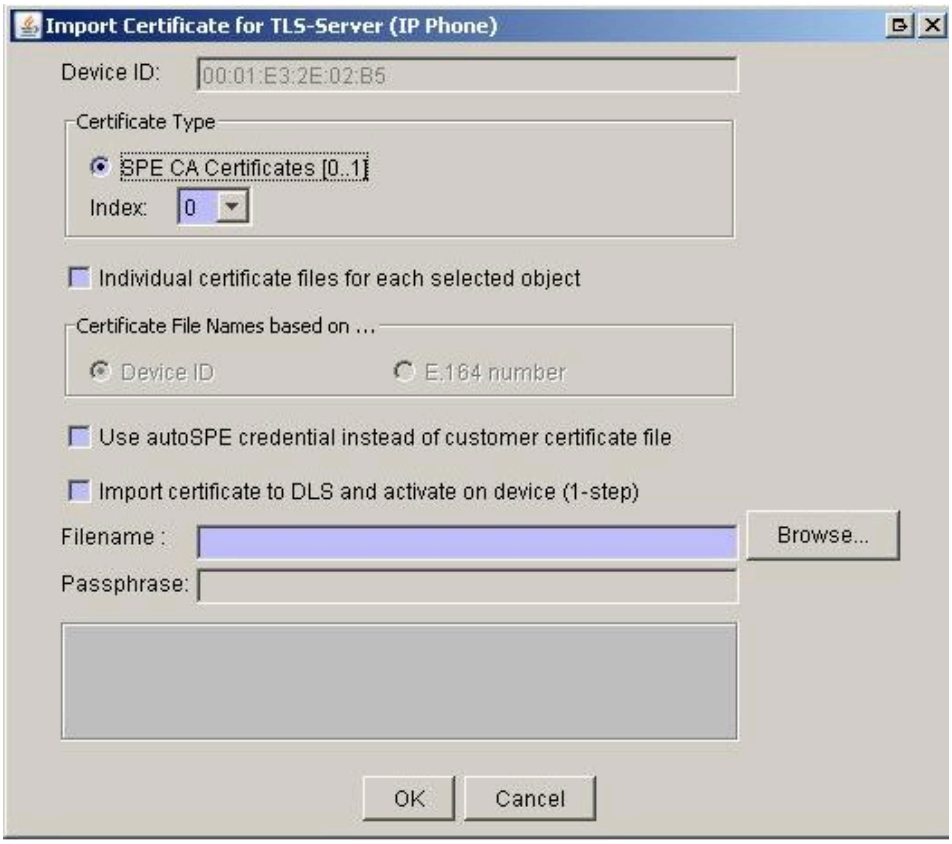
Wenn das Endgerät das TLS-Protokoll nutzt, wird das SPE-Zertifkat direkt vom Gateway an das IP-Endgerät gesendet. Das CA-Zertifikat kann nur über den DLS an das Telefon weitergeleitet werden.

Verteilung des Zertifikats an den Teilnehmer über DLS.

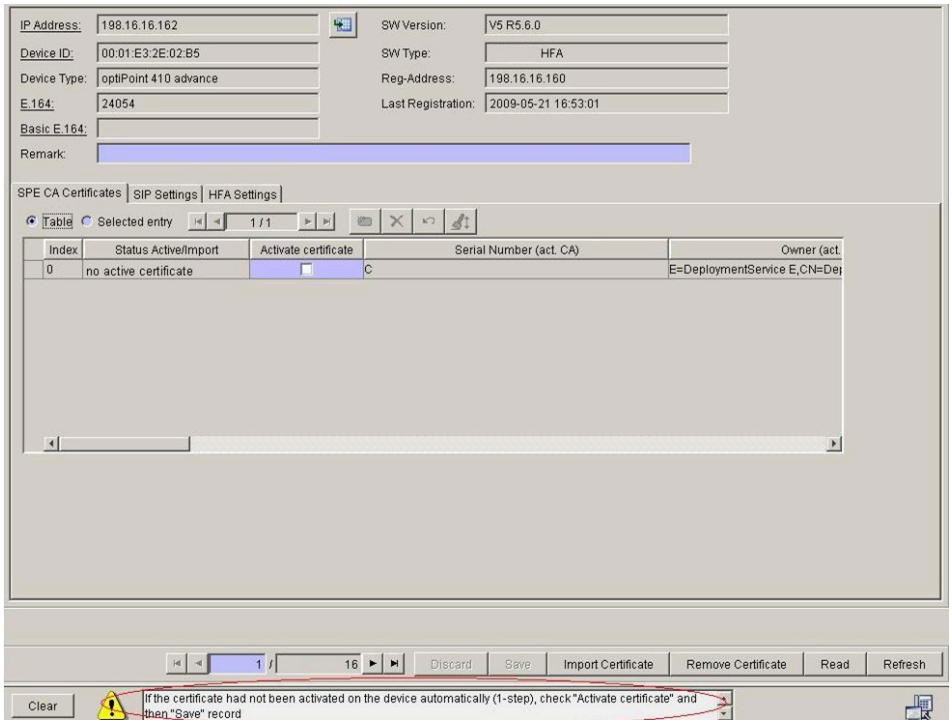
IP Devices > **IP Phone Konfiguration** > **Signaling und Payload Encryption (SPE)** > Register **SPE CA-Zertifikat**



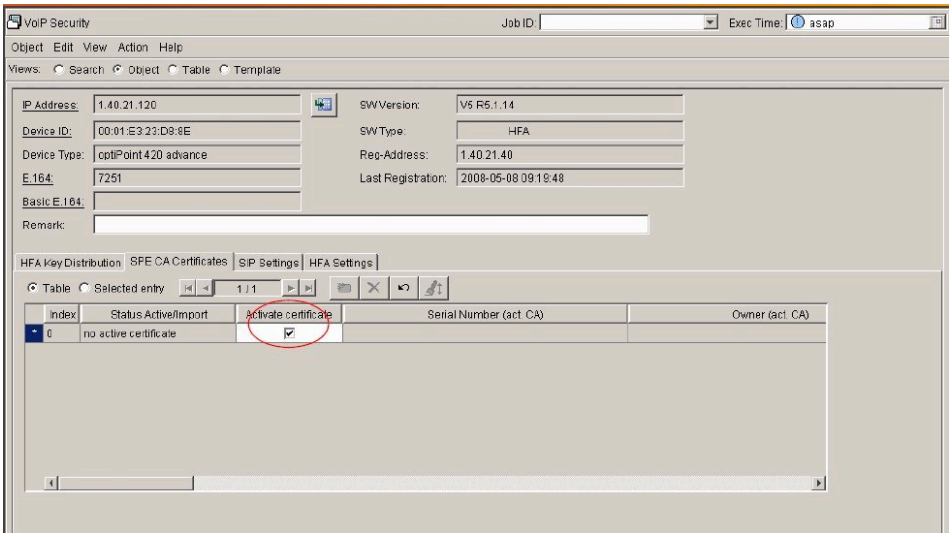
Wählen Sie das CA-Zertifikat über die Schaltflächen **Zertifikat importieren** und **Durchsuchen** aus.



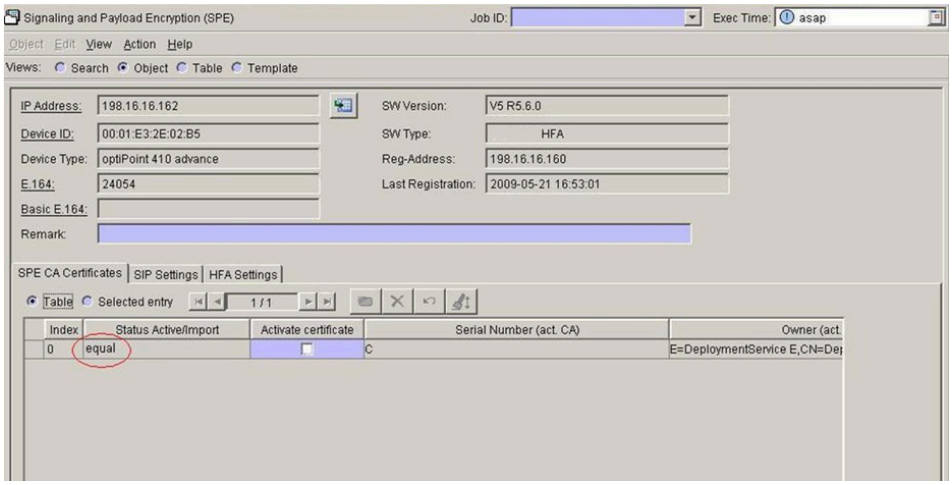
Wenn der Import des Zertifikats erfolgreich war, wird eine Meldung angezeigt.



Aktivierung des Zertifikats.



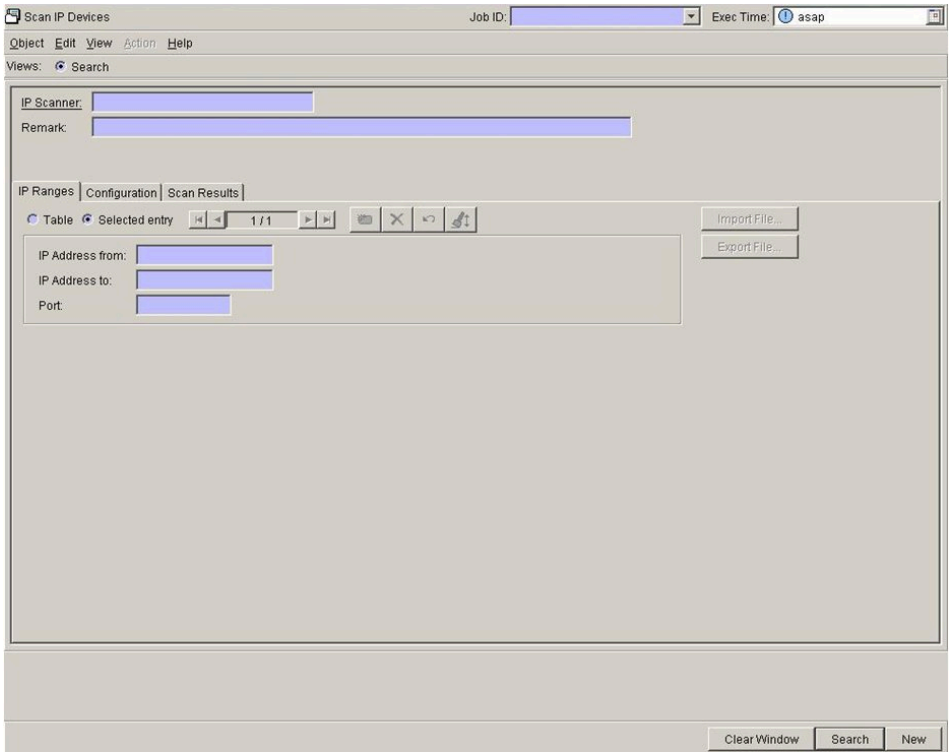
Nach erfolgreicher Aktivierung wechselt der Status (**Status Aktiv/Import**) von **kein aktives Zertifikat** zu **gleich**.



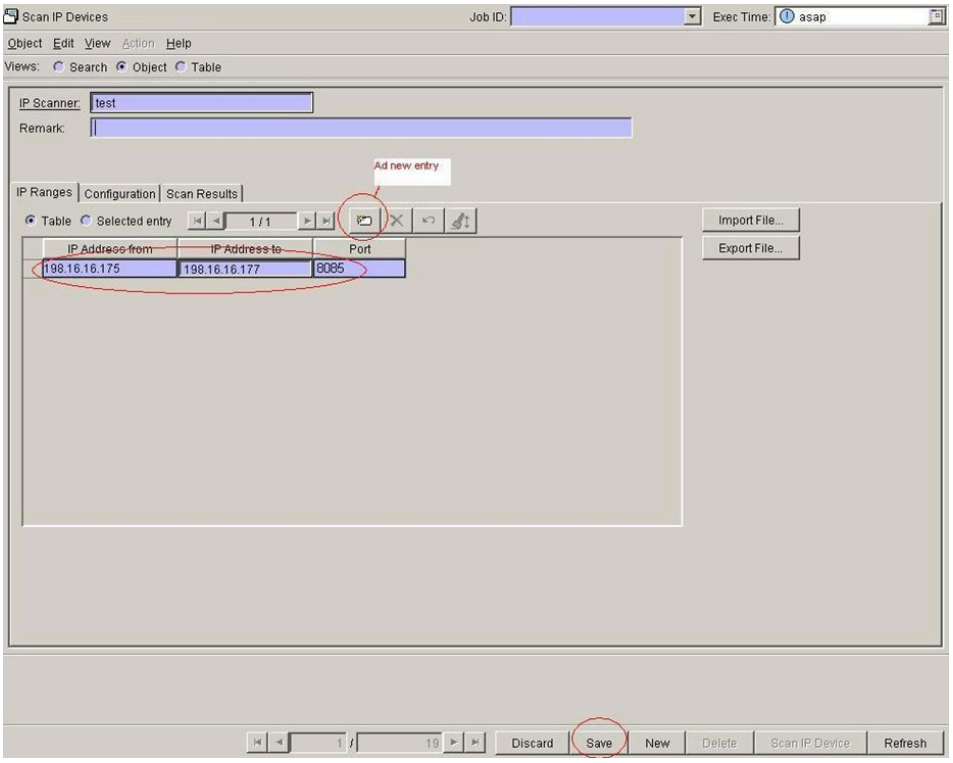
18.6.2.2 Scannen der IP Devices (Endgeräte)

Zum Hinzufügen der IP-Teilnehmer im DLS muss der IP-Bereich gescannt werden, dem die Teilnehmer angehören.

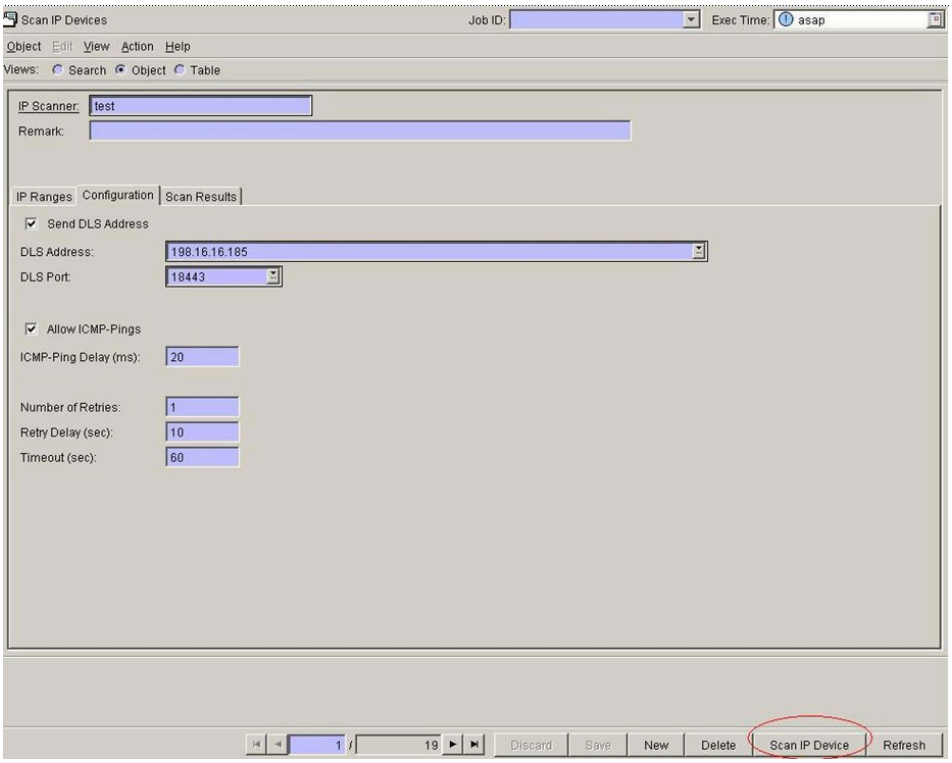
IP Device > **IP Device Interaktion** > **IP Devices scannen**



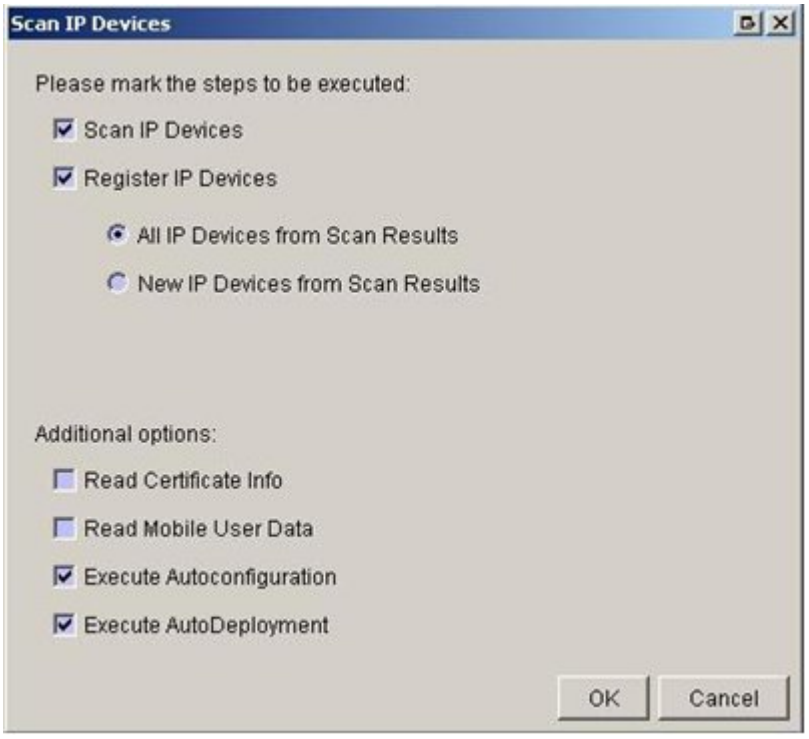
Register: **IP Bereiche** Geben Sie hier den Namen für den **IP-Scanner**, den IP-Adressbereich (**IP Adresse von, IP Adresse bis**) und den **Port 8085** ein.



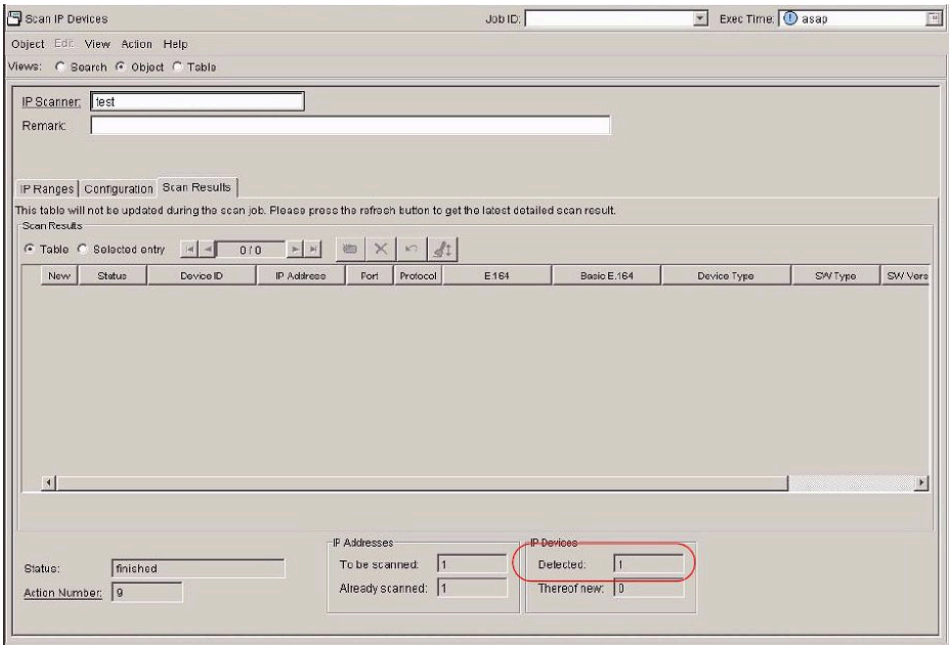
Register: **Konfiguration** Geben Sie hier die IP-Adresse (**DLS Adresse**) und den Port (**DLS Port**) des DLS ein, und aktivieren Sie das Kontrollkästchen **Sende DLS Adresse**. Starten Sie das Scannen der IP-Endgeräte, indem Sie auf Schaltfläche **IP Devices scannen** klicken.



Wählen Sie **IP Devices scannen**, **IP Devices registrieren** und **Alle IP Devices aus den Scan Ergebnissen**, und klicken Sie dann auf **OK**.



Register: **Scan Ergebnisse** Hier wird die Anzahl der erkannten Gateways (**IP Devices > Detected (Erkannt)**) angezeigt.



18.7 AutoSPE-Konfiguration

Wichtig: Dieses Kapitel soll nur einen kurzen Überblick über die notwendigen Schritte im Deployment Service (DLS) vermitteln. Eine genaue Beschreibung finden Sie im Administratorhandbuch des DLS.

Wichtig: Ab OpenScape 4000 V7 R1.8 wird SHA256 Protokoll unterstützt. Vor OpenScape 4000 V7 R1.8 musste Auto SPE auf DLS Seite über eine Funktion, die ab DLS V7 R1.11.2 zur Verfügung steht, explizit für SHA 128 konfiguriert werden. Bitte sehen Sie im Abschnitt 16.5.6 „SHA1-Konfiguration für AutoSPE“ in der Dokumentation „OpenScape Deployment Service V7, Administratordokumentation“ nach.

Der Bereich der automatischen SPE Konfiguration im DLS ermöglicht dem Anwender die automatische Konfiguration von PKI-basierter Signalisierungs- und Sprachverschlüsselung (SPE). Dies ist insbesondere dann nützlich, wenn keine Kunden-PKI zur Verfügung steht.

DLS unterstützt das Generieren und Bereitstellen von SPE CA-Zertifikaten (CA= Certificate Authority, Zertifizierungsstelle) für administrierte IP-Geräte (Gateways und Teilnehmer). Beim Aktivieren eines SPE CA-Zertifikats wird für jedes administrierte Gateway ein SPE CA-Zertifikat generiert und bereitgestellt.

Mittels Export und Import ist es möglich, CA-Zertifikate von einem DLS zum anderen umzuziehen.

Bei der automatischen SPE-Konfiguration per DLS erhalten alle in DLS bekannten Teilnehmer (unabhängig vom Gateway) auch das von der AutoSPE-Konfiguration generierte CA-Zertifikat. Die Gültigkeit dieses Zertifikats kann in

den Sicherheitseinstellungen des Teilnehmers überprüft werden (DLS: HFA Server Validation, Telefon: Certificate Check).

18.7.1 OpenScape 4000

Anforderungen für SPE

Wichtig: SPE-Zertifikate können auch dann an den Gateways konfiguriert werden, wenn SPE deaktiviert ist.

1) Ein NTP-Server muss für die Zeitsynchronisierung konfiguriert sein.
2) In AMO ZANDE SPESUPP=YES muss Folgendes eingestellt sein: CHANGE-ZANDE:TYPE=SECURITY,SPESUPP=YES; Wenn AP-Shelfs oder SoftGate konfiguriert sind, sollte auch der folgende Befehl ausgeführt werden: CHANGE-SIPCO:TYPE=SECURITY,IPDAENCR=Y;
3) Im Falle einer Duplex-Konfiguration sollte der Standby-Knoten ebenfalls neu gestartet werden:
4) `EX-REST:TYPE=UNIT,UNIT=BPS,RSLEVEL=HARD;`

   `EX-REST:TYPE=UNIT,UNIT=BP,RSLEVEL=HARD;`
5) Folgende Teilnehmereinstellungen müssen verifiziert werden: Je SPE-Teilnehmer muss der Parameter CLASSEC=SECURE im AMO SDAT gesetzt sein:
6) `CHANGE-SDAT:TYPE=DATA1,CLASSEC=SECURE;`
7) Für HFA-Teilnehmer muss im AMO CGWB überprüft werden, ob im Parameterzweig **TYP=GLOBIF** der Wert für **TLSP=4061** ist.

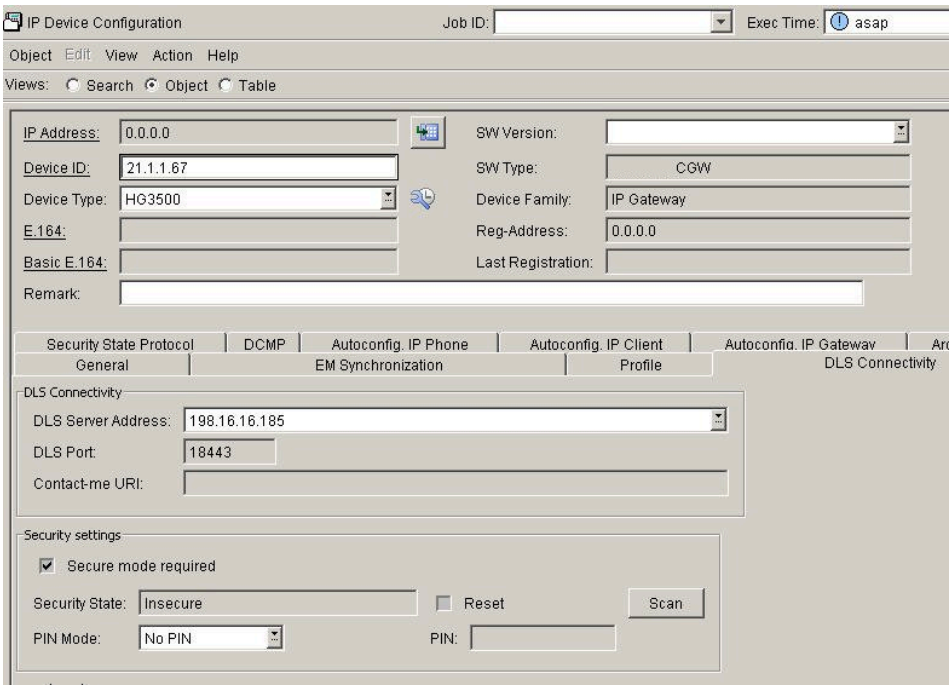
18.7.2 Deployment Service DLS

18.7.2.1 Zeitserver DLS

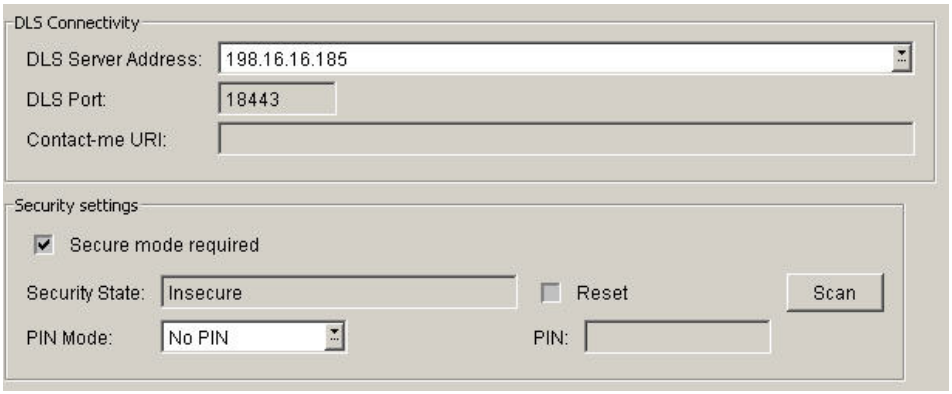
z.B. Freware-Tool „Nettime“

Wichtig: Der Windows Time Service muss beendet werden!

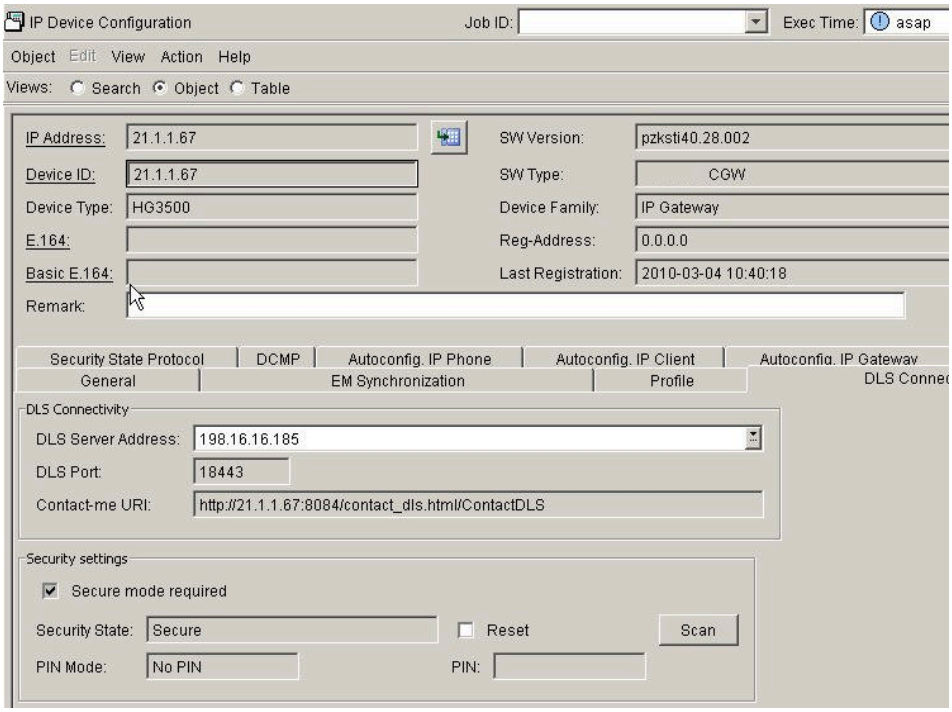
18.7.2.2 Vorbereitungen DLS



Virtuelles Device / IP-Gateway anlegen



IP-Gateway scannen

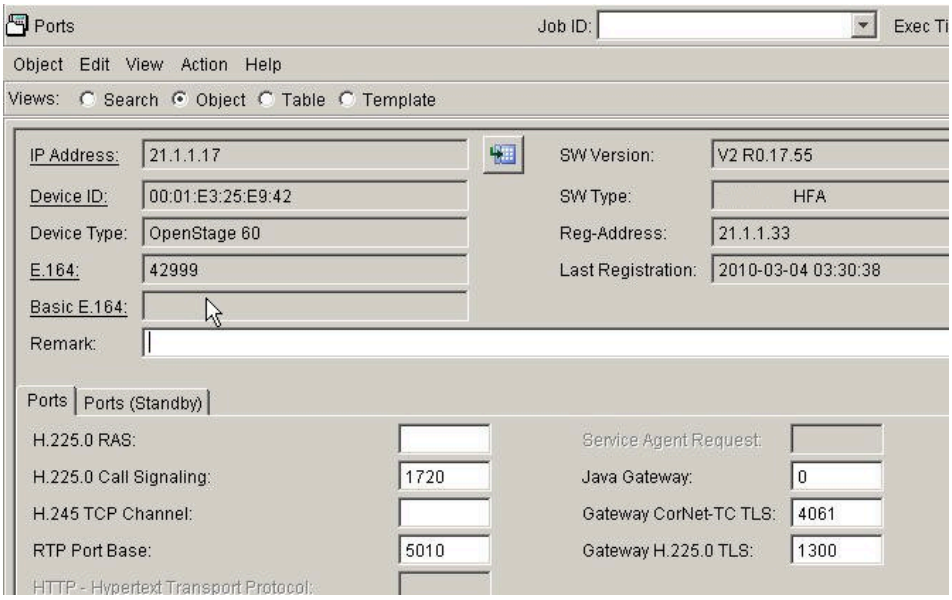


IP-Gateway „gescannt“

18.7.3 Endgeräte-Konfiguration

18.7.3.1 Vorbereitungen

Wichtig: Der Wert für H.225.0 TLS muss 1300 sein!



Vorbereitungen Endgeräte

Die Display & Trace-Time kann auch auf „SNTP“ gesetzt werden.

18.7.3.2 Zeitserver

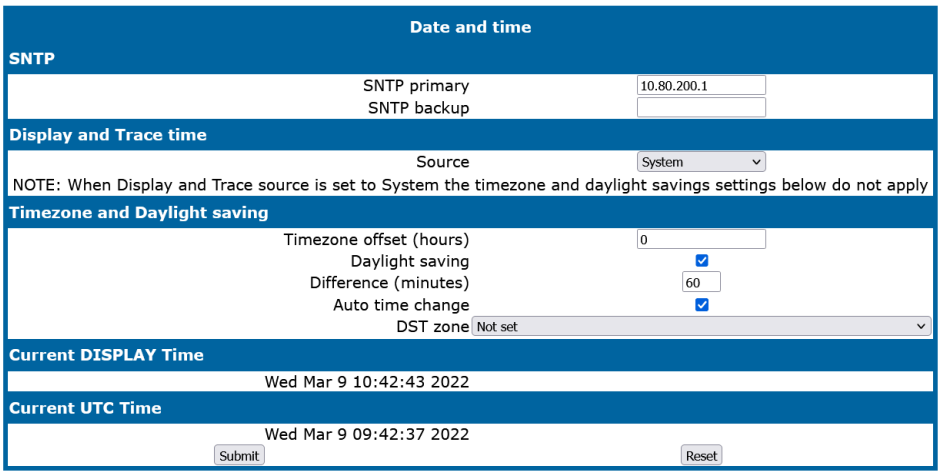
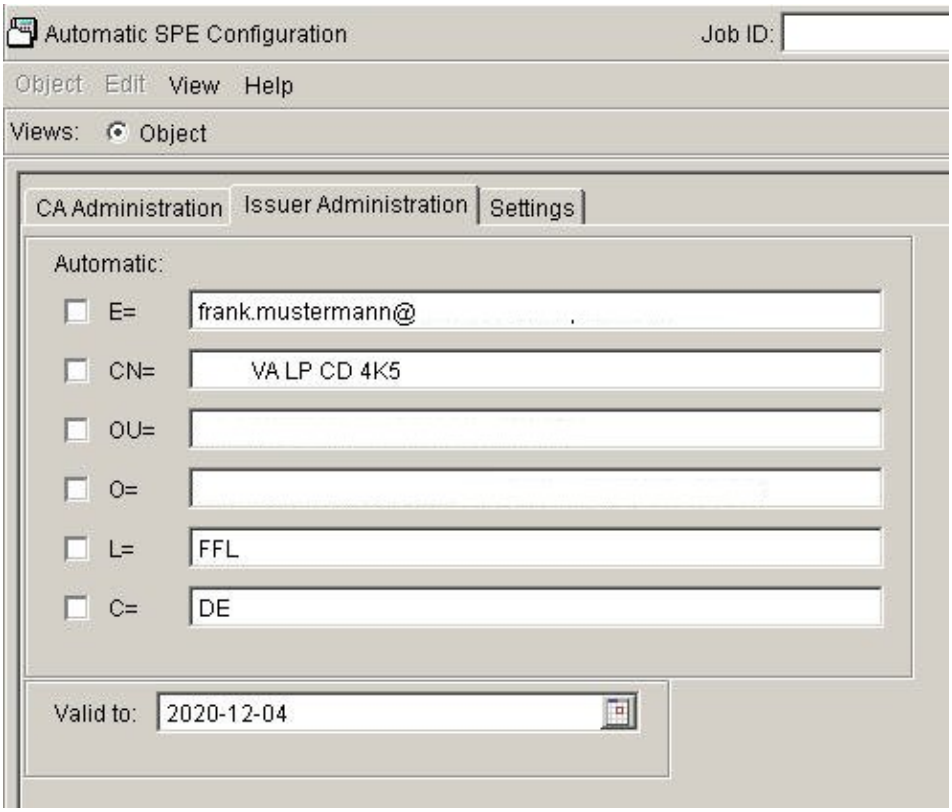
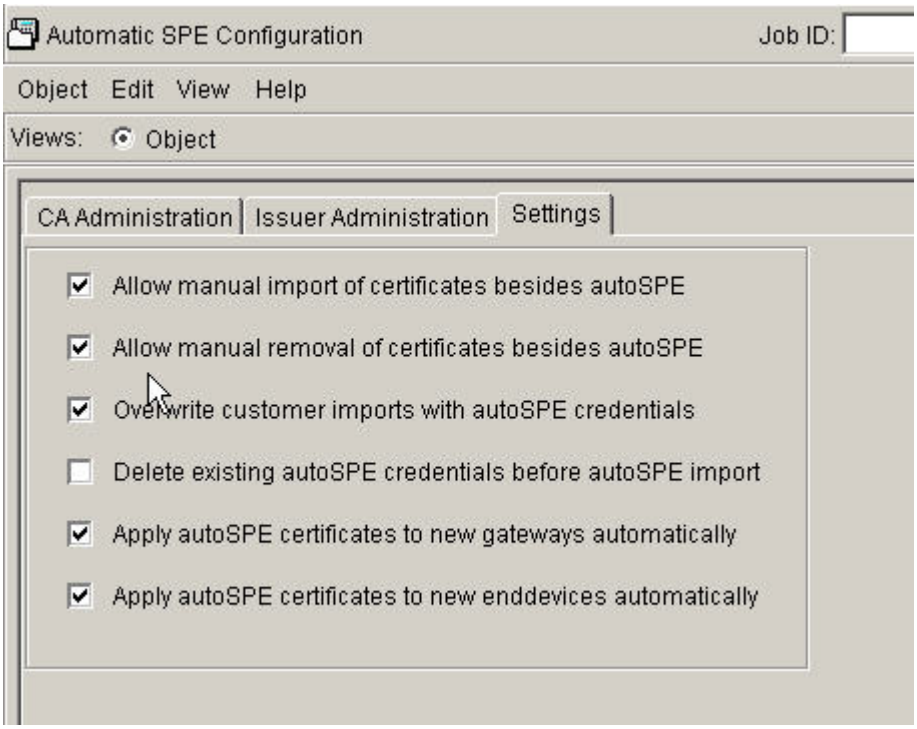


Abbildung 336: Zeitserver Endgeräte

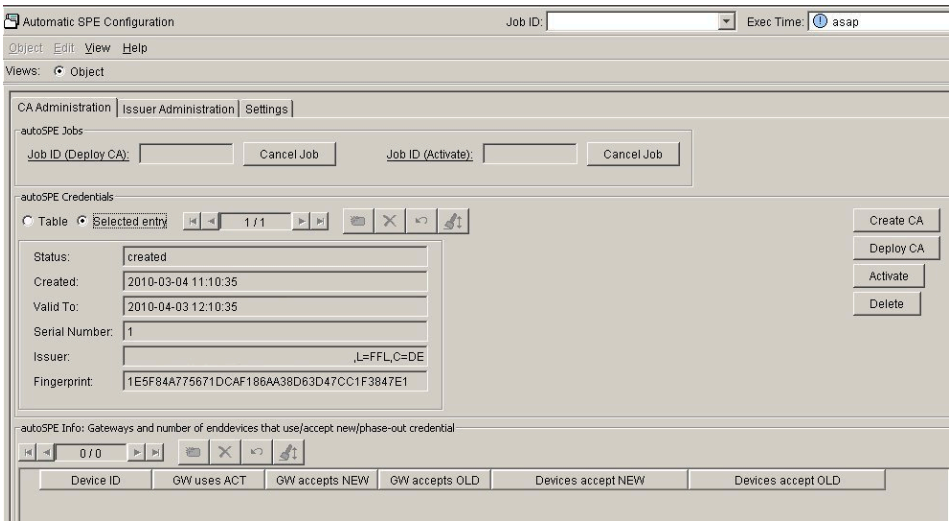
18.7.4 Automatische Zertifikatserstellung



Aussteller Administration



Aussteller Administration > Einstellungen



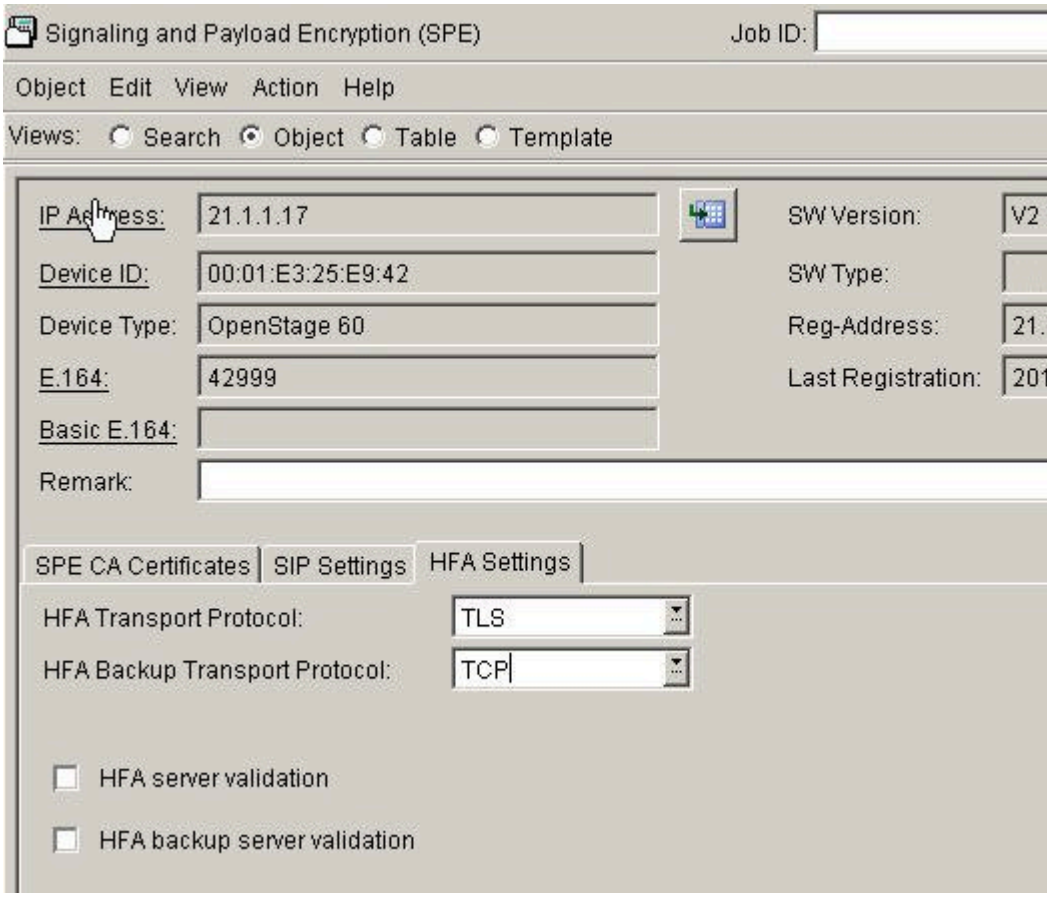
CA Administration

Bei der CA-Administration muss zunächst ein Zertifikat erzeugt, danach verteilt und zum Schluss aktiviert werden. Dies kann im Status abgefragt werden.

Die untere Tabelle zeigt, wie viele Teilnehmer Zertifikate erhalten haben.

18.7.5 Sprachverschlüsselung aktivieren

Zum aktivieren von SPE muss nun noch das Transport-Protokoll auf „TLS“ umgeschaltet werden:



Sprachverschlüsselung aktivieren

18.7.6 Zertifikate überprüfen

Aktuelles Zertifikat am Teilnehmer anzeigen: SPE CA certificate(s).

Anzeige des aktuellen Zertifikats auf dem Gateway: SPE CA Zertifikate

Wichtig: Diese beiden Zertifikate müssen immer identisch sein!

18.7.7 SPE überprüfen

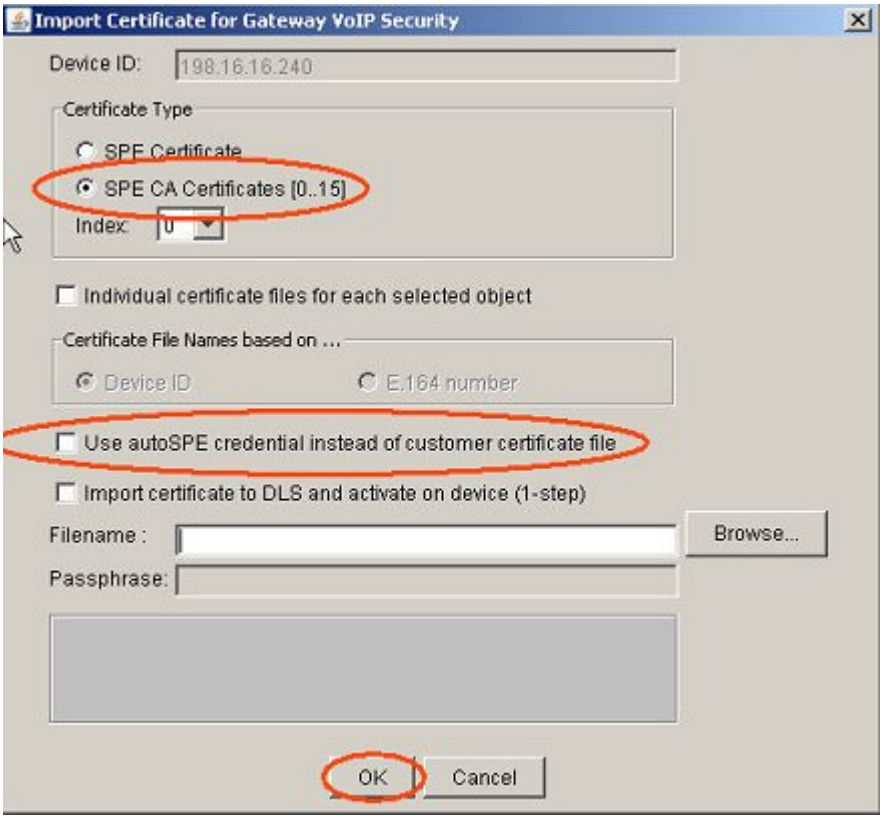
In AMO TAPRO kann ein Schlüssel für die Anzeige des SPE-Status des Teilnehmers konfiguriert werden (siehe Kapitel 3, „Konfiguration“

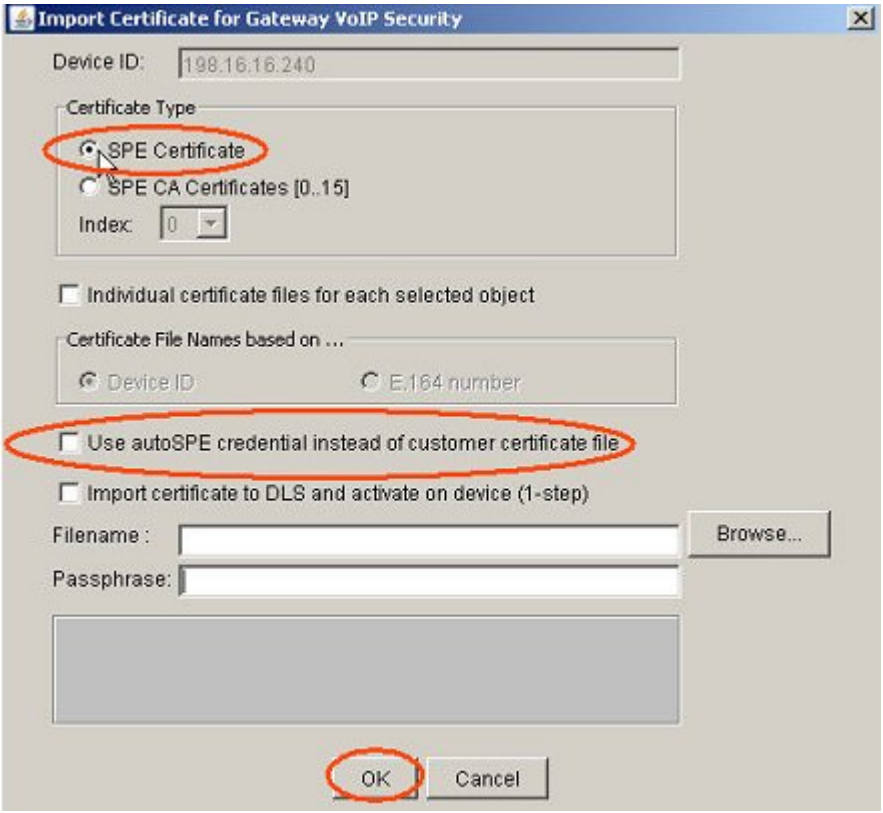
18.7.8 Hinzufügen neuer Gateways nach der AutoSPE-Aktivierung

Die Baugruppe muss im DLS als virtuelles Gerät hinzugefügt, urgeladen und gescannt werden (siehe Abschnitt 6.1, „Verteilung von Zertifikaten an Gateways“).

Anschließend wird die Baugruppe in der Baugruppenliste unter „AutoSPE-Konfiguration“ sowie unter **IP Devices** > **IP Gateway Konfiguration** > **Signaling und Payload Encryption (SPE)** angezeigt.

Um die bereits generierten AutoSPE CA- und SPE-Zertifikate an den neuen Gateway zu senden, müssen Sie zu **IP Devices** > **IP Gateway Konfiguration** > **Signaling und Payload Encryption (SPE)** wechseln. Von dort aus können Sie die Zertifikate von Hand auf den neuen Gateway importieren.





18.8 MTLS-Implementierung für CGW und SG

18.8.1 SYSTEMEINSTELLUNG

Systemkonfiguration ist identisch mit normaler SPE (siehe Kapitel 8, „OpenScape 4000“).

18.8.2 AKTIVIEREN DER ERZWUNGENEN SICHEREN TLS-NEUAUSHANDLUNG (RFC 5746)

Sie können die sichere Neuaushandlung für HFA-Geräte verwenden (nicht OptiPoint). Mögliche Werte: 0 bis 167 Stunden, 0 deaktiviert die Neuaushandlung.

1) Aktivierung/Deaktivierung für CGW:

STMI WBM > Configuration > Security > Signalling & Payload encryption (SPE) > Rechtsklick auf **SPE Security Setup > Edit Security Setup > Enforce Secure Renegotiation (RFC 5746)**

1) Neuaushandlungsintervall für CGW:

STMI WBM > Configuration > Security > Signalling & Payload encryption (SPE) > Rechtsklick auf **SPE Security Setup > Edit Security Setup > Maximum Re-Keying interval**

1) Aktivierung/Deaktivierung für SG:

NCUI WBM > Configuration > Security > Security Options > Enforce Secure TLS Renegotiation (RFC 5746)

1) Neuaushandlungsintervall für SG:

STMI WBM > Configuration > SPE > SPE Security Setup > Maximum Re-Keying interval

18.8.3 GERÄTEEINSTELLUNG

18.8.3.1 OPENSTAGE-TELEFONE

WBM> Administrator Pages > System > Security > System

Wählen Sie für SPE in den Feldern **Signalling transport main** und **Signalling transport standby** das **TLS**-Protokoll aus.

Zum Validieren des GW-Zertifikats aufseiten des Telefons aktivieren Sie die Kontrollkästchen **Certificate validation main** und **Certificate validation standby**.

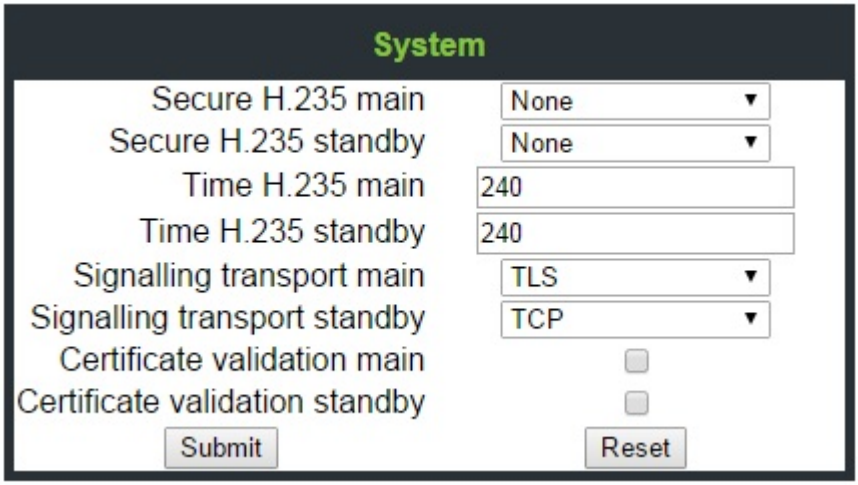


Abbildung 337: OpenStage – SPE aktivieren

18.8.3.2 OPTIPOINT-TELEFONE

OptiPoint-Telefone unterstützen SPE, nicht aber Mutual TLS. Es können nur GW-Zertifikate geprüft werden.

WBM> Administration > System > Signaling & Payload Encryption (SPE)

Wählen Sie für SPE im Feld **Transport mode** das **TLS**-Protokoll aus (unter **Base** und Standby).

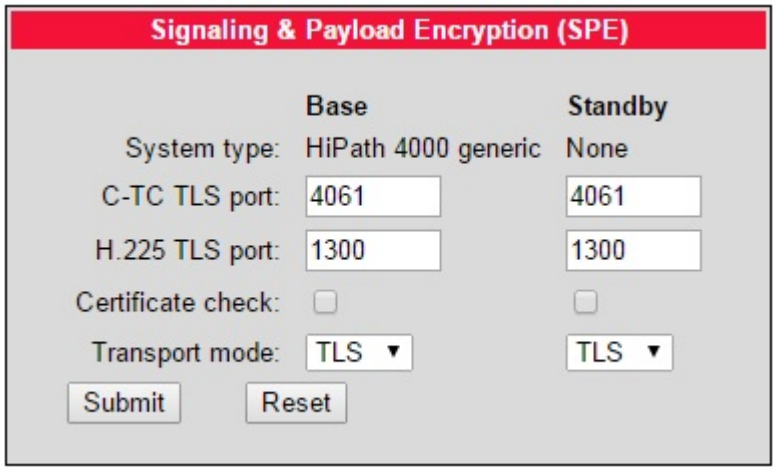


Abbildung 338: OptiPoint – SPE aktivieren

Zum Validieren des GW-Zertifikats aufseiten des Telefons aktivieren Sie **beide Kontrollkästchen** in der Zeile Certificate check (Zertifikatsprüfung).

18.8.4 DLS-GERÄTEEINSTELLUNG

18.8.4.1 PROTOKOLLEINSTELLUNG

Für die Einstellung des Geräteprotokolls kann auch der Deployment Service-Server verwendet werden. Diese Option befindet sich im Menü: D**eployment service > IP Devices > IP Phone Configuration > Signalling & Payload encryption > HFA Setting > HFA Transport Protocol**

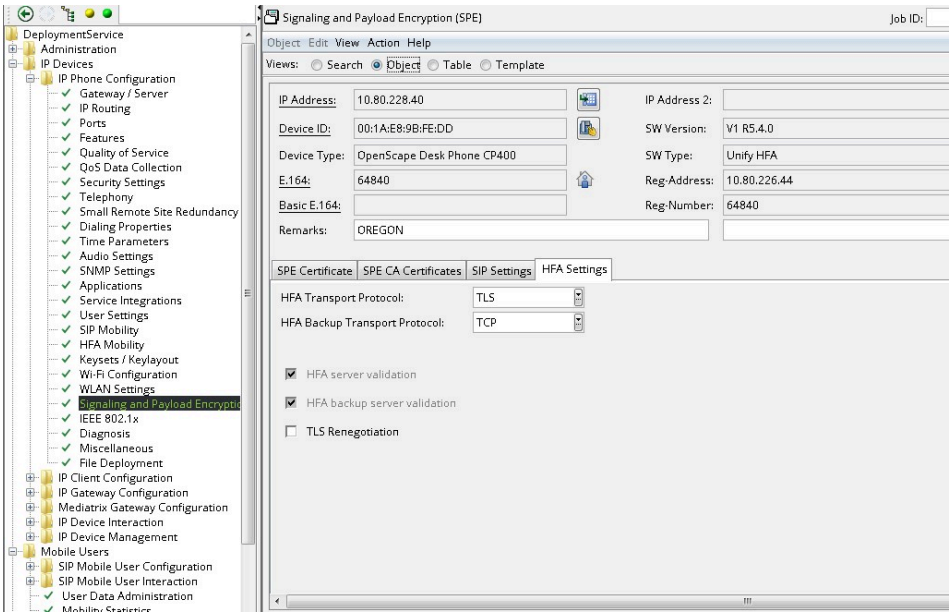


Abbildung 339: DLS-Telefon – Protokolleinstellung

Wählen Sie für SPE in den Feldern **HFA Transport Protocol** und **HFA Backup Transport Protocol** das **TLS**-Protokoll aus.

Zum Validieren des GW-Zertifikats aufseiten des Telefons aktivieren Sie die Kontrollkästchen **HFA server validation** und **HFA backup server validation**.

18.8.4.2 Hochladen des Zertifikats

Das Zertifikat für die Verifizierung des Telefons aufseiten des GW kann nur über den DLS-Server auf das Telefon hochgeladen werden.

Diese Option befindet sich im Menü: **Deployment service > IP Devices > IP Phone Configuration > Signalling & Payload encryption > SPE Certificate**

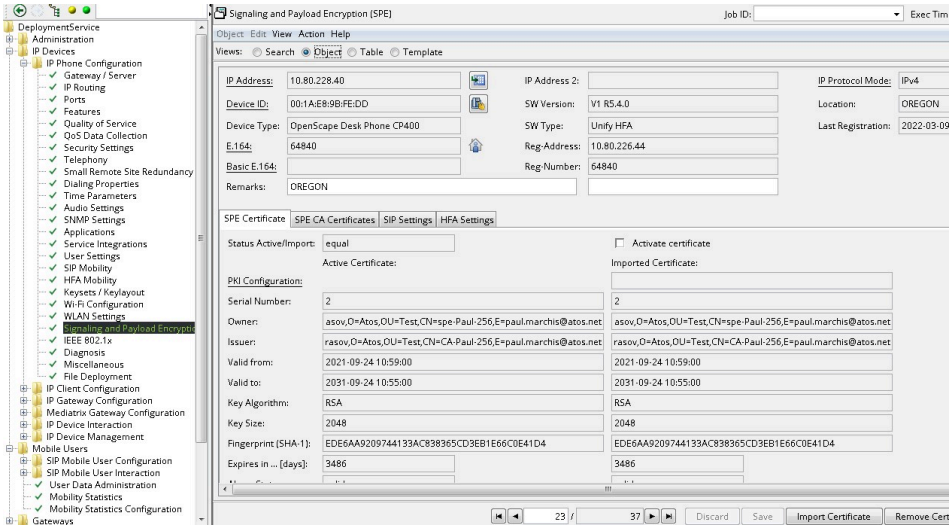


Abbildung 340: DLS-Telefon – Zertifikateinstellung

Zum Importieren neuer oder Umschreiben vorhandener Zertifikate verwenden Sie die Schaltfläche **Import** Certificate (Zertifikat importieren). Klicken Sie im folgenden Bildschirm auf die Schaltfläche **Browse** (Durchsuchen) und wählen Sie das zu importierende Zertifikat aus. Geben Sie das Passwort für den Privatschlüssel ein, aktivieren Sie das Kontrollkästchen **Import certificate to DLS and activate on device** (Zertifikat in DLS importieren und auf dem Gerät aktivieren) und klicken Sie auf **OK**.

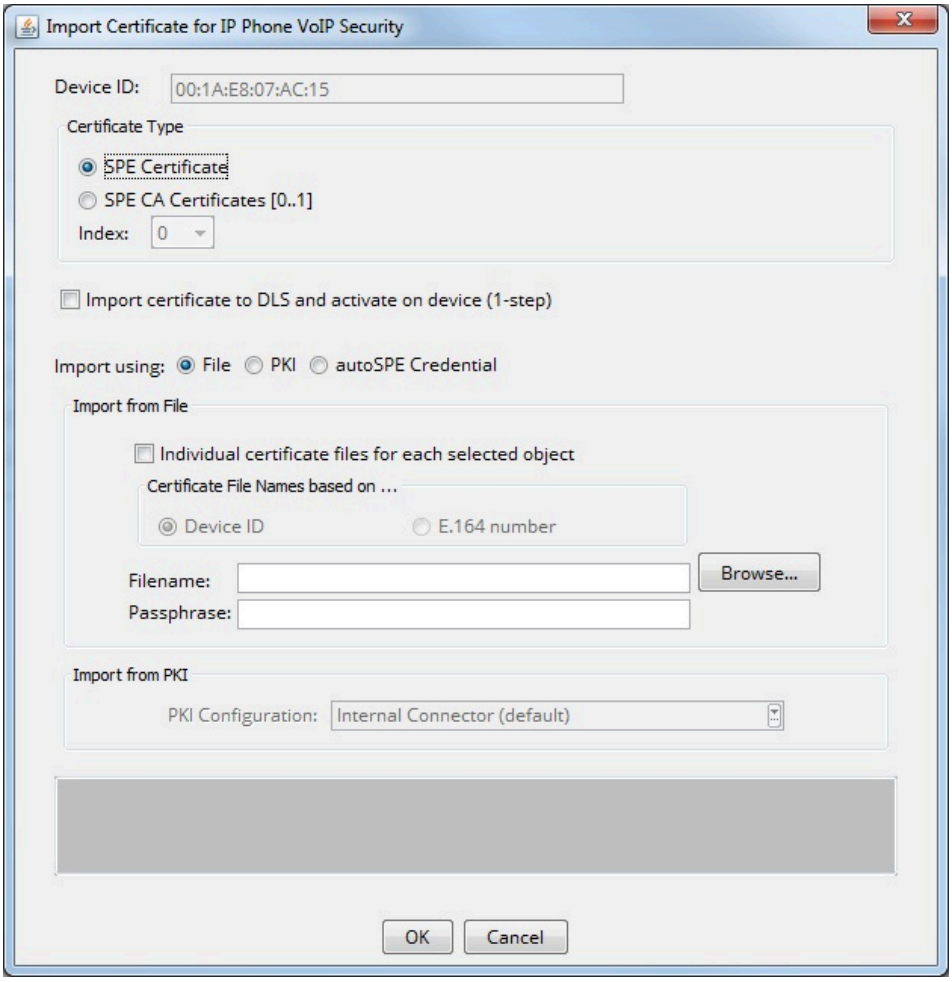


Abbildung 341: DLS-Telefon – Dialogfeld Import Certificate

18.8.4.3 HOCHLADEN DES CA-ZERTIFIKATS

Das CA-Zertifikat für die Verifizierung aufseiten des GW kann nur über den DLS-Server auf das Telefon hochgeladen werden.

Diese Option befindet sich im Menü: **Deployment service > IP Devices > IP Phone Configuration > Signaling & Payload encryption > SPE CA Certificate**

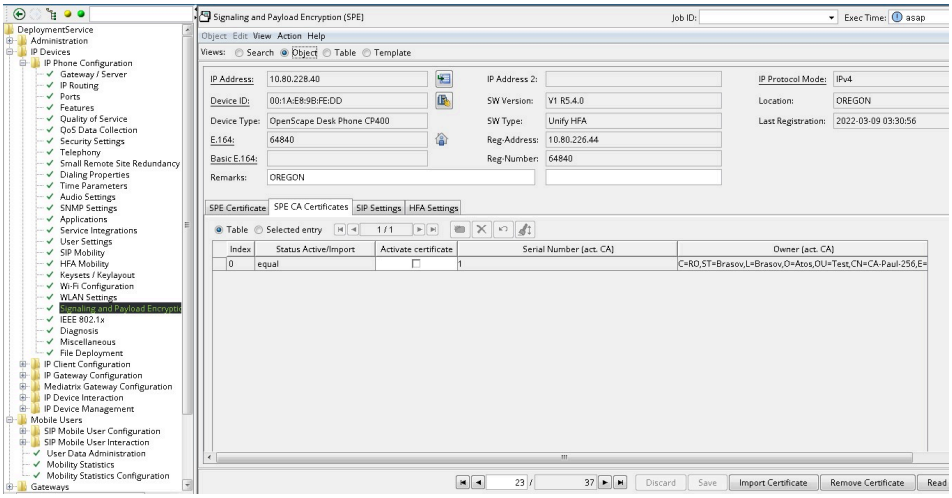


Abbildung 342: DLS-Telefon – CA-Zertifikateinstellung

Zum Importieren neuer CA-Zertifikate oder Umschreiben momentan benutzter CA-Zertifikate verwenden Sie die Schaltfläche **Import Certificate** (Zertifikat importieren). Klicken Sie im folgenden Bildschirm auf die Schaltfläche **Browse** (Durchsuchen) und wählen Sie das zu importierende CA-Zertifikat aus. Aktivieren Sie das Kontrollkästchen **Import certificate to DLS and activate on device** (Zertifikat in DLS importieren und auf dem Gerät aktivieren) und klicken Sie auf **OK**.

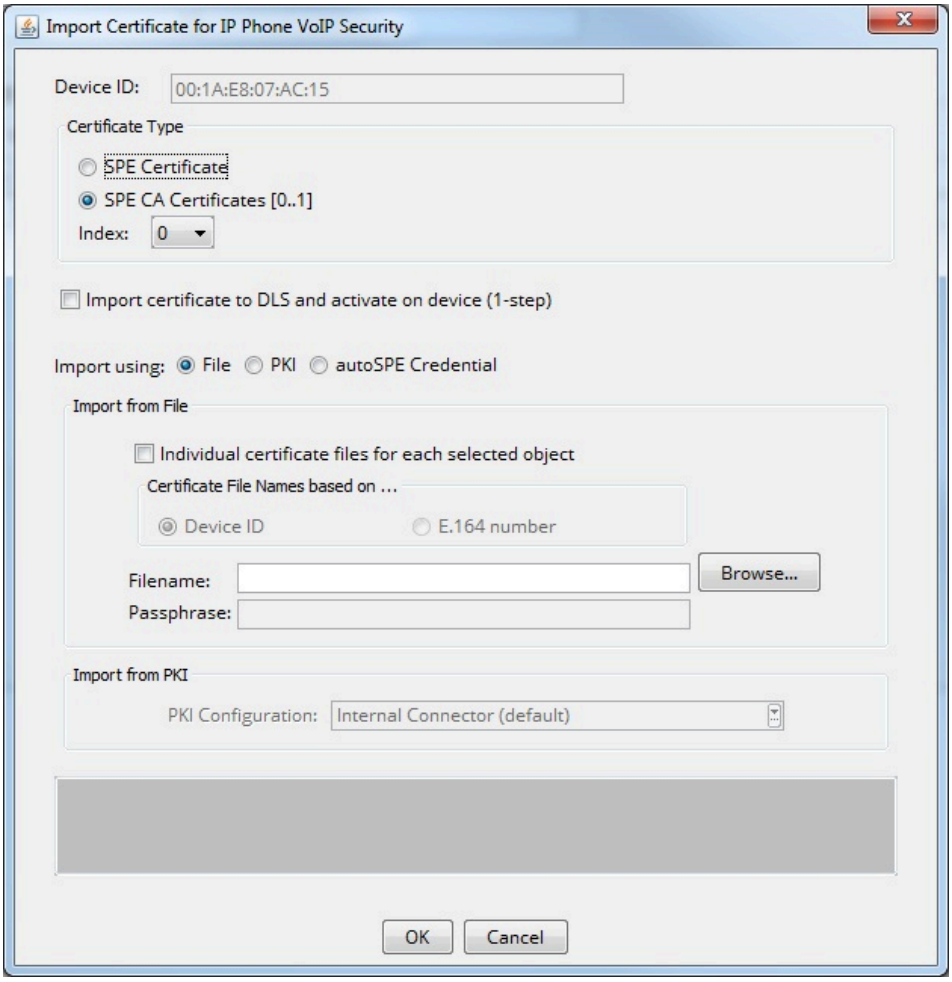


Abbildung 343: DLS-Telefon – Dialogfeld Import CA Certificate

18.8.5 HFA-IMPLEMENTIERUNG

18.8.5.1 CGW

18.8.5.1.1 Konfiguration

MTLS für HFA wird über die Option **Certificate Verification Level** (Zertifikatsprüfungsstufe) im HG3500 WBM indirekt aktiviert oder deaktiviert. Diese Option befindet sich im Menü:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters.

Zum Anpassen der Einstellungen klicken Sie mit der rechten Maustaste auf **SPE Security Setup** (SPE-Sicherheitseinstellungen).

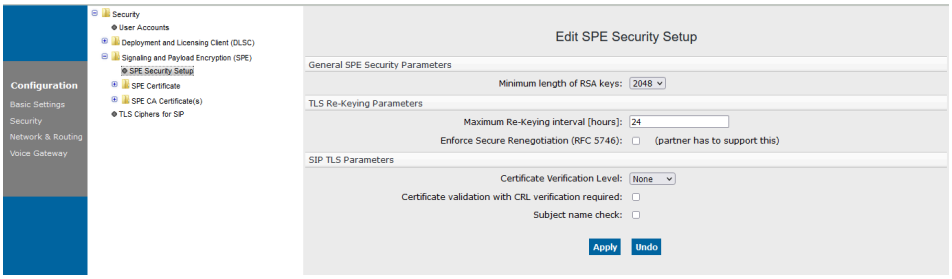


Abbildung 344: HFA SPE-Konfiguration

Wenn die Prüfungsstufe auf **Trusted** (Vertrauenswürdig) oder **Full** (Vollständig) eingestellt ist, wird das während des SSL/TLS-Handshake das Client-Zertifikat angefordert und überprüft. Das Client-Zertifikat muss von einer vertrauenswürdigen CA signiert sein, deren Public-Key-Zertifikat auf dem CGW vorhanden sein muss. (Es können noch weitere CA-Zertifikate vorhanden sein.)

18.8.5.1.2 CA-Zertifikatsverwaltung

Das CA-Zertifikat wird im PEM- oder DER-Format über den HG3500 WBM importiert:

Configuration > Security > Signaling and Payload Encryption (SPE) > Rechtsklick auf **SPE CA Certificate(s) > Import trusted CA certificate (PEM or binary)**



Abbildung 345: HFA SPE – CA-Zertifikat importieren

Klicken Sie im folgenden Bildschirm auf die Schaltfläche „**Browse**...“ (Durchsuchen) und wählen Sie das zu importierende CA-Zertifikat aus. Wenn der CRL-Distributionspunkt für importierte CA-Zertifikate verfügbar ist, wählen Sie die CRL-Verteilungsmethode aus (derzeit wird nur HTTP unterstützt) und tragen Sie in das Textfeld „CDP“ die CDP-Adresse ein.

Wichtig: Bevor das CA-Zertifikat in den CGW importiert wird, muss sein Fingerabdruck überprüft werden, da es in der Folge als vertrauenswürdiges Zertifikat behandelt wird.

Eine Liste der auf dem CGW vorhandenen vertrauenswürdigen Zertifikate finden Sie unter:

Configuration > Security > Signaling and Payload Encryption (SPE) > Doppelklick auf **SPE CA Certificate(s).**

Zum Anzeigen der Details des CA-Zertifikats doppelklicken Sie auf den entsprechenden Listeneintrag. Zum Anzeigen der CDP-Adresse und der Liste derzeit widerrufener Client-Zertifikate klicken Sie auf „*Show CDP and CRL“* (CDP und CRL anzeigen). Sie können ein Zertifikat aus der Liste vertrauenswürdiger Zertifikate entfernen, indem Sie mit der rechten Maustaste

auf den betreffenden Listeneintrag klicken und im Dropdown-Menü den Befehl **„Remove Certificate“ (Zertifikat entfernen) wählen.**

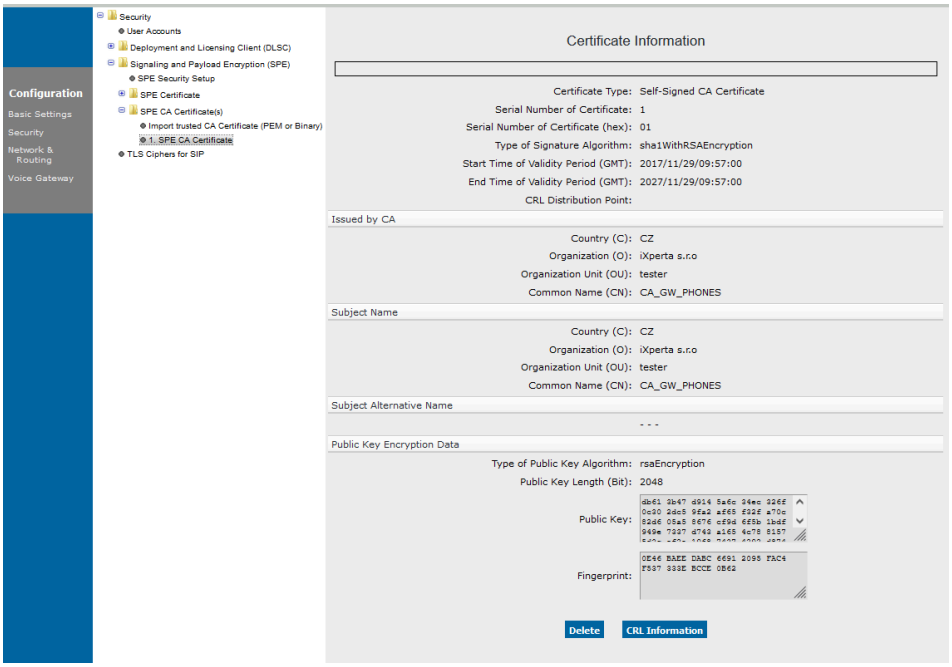


Abbildung 346: HFA SPE – CA-Zertifikat CRL

Die CRL-Prüfung wird mit der folgenden Option aktiviert:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters > Certificate validation with CRL verification required.

Wenn Sie diese Option aktivieren, wird die CRL sofort vom CDP heruntergeladen. Bei aktivierter CRL-Prüfung werden CRL-Updates automatisch in regelmäßigen Zeitabständen heruntergeladen. Beachten Sie, dass CGW derzeit nur die binäre CRL-Version akzeptiert.

18.8.5.1.3 TLSv1.2

Derzeit werden nur die Protokolle TLSv1.0 und höher unterstützt. SSLv2 und SSLv3 sind aufgrund von Sicherheitsproblemen nicht zulässig. Die standardmäßige minimale Länge des RSA-Schlüssels ist 2048.

TLS-Version wird im WBM-Menü konfiguriert:

Configuration > Security > Signaling and Payload Encryption (SPE) > Rechtsklick auf **TLS Ciphers for HFA > Edit TLS Cipher Configuration.**

Im folgenden Bildschirm können die bereitgestellte TLS-Version, die Schlüsselaushandlungsmethode, der Verschlüsselungsalgorithmus und der verwendete Betriebsmodus konfiguriert werden. (Weitere Informationen zu TLSv1.2 finden Sie unter https:// www.ietf.org/rfc/rfc5246.txt.)

Wichtig: Nach dem Ändern und Speichern der TLS HFA-Einstellungen muss das CGW neu gestartet werden, damit die Änderungen in Kraft treten.

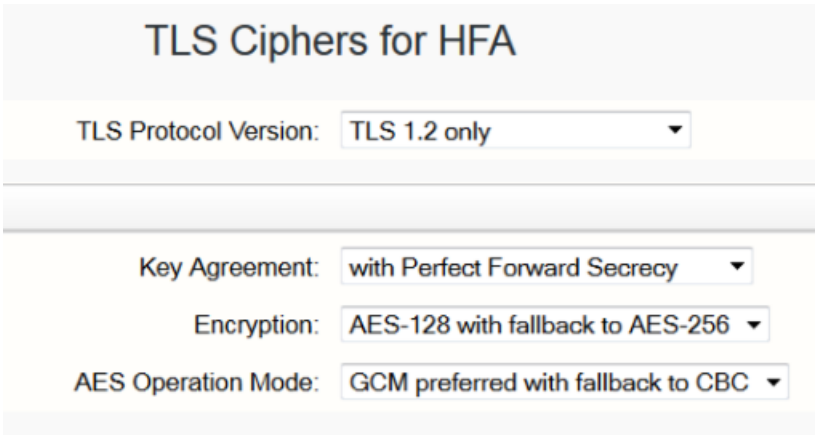


Abbildung 347: HFA SPE-Konfiguration – TLS

18.8.5.1.4 Leistungsmerkmale auf der Stufe Trusted

Wenn MTLS auf der Stufe **Trusted** (Vertrauenswürdig) aktiviert ist, wird das Client-Zertifikat bei jedem SSL/TLS-Handshake (also sowohl beim ersten Handshake als auch bei jeder nachfolgenden Neuaushandlung) angefordert und überprüft.

Das letzte Zertifikat in der vom Client vorgelegten Zertifikatskette muss von einer vertrauenswürdigen CA signiert sein. Keines der Zertifikate in der Kette darf abgelaufen sein, sonst schlägt der Handshake augenblicklich fehl und die Verbindung wird beendet.

Wenn die CRL-Widerrufsprüfung aktiviert ist, werden alle nicht abgelaufenen CRLs geprüft und sämtliche Zertifikate in der Client-Zertifikatskette auf ihren Widerrufsstatus hin untersucht.

Auf der Stufe **Trusted** (Vertrauenswürdig) werden alle (auch unbekannte und kritische) X509v3-Erweiterungen ignoriert.

18.8.5.1.5 Leistungsmerkmale auf der Stufe Full

Wenn MTLS auf Stufe **Full** aktiviert ist, ist das grundlegende Szenario für die Verifizierung von Clients dieselbe wie auf der Stufe **Trusted** (Vertrauenswürdig). Zusätzlich werden während des SSL/TLS-Handshake die X509v3-Erweiterungen des Client-Zertifikats geprüft. Die Zertifikatsprüfung schlägt fehl, wenn eine unbekannte kritische Erweiterung gefunden wird oder die Nutzung bekannter Erweiterungen (basicConstraints, keyUsage, extendedKeyUsage und nsCertType) gegen den aktuellen Standard verstößt.

Die Prüfungsstufe **Full** auf dem Client ermöglicht auch eine Subjekt-Identitätsprüfung des Client basierend auf den im Zertifikat enthaltenen Eigenschaften SubjectAlternativeName oder CommonName. Die Identitätsprüfung ist standardmäßig aktiviert. Dieses Verhalten kann per Kontrollkästchen geändert werden:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > HFA/H.323 TLS Parameters > Subject name check.

Bei der Identitätsprüfung wird versucht, SubjectAlternativeName bzw. CommonName per DNS aufzulösen und die diesem Namen zugeordnete IP-Adresse zu bestimmen. Wenn eine Adresse gefunden wird und diese mit der tatsächlichen IP-Adresse des betreffenden Clients übereinstimmt, gilt die Identitätsprüfung als erfolgreich, andernfalls schlägt der Handshake augenblicklich fehl.

18.8.5.1.6 Dynamisches Verhalten

Dynamische Leistungsmerkmale:

1) Änderung der HFA TLS-Parameter

2)
- Hinzufügen/Entfernen des CA-Zertifikats und des privaten Zertifikats
- Ablauf des CA-Zertifikats und des privaten Zertifikats (betrifft die Schlüssel-Neuaushandlung)
- CRL-Download

Statische Leistungsmerkmale:

- Konfiguration der TLS-Version
- Konfiguration der TLS-Verschlüsselung
- Konfiguration der TLS-Schlüsselaushandlung
- Konfiguration des TLS AES-Betriebsmodus

Eine Änderung statischer Leistungsmerkmale tritt erst nach dem Neustart des CGW in Kraft. Dies wird auch durch ein Symbol in WBM angezeigt. Alle dynamischen Leistungsmerkmale können bei aktivem CGW angepasst werden. Ein solches Ereignis löst einen neuen SSL/TLS-Handshake mit Überprüfung der Client-Zertifikatskette mit allen Folgen für alle aktiven Verbindungen aus. Bei erfolgreichem Handshake sollten bestehende Verbindungen nicht abgebrochen werden.

18.8.5.1.7 Einschränkungen

Subject name check (Subjektnamensprüfung): Bei der Identitätsprüfung wird anhand der IP-Adresse des Telefons der Hostname ermittelt und mit der im Zertifikat angegebenen Eigenschaft SubjectAlternativeName/CommonName verglichen. Dieses Verhalten kann in Zukunft jedoch aufgrund neuer Unify-Empfehlungen geändert werden.

Widerruf: Der CGW akzeptiert nur die binäre CRL-Form im DER-Format (nicht PEM). Die Umwandlung kann z. B. mit dem OpenSSL CRL-Tool vorgenommen werden.

18.8.5.2 SOFTGATE

18.8.5.2.1 Konfiguration

MTLS für HFA wird über die Auswahl im Feld **„Certificate Verification Level“** (Zertifikatsprüfungsstufe) im vHFA WBM indirekt aktiviert oder deaktiviert. Diese Option befindet sich im Menü:

Configuration > SPE > SPE Security Setup > TLS Parameters.

Zum Anpassen der Einstellungen klicken Sie auf das Auswahlfeld **Certificate Verification Level** (Zertifikatsprüfungsstufe) und bestätigen Ihre Auswahl mit der Schaltfläche **Apply** (Übernehmen).

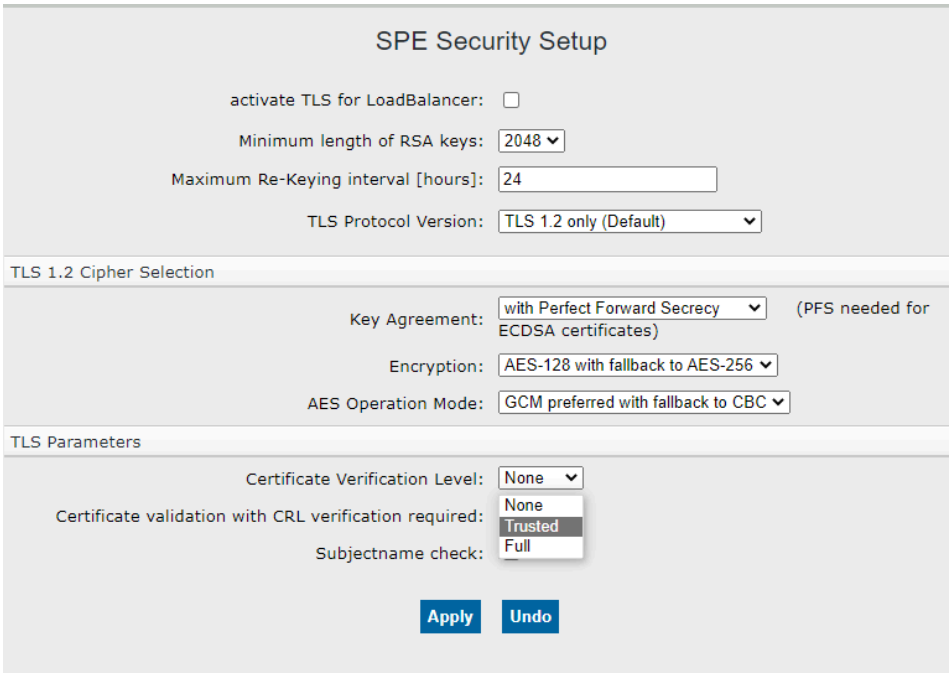


Abbildung 348: SPE-Sicherheit einrichten – Schlüsselzertifikat

Wenn die Prüfungsstufe auf **None** (Keine) eingestellt ist, wird keine Authentifizierung der Remote-Entity durchgeführt. Wenn die Prüfungsstufe auf **Trusted** (Vertrauenswürdig) oder **Full** (Vollständig) eingestellt ist, wird das während des SSL/TLS-Handshake das Client-Zertifikat angefordert und überprüft. Das Client-Zertifikat muss von einer vertrauenswürdigen CA signiert sein, deren Public-Key-Zertifikat auf dem SG vorhanden sein muss. (Es können noch weitere CA-Zertifikate vorhanden sein.)

18.8.5.2.2 CA-Zertifikatsverwaltung

Das CA-Zertifikat wird im PEM- oder DER-Format über den vHFA WBM importiert:

Configuration > SPE > SPE CA Certs > Klicken Sie auf Importieren

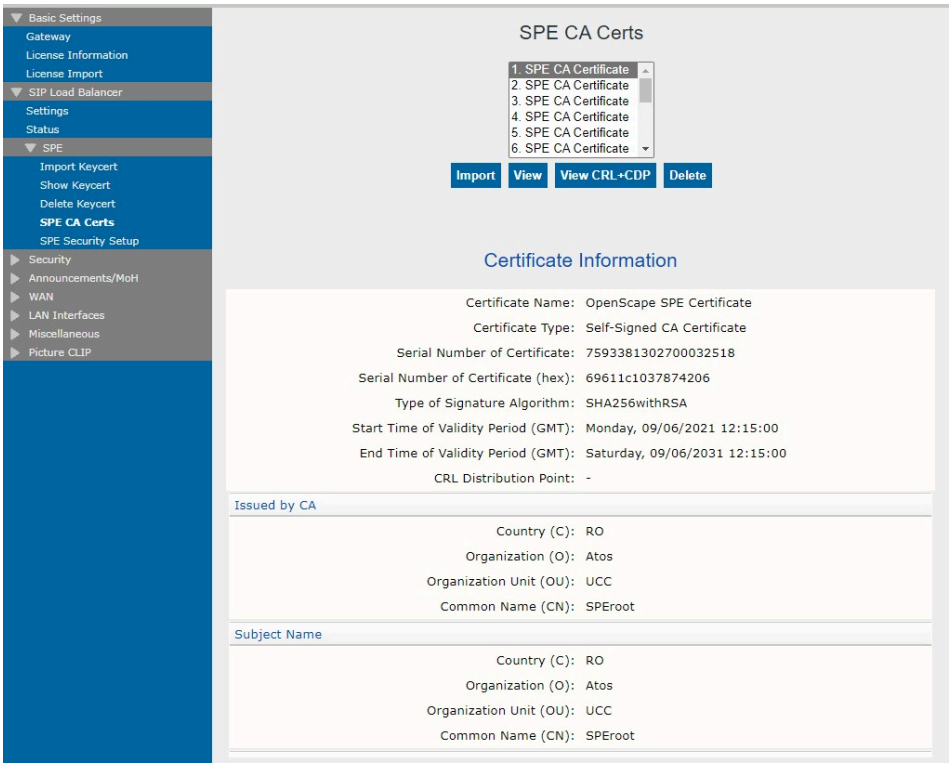


Abbildung 349: SPE CA-Zertifikate importieren

Klicken Sie im folgenden Bildschirm auf die Schaltfläche **Browse** (Durchsuchen) und wählen Sie das zu importierende CA-Zertifikat aus. Wenn der CRL-Distributionspunkt für importierte CA-Zertifikate verfügbar ist, wählen Sie die CRL-Verteilungsmethode aus (derzeit wird nur HTTP unterstützt) und tragen Sie in das Textfeld „CDP“ die CDP-Adresse ein. Bevor das CA-Zertifikat in den CGW importiert wird, muss sein Fingerabdruck durch Klicken auf **View Fingerprint of Certificate** (Fingerabdruck des Zertifikats anzeigen) überprüft werden, da es in der Folge als vertrauenswürdiges Zertifikat behandelt wird!

Eine Liste der auf dem SG vorhandenen vertrauenswürdigen Zertifikate finden Sie unter:

Configuration > SPE > SPE CA Certs

Zum Anzeigen der Details des CA-Zertifikats klicken Sie auf den entsprechenden Listeneintrag. Zum Anzeigen der CDP-Adresse und der Liste derzeit widerrufener Client-Zertifikate klicken Sie auf einen Eintrag in der Liste **SPE CA Certificate** und wählen **View CRL + CDP (CRL + CDP anzeigen).** Sie können ein Zertifikat aus der Liste vertrauenswürdiger Zertifikate entfernen, indem Sie auf den betreffenden Listeneintrag und anschließend auf die Schaltfläche **Delete** (Löschen) klicken.

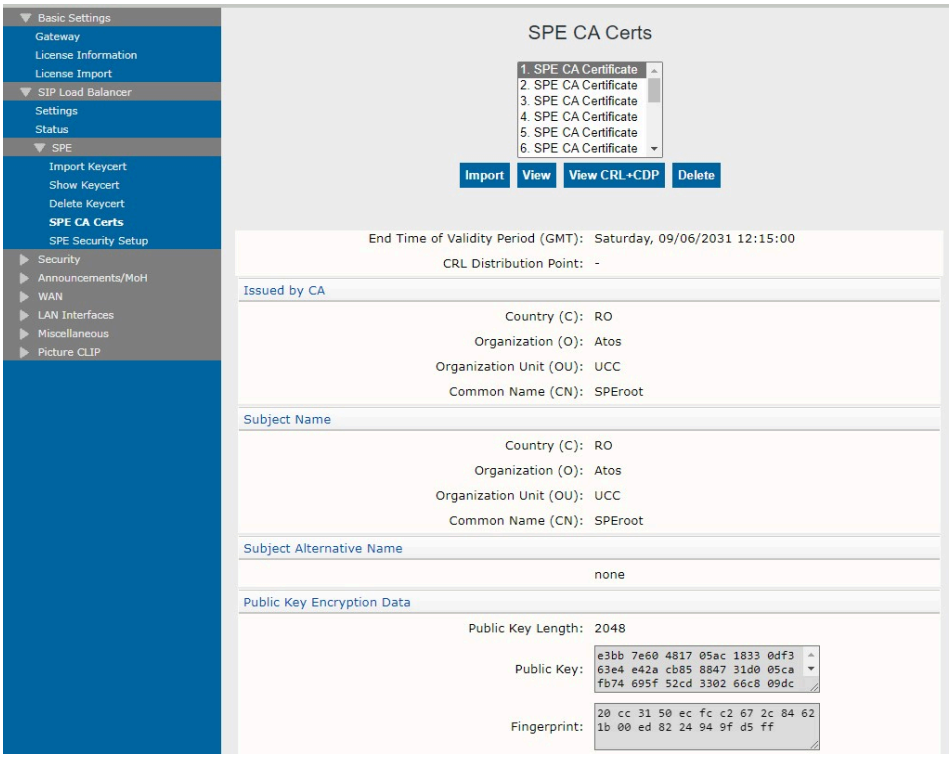


Abbildung 350: SPE – CA-Zertifikate

18.8.5.2.3 TLS

Derzeit werden nur die Protokolle TLSv1.0 und höher unterstützt. SSLv2 und SSLv3 sind aufgrund von Sicherheitsproblemen nicht zulässig. TLS-Version wird im WBM-Menü konfiguriert:

Konfiguration > SPE > SPE-Sicherheitsaufbau

Auf dem folgenden Bildschirm kann die bereitgestellte TLS-Version, die Methode zur Schlüsselvereinbarung, der Verschlüsselungsalgorithmus und der Betriebsmodus konfiguriert werden (weitere Informationen zu TLSv1.2 und TLSv1.3 finden Sie unter https://www.ietf.org/rfc/rfc5246.txt und https://www.ietf.org/rfc/rfc8446.txt).

IMPORTANT: Nach dem Ändern und Speichern von TLS-HFA-Einstellungen, **muss CGW neu gestartet werden,** damit die Änderungen wirksam werden.

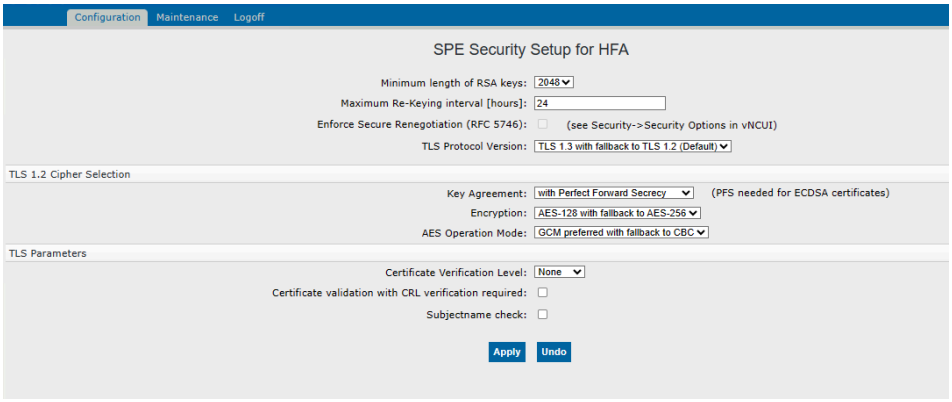


Figure 351: SPE-Sicherheit einrichten – TLS

18.8.5.2.4 Leistungsmerkmale auf der Stufe Trusted

Wenn MTLS auf der Stufe **Trusted** (Vertrauenswürdig) aktiviert ist, wird das Client-Zertifikat bei jedem SSL/TLS-Handshake (also sowohl beim ersten Handshake als auch bei jeder nachfolgenden Neuaushandlung) angefordert und überprüft.

Das letzte Zertifikat in der vom Client vorgelegten Zertifikatskette muss von einer vertrauenswürdigen CA signiert sein. Keines der Zertifikate in der Kette darf abgelaufen sein, sonst schlägt der Handshake augenblicklich fehl und die Verbindung wird beendet.

Wenn die CRL-Widerrufsprüfung aktiviert ist, werden alle nicht abgelaufenen CRLs geprüft und sämtliche Zertifikate in der Client-Zertifikatskette auf ihren Widerrufsstatus hin untersucht.

Auf der Stufe **Trusted** (Vertrauenswürdig) werden alle (auch unbekannte und kritische) X509v3-Erweiterungen ignoriert.

18.8.5.2.5 Leistungsmerkmale auf der Stufe Full

Wenn MTLS auf Stufe **Full** aktiviert ist, ist das grundlegende Szenario für die Verifizierung von Clients dieselbe wie auf der Stufe **Trusted** (Vertrauenswürdig). Zusätzlich werden während des SSL/TLS-Handshake die X509v3-Erweiterungen des Client-Zertifikats geprüft. Die Zertifikatsprüfung schlägt fehl, wenn eine unbekannte kritische Erweiterung gefunden wird.

Die Prüfungsstufe **Full** auf dem Client ermöglicht auch eine Identitätsprüfung des Client basierend auf den im Zertifikat enthaltenen Eigenschaften SubjectAlternativeName oder CommonName.Die Identitätsprüfung ist standardmäßig aktiviert. Die Identitätsprüfung ist standardmäßig aktiviert. Dieses Verhalten kann per Kontrollkästchen geändert werden:

Configuration > SPE > SPE Security Setup > Subject name check.

Bei der Identitätsprüfung wird versucht, SubjectAlternativeName bzw. CommonName per DNS aufzulösen und die diesem Namen zugeordnete IP-Adresse zu bestimmen. Wenn eine Adresse gefunden wird und diese mit der tatsächlichen IP-Adresse des betreffenden Clients übereinstimmt, gilt die Identitätsprüfung als erfolgreich, andernfalls schlägt der Handshake augenblicklich fehl.

18.8.5.2.6 Dynamisches Verhalten

Dynamische Leistungsmerkmale:

1) Änderung der HFA TLS-Parameter

2) • Hinzufügen/Entfernen des CA-Zertifikats und des privaten Zertifikats

- Ablauf des CA-Zertifikats und des privaten Zertifikats (betrifft die Schlüssel-Neuaushandlung)
- CRL-Download

Statische Leistungsmerkmale:

- Konfiguration der TLS-Version
- Konfiguration der TLS-Verschlüsselung
- Konfiguration der TLS-Schlüsselaushandlung
- Konfiguration des TLS AES-Betriebsmodus

Eine Änderung statischer Leistungsmerkmale tritt erst nach dem Neustart des SG in Kraft. Dies wird auch durch ein Symbol in WBM angezeigt. Alle dynamischen Leistungsmerkmale können bei aktivem SG angepasst werden. Ein solches Ereignis löst einen neuen SSL/TLS-Handshake mit Überprüfung der Client-Zertifikatskette mit allen Folgen für alle aktiven Verbindungen aus. Bei erfolgreichem Handshake sollten bestehende Verbindungen nicht abgebrochen werden.

18.8.5.2.7 Einschränkungen

Subject name check (Subjektnamensprüfung): dieses Leistungsmerkmal ist für vHFA derzeit noch nicht verfügbar.

18.8.6 UFA-IP-Implementierung

18.8.6.1 CGW und SoftGate

18.8.6.1.1 Konfiguration

MTLS für HFA wird über die Option Certificate Verification Level (Zertifikatsprüfungsstufe) im HG3500 WBM indirekt aktiviert oder deaktiviert. Diese Option befindet sich im Menü:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup

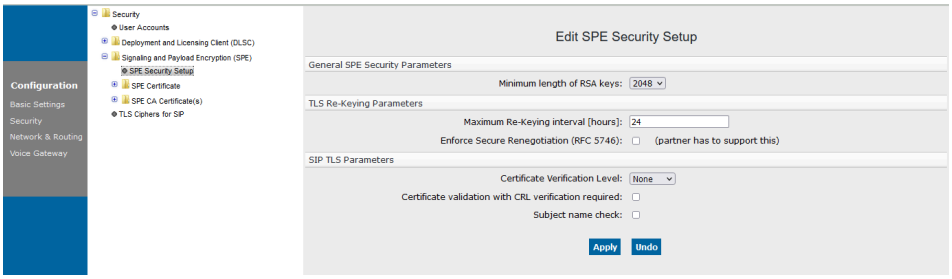


Abbildung 352: Edit SPE Security Setup

Wenn die Prüfungsstufe auf Trusted (Vertrauenswürdig) oder Full (Vollständig) eingestellt ist, wird während des SSL/TLS-Handshakes das Client-Zertifikat angefordert und überprüft. Das Client-Zertifikat muss von einer vertrauenswürdigen CA signiert sein, deren Public-Key-Zertifikat auf dem GW vorhanden sein muss. (Es können noch weitere CA-Zertifikate vorhanden sein.)

18.8.6.1.2 CA-Zertifikatsverwaltung

Das CA-Zertifikat wird im PEM- oder DER-Format über den HG3500 WBM importiert:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE CA Certificate(s) > Import trusted CA certificate (PEM or binary)

Klicken Sie im folgenden Bildschirm auf die Schaltfläche Browse (Durchsuchen) und wählen Sie das zu importierende CA-Zertifikat aus. In der aktuellen Version wird die CRL-Prüfung nicht unterstützt; die Unterstützung ist geplant für V7R3.

Wichtig: Bevor das CA-Zertifikat in den CGW importiert wird, muss sein Fingerabdruck überprüft werden, da es in der Folge als vertrauenswürdiges Zertifikat behandelt wird!



Abbildung 353: Import trusted CA certificate (PEM or binary)

Eine Liste der auf dem GW vorhandenen vertrauenswürdigen Zertifikate finden Sie unter:

Configuration > Security > Signaling and Payload Encryption (SPE) > Rechtsklick auf SPE CA Certificate(s) > Load a SPE CA Certificate via HTTP

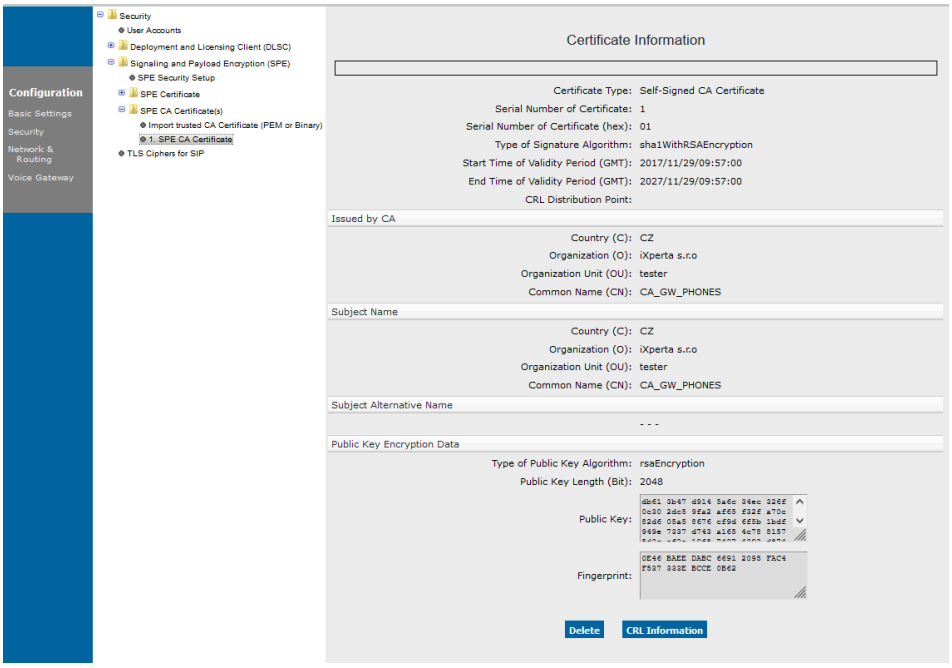


Abbildung 354: Zertifikatsinformationen

Zum Anzeigen der Details des CA-Zertifikats doppelklicken Sie auf den entsprechenden Listeneintrag. Sie können ein Zertifikat aus der Liste

vertrauenswürdiger Zertifikate entfernen, indem Sie auf den betreffenden Listeneintrag und anschließend auf die Schaltfläche Delete (Löschen) klicken.

18.8.6.1.3 TLS

Derzeit werden nur die Protokolle TLSv1.0 und höher unterstützt. SSLv2 und SSLv3 sind aufgrund von Sicherheitsproblemen nicht zulässig. Die standardmäßige minimale Länge des RSA-Schlüssels ist 2048.

TLS-Version wird im WBM-Menü konfiguriert:

Konfiguration > Sicherheit > Signalisierung und Nutzlast-Verschlüsselung (SPE) > klicken Sie mit der rechten Maustaste auf TLS-Chiffren für SIP > Bearbeiten Sie die TLS-Chiffre-Konfiguration.

Auf dem folgenden Bildschirm kann die bereitgestellte TLS-Version, die Methode zur Schlüsselvereinbarung, der Verschlüsselungsalgorithmus und der Betriebsmodus konfiguriert werden (weitere Informationen zu TLSv1.2 und TLSv1.3 finden Sie unter https://www.ietf.org/rfc/rfc5246.txt und https://www.ietf.org/rfc/rfc8446.txt).

IMPORTANT: Nach dem Ändern und Speichern der TLS-SIP-Einstellungen muss GW neu gestartet werden, damit die Änderungen wirksam werden!

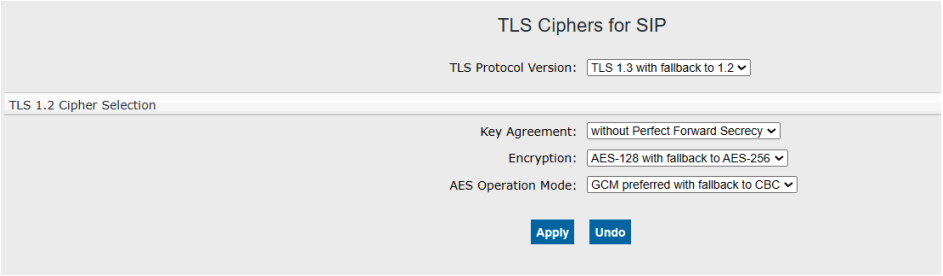


Figure 355: TLS Ciphers for SIP (TLS-Chiffren für SIP)

Ab V11R0 wird TLS Version 1.3 auf den VoIP-Schnittstellen (HFA und SIP) unterstützt.

NOTICE: TLS1.3-Chiffren können nicht konfiguriert werden (Einstellungen beheben).

18.8.6.1.4 Leistungsmerkmale auf der Stufe Trusted

Wenn MTLS auf der Stufe Trusted (Vertrauenswürdig) aktiviert ist, wird das Client-Zertifikat bei jedem SSL/TLS-Handshake (also sowohl beim ersten Handshake als auch bei jeder nachfolgenden Neuaushandlung) angefordert und überprüft.

Das letzte Zertifikat in der vom Kunden bereitgestellten Zertifikatskette muss von einer vertrauenswürdigen CA signiert sein und darf nicht abgelaufen sein, andernfalls schlägt der Handshake augenblicklich fehl und die Verbindung wird getrennt.

Falsche X509v3-Erweiterungen und unbekannte kritische X509v3-Erweiterungen werden aufgrund des zugrunde liegenden Frameworks auf der Stufe Trusted nicht ignoriert (obwohl dies eigentlich der Fall sein sollte).

18.8.6.1.5 Leistungsmerkmale auf der Stufe Full

Wenn MTLS auf Stufe Full aktiviert ist, ist das grundlegende Szenario für die Verifizierung von Clients dieselbe wie auf der Stufe Trusted (Vertrauenswürdig). Zusätzlich werden während des SSL/TLS-Handshake die X509v3-Erweiterungen des Client-Zertifikats geprüft. Die Zertifikatsprüfung schlägt fehl, wenn eine unbekannte kritische Erweiterung gefunden wird oder die Nutzung bekannter Erweiterungen (basicConstraints, keyUsage, extendedKeyUsage und nsCertType) gegen den aktuellen Standard verstößt.

Die Prüfungsstufe Full auf dem Client ermöglicht auch eine Identitätsprüfung des Client basierend auf den im Zertifikat enthaltenen Eigenschaften SubjectAlternativeName oder CommonName. Die Identitätsprüfung ist standardmäßig aktiviert. Dieses Verhalten kann per Kontrollkästchen geändert werden:

Configuration > Security > Signaling and Payload Encryption (SPE) > SPE Security Setup > SIP TLS Parameters > Subject name check.

Bei der Identitätsprüfung wird versucht, SubjectAlternativeName bzw. CommonName per DNS aufzulösen und die diesem Namen zugeordnete IP-Adresse zu bestimmen. Wenn eine Adresse gefunden wird und diese mit der tatsächlichen IP-Adresse des betreffenden Clients übereinstimmt, gilt die Identitätsprüfung als erfolgreich, andernfalls schlägt der Handshake augenblicklich fehl.

18.8.6.1.6 Leistungsmerkmale

1) Hinzufügen/Entfernen des CA-Zertifikats und des privaten Zertifikats

2)
- Änderung der SIP TLS-Parameter
- Ablauf des CA-Zertifikats und des privaten Zertifikats (betrifft die Schlüssel-Neuaushandlung)
- Konfiguration der TLS-Version
- Konfiguration der TLS-Verschlüsselung
- Konfiguration der TLS-Schlüsselaushandlung
- Konfiguration des TLS AES-Betriebsmodus

Eine Leistungsmerkmaländerung tritt erst nach dem Neustart des GW in Kraft. Dies wird auch durch ein Symbol in WBM angezeigt. Alle dynamischen Leistungsmerkmale können bei aktivem GW angepasst werden. Ein solches Ereignis löst einen neuen SSL/TLS-Handshake mit Überprüfung der Client-Zertifikatskette mit allen Folgen für alle aktiven Verbindungen aus. Bei erfolgreichem Handshake sollten bestehende Verbindungen nicht abgebrochen werden.

18.8.6.1.7 Einschränkungen

Widerruf: In der aktuellen Version wird die Zertifikatwiderrufsprüfung NICHT unterstützt; die Unterstützung ist geplant für V7R3.

19 Payload Switching DMC

19.1 Leistungsmerkmalbeschreibung

Zur Unterstützung des Leistungsmerkmals „Payload Switching“ wird in OpenScape 4000 für Voice over IP (VoIP)-Verbindungen das Leistungsmerkmal DMC (Direct Media Connection) verwendet.

Die Funktion DMC lässt sich wie folgt beschreiben:

1) Die Payload (Sprachkanal) einer OpenScape 4000-internen oder netzweiten Sprachverbindung wird über ein LAN vermittelt, in welchem eine direkte IP-Verbindung ohne vorherige Umwandlung in einen TDM-Datenstrom möglich ist.

Bei Verwendung des Leistungsmerkmals „DMC Any-to-any“ werden in einem HiPath 4000-/OpenScape 4000-Netz die Payload-Daten ohne mehrmalige IP-TDM-Umwandlung direkt zwischen den IP-Endpunkten befördert. Diese direkte Payload-Verbindung bezeichnet man als Direct Media Connection (DMC).

DMC hat zwei Ziele:

- Verminderung der Sprachqualität verhindern, indem die Anzahl der IP/TDM Hops/Konvertierungen minimiert wird.
- Optimierung der Bandbreite: in diesem Fall ist die Aktivierung von VAD sehr wichtig.

19.2 Direct Media Connect (DMC) in Verbindung mit HFA-Teilnehmer

19.2.1 Leistungsmerkmalbeschreibung

19.2.1.1 Hintergrund

Ohne die Funktion „DMC (Direct Media Connection)“ würde bei einer Gesprächsverbindung zwischen zwei HFA IP-Telefonen eine zweimalige IP/TDM-Umwandlung erfolgen. Die mehrmalige Umwandlung der Payload von IP auf TDM und wieder zurück führt zu einem spürbaren Qualitätsverlust bei der Sprachübertragung. Um diesen Qualitätsverlust zu vermeiden, wird die IP Payload, wenn es sich um eine normale Zweierverbindung handelt, direkt zwischen den beiden Teilnehmern vermittelt.

Als IP-Endpunkte kommen in Frage:

- HFA IP-Telefone
- IP Trunking-Gateways (z.B.: HG 3500)
- IPDA-Baugruppen (z.B.: HG 3500)

Die IP-Endpunkte können dabei als Endpunkte der Verbindung (d.h. es besteht eine Master-Verbindung zwischen den beiden IP-Telefonen) oder lediglich als Endpunkte innerhalb eines Abschnitts der Master-Verbindung fungieren.

Beispielsweise kann ein Anate oder Digite die Funktion DMC nutzen, wenn das Endgerät über einen IPDA Access Point oder ein IP Trunking-Gateway mit dem Gegenteilnehmer verbunden ist.

Der Verbindungsaufbau erfolgt bei einem Gespräch in mehreren Schritten.

Bei den Schritten 1 und 2 handelt es sich um das normale Verfahren beim Verbindungsaufbau in HiPath 4000 V1.0. Das Ergebnis wird als Master-Verbindung bezeichnet. Der normale Verbindungsaufbau wird nun um die Schritte 3 und 4 ergänzt, mit denen die optionale Direct Media Connection aufgebaut wird.

1) In einem ersten Schritt wird eine Signalisierungsverbindung zwischen den Teilnehmern hergestellt.

2) Parallel zu der Signalisierungsverbindung wird für die Payload eine so genannte Master-Verbindung (Master Connection, MC) hergestellt. Der Payload-Pfad der Master-Verbindung kann in einen TDM-Pfad und einen IP-Pfad aufgeteilt werden:

3)
- in einem TDM-Netz ist dies ein bestimmter B-Kanal
- in einem IP-Netz ist dies eine RTP-Verbindung.

Die RTP-Payloadverbindung wird über H.323-Verfahren (insbesondere über das Fast Connect-Verfahren) hergestellt und kontrolliert.

4) Nachdem die Master-Verbindung zwischen den beiden Teilnehmern hergestellt und durchgeschaltet wurde (d.h. die beiden Teilnehmer befinden sich im Gesprächszustand), kann zwischen den IP-Endpunkten der Master-Verbindung eine DMC-Verbindung hergestellt werden. Der Aufbau der DMC-Verbindung wird hierbei von dem IP-Endpunkt eingeleitet, der den Anruf empfangen hat.

5) Nach erfolgtem Aufbau der DMC-Verbindung wird die Payload über die H.323-Verbindung befördert. Die Master-Verbindung bleibt parallel dazu bestehen. Über diese Verbindung wird jedoch keine Payload transportiert, solange die DMC-Verbindung besteht; die Master-Verbindung befindet sich gewissermaßen in einem Standby-Modus.

6) Wird die Gesprächsverbindung ausgelöst (z.B. zum Aufbau einer Rückfrageverbindung), schaltet der IP-Endpunkt umgehend auf die Master-Verbindung um und löst die DMC-Verbindung aus.

19.2.1.2 Hinweise zu Direct Media Connection DMC

- Die DMC-Verbindung wird bei einer Zweierverbindung durchgeschaltet, also bei einem Basic Call und bei einer einfachen Rückfrageverbindung. Außerdem wird eine DMC durchgeschaltet, wenn der Verbindungsaufbau über ein Leistungsmerkmal wie Anrufumleitung oder Anrufübernahme in der Gruppe erfolgt oder wenn von einem Zweitanschluss ein Anruf auf ein Keyset abgefragt wird. Bei **Konferenzverbindungen** ist DMC auch möglich.
- Befinden sich die Gesprächsteilnehmer in einer anderen Verbindung als in einer Zweierverbindung, wird eine IP/TDM-Umwandlung durchgeführt. Die Vermittlung erfolgt dann über das TDM-Koppelfeld (MTS).
- Wurde eine Direct Media Connection hergestellt, muss der Verbindungsweg über das MTS-Koppelfeld für die mehrmalige IP/TDM-Umwandlung (Master-Verbindung) parallel zur IP-Direktverbindung durchgeschaltet bleiben, damit nach Beendigung des Gesprächszustands zwischen beiden Teilnehmern die MTS mit ihren Ton- und Konferenzfunktionen für die Leistungsmerkmalsteuerung durch die Vermittlungstechnik sofort zur Verfügung steht.

- DMCs werden auch für Fax- und Modemverbindungen hergestellt.

19.2.1.3 Überlegungen zur Bandbreite

19.2.1.3.1 Allgemeine Hinweise

Solange eine DMC besteht, werden über die Master-Verbindung nur SID (Silence Insertion Descriptor)-/CN (Comfort Noise)-Frames gesendet, wenn die beteiligten Komponenten mit VAD konfiguriert wurden (siehe Abschnitt 2.3.3, „Sprachpausenerkennung (Voice Activity Detection, VAD)“). Somit benötigt die Master-Verbindung nur eine beschränkte Bandbreite.

Die Tabellen für den Bandbreitenbedarf finden Sie im Dokument „Gateways HG 3500 und HG 3575“, Abschnitt 2.5.4, „Bandbreitenbedarf pro Verbindung“.

Weitere Informationen zu Bandbreitenverwaltung finden Sie im Ressourcen-Manager und in AMO GKTOP.

Durch Einfügen der SID/CN wird bei Stille ein analoges Hintergrundgeräusch simuliert, an dem der Listener erkennt, dass die Verbindung aktiv und betriebsbereit ist. Die RTP-Pakete mit CN-Flag für das Hintergrundgeräusch werden einmal pro Sekunde über die Master- oder Slave-Verbindung übertragen.

19.2.1.3.2 Gateways

Nur DMC-Endpunkte sind in der Lage, DMC-Verbindungen zu erkennen und die Bandbreite der Master-Verbindung entsprechend zu verringern.

Wenn es sich bei dem Gateway nicht um einen DMC-Endpunkt handelt, was beispielsweise in einem Multihop-Szenario der Fall sein kann, erkennt das Gateway die DMC-Verbindung **NICHT**. Zur Verringerung des Bandbreitenbedarfs sollten die Gateways mit einem VAD-fähigen Codec konfiguriert werden. Außerdem muss die VAD-Funktion aktiviert werden (die in diesem Fall zu dem Gateway leitet, das die CN-Pakete generiert).

Wichtig: HG 3530 ist nie ein DMC-Endpunkt.

In AMO CGWB werden folgende ASC-Einstellungen empfohlen:

Tabelle 88: Empfohlene ASC-Einstellungen in AMO CGWB

PRIO1:	CODEC = G711A	VAD = YES	RTP-SIZE = 30
PRIO2:	CODEC = G729AB	VAD = YES	RTP-SIZE = 20
PRIO3:	CODEC = G723	VAD = YES	RTP-SIZE = 30
PRIO4:	CODEC = NONE	VAD = NO	RTP-SIZE = 20
PRIO5:	CODEC = NONE	VAD = NO	RTP-SIZE = 20
PRIO6:	CODEC = NONE	VAD = NO	RTP-SIZE = 20

PRIO7:	CODEC = G729A	VAD = NO	RTP-SIZE = 20**

** Diese Einstellung sollte entfernt werden, wenn Bandbreitenreduktion immer gewünscht wird. In diesem Fall **muss** auf dem Telefon jedoch die Sprechpausenerkennung (VAD) wie unter Abschnitt 2.3.3, „Sprachpausenerkennung (Voice Activity Detection, VAD)“ beschrieben aktiviert werden, weil folgende Funktionen erforderlich sind:

- G729AB: **VAD = YES** in AMO CGWB, wenn das Kontrollkästchen für die Sprechpausenerkennung auf den Telefonen aktiviert wird.

oder

- G729A: **VAD = NO** in AMO CGWB, wenn das Kontrollkästchen für die Sprechpausenerkennung auf den Telefonen nicht aktiviert wird.

Anmerkung: Wenn bei G729AB nur **VAD = YES** in AMO CGWB eingestellt und das Kontrollkästchen für die Sprechpausenerkennung auf den Telefonen **nicht aktiviert** ist, schlagen alle Verbindungsversuche mit dem Code HY2 (keine Bearer Capabilities) in der Anzeige fehl.

19.2.1.3.3 HFA

optiPoint-Telefone generieren CN Frames auf der Master-Verbindung, sobald die DMC-Verbindung hergestellt ist.

OpenStage-Telefone generieren bei bestehender DMC-Verbindung **keine** CN-Frames auf der Master-Verbindung.

Der Versand von CN-Frames über normale Verbindungen und DMC-Slave-Verbindungen wird durch die VAD-Einstellung in AMO SDAT gesteuert.

Der DSP (Digital Signal Processor) des Telefons akzeptiert VAD für G711, G729 oder G723 unabhängig von der VAD SDAT-Einstellung. Für G722 ist VAD nicht definiert.

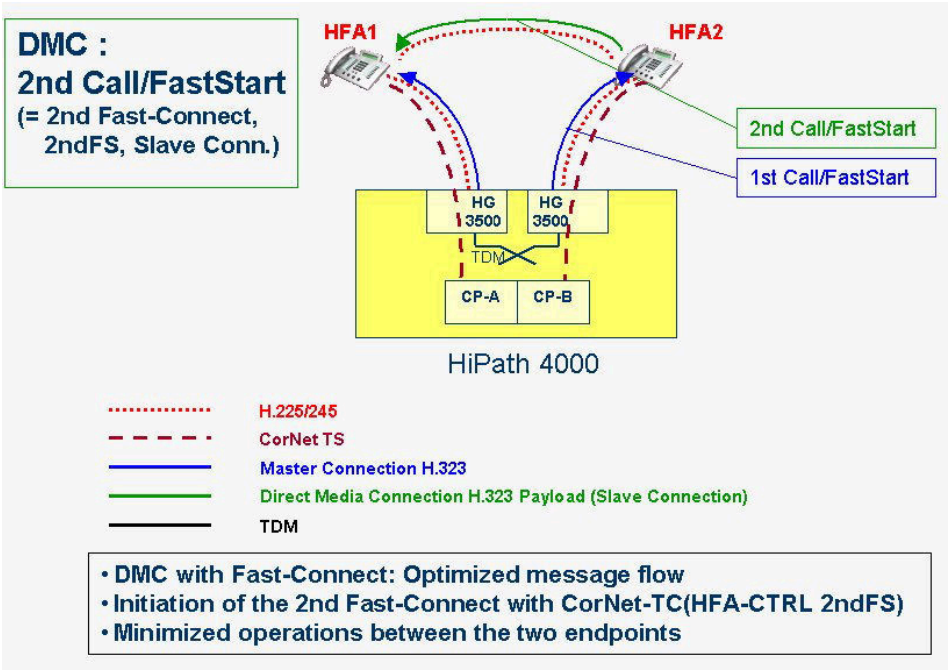
Codecs und Sprechpausenerkennung

- G711 – Hochwertiger Codec mit Unterstützung für Sprechpausenerkennung (VAD) und Comfort Noise Generation (CN)
- G723.1 – Audio-Codec für Sprache mit Sprachaudiokomprimierung in 30-ms-Frames sowie Unterstützung für Sprechpausenerkennung (VAD) und Comfort Noise Generation (CN); keine zuverlässige Übertragung von Musik oder Tönen (z. B. DTMF oder Fax).
- G729 – Codec mit Sprachkomprimierung ohne Unterstützung für Sprechpausenunterdrückung (VAD implizit deaktiviert)
- G729A – Codec mit Sprachkomprimierung ohne Unterstützung für Sprechpausenunterdrückung (VAD implizit deaktiviert)
- G729B – Codec mit Sprachkomprimierung und Unterstützung für Sprechpausenunterdrückung (VAD) – nicht kompatibel mit G729 oder G729A
- G729AB – Codec mit Sprachkomprimierung und Unterstützung für Sprechpausenunterdrückung (VAD) – nur kompatibel mit G729B

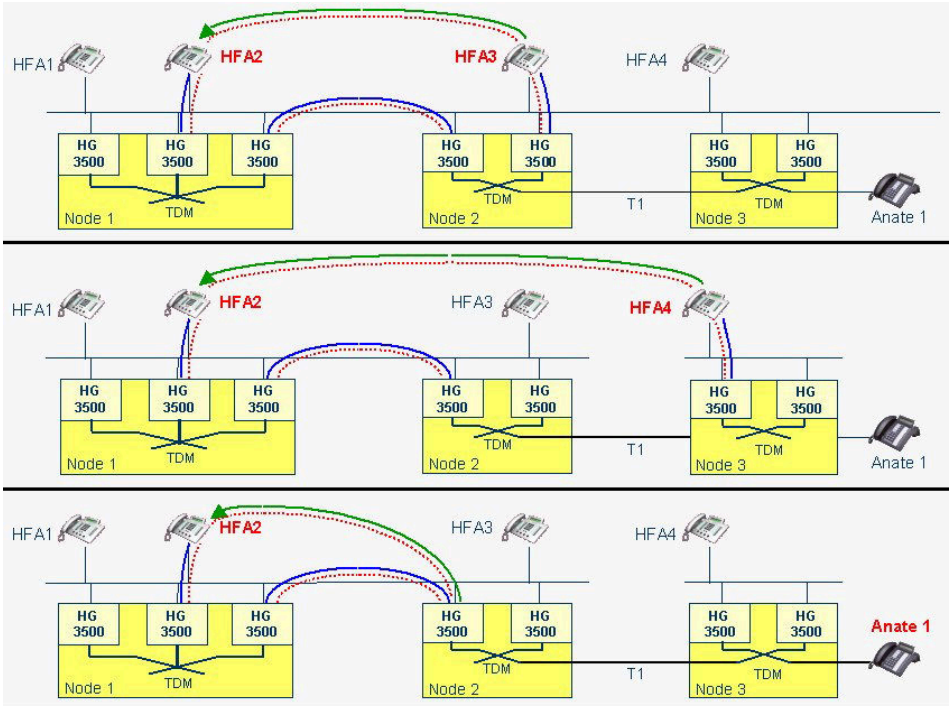
19.2.1.4 Szenarien

Es werden folgende Szenarien betrachtet:

Szenario A: Direct Media Connection (DMC) innerhalb desselben OpenScape 4000-Knotens

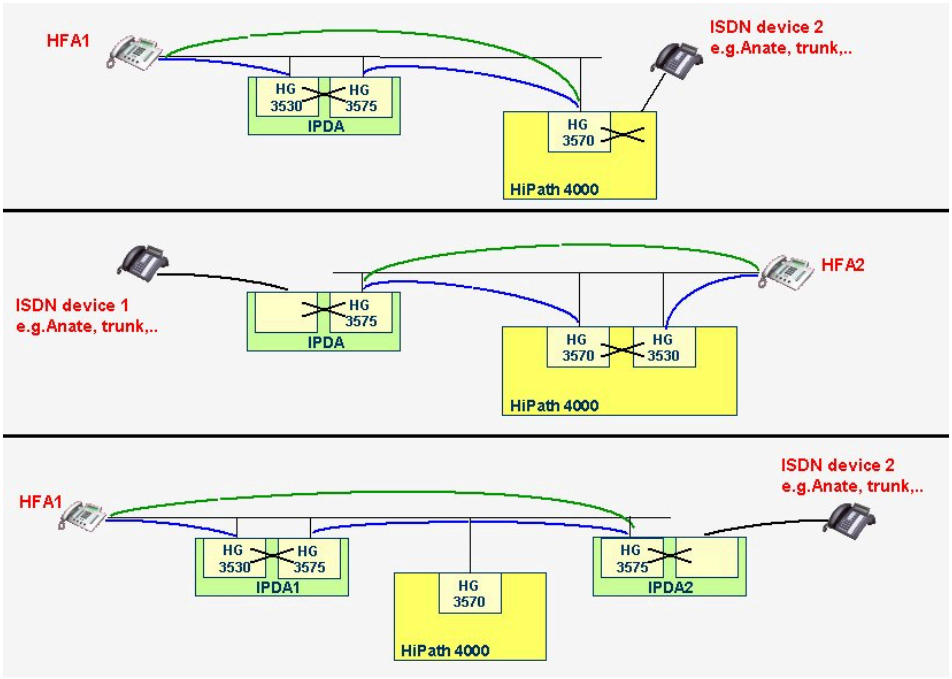


Szenario B: Direct Media Connection (DMC) zwischen HFA IP-Telefonen in einem HiPath 4000-/OpenScape 4000-Netz

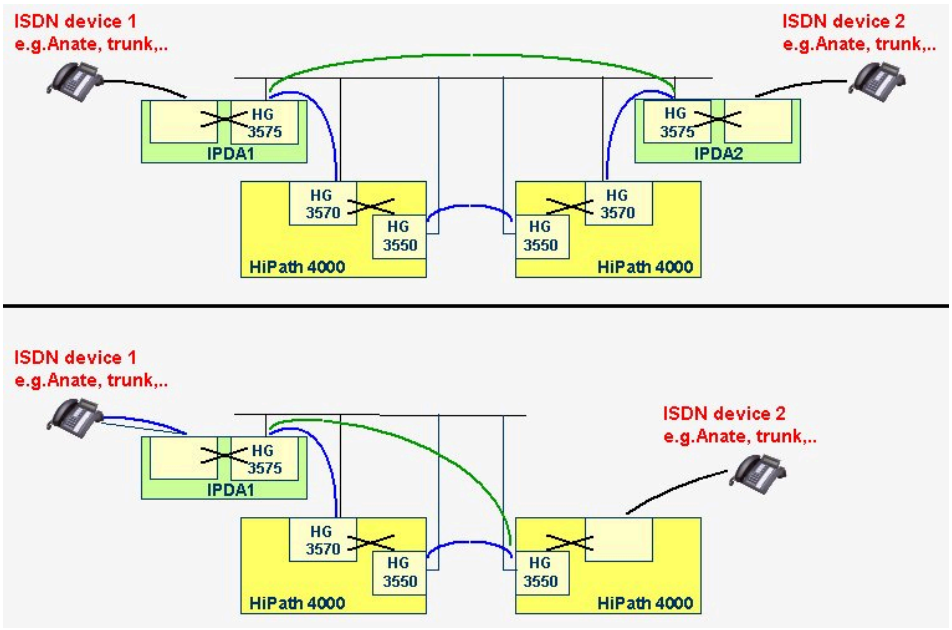


Dieses Szenario wird bei OpenScape 4000 in Verbindung mit dem IP-Gateway HG 3500 unterstützt.

Szenario C: Direct Media Connection (DMC) zwischen HFA IP-Telefon und IPDA-Shelf innerhalb desselben OpenScape 4000-Knotens

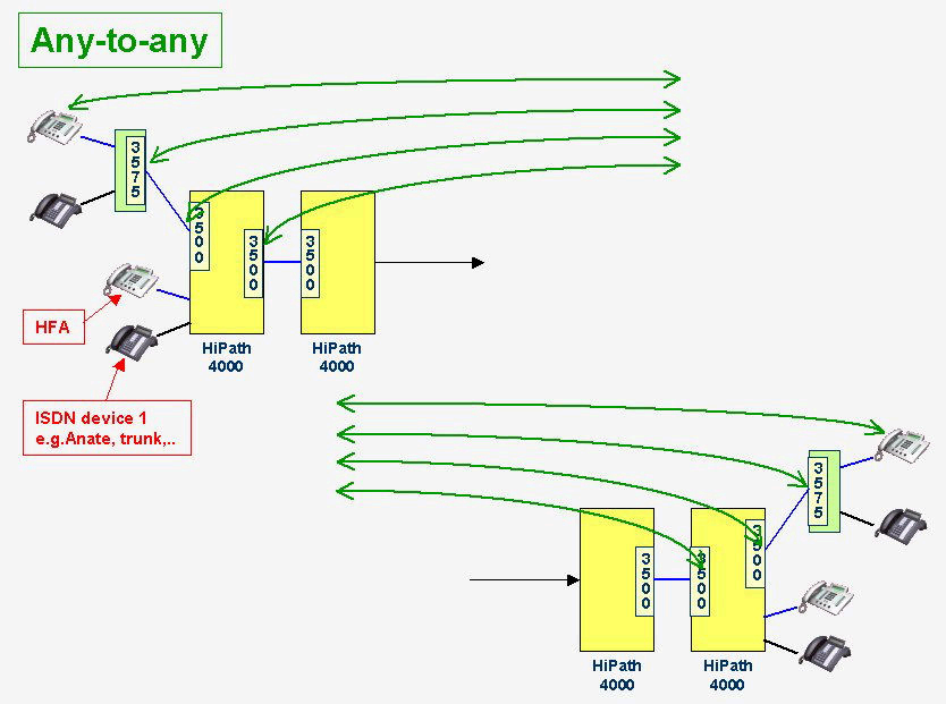


Szenario D: Direct Media Connections (DMC) zwischen IPDA-Shelves netzweit



DMC in gemischten Szenarien

Bei gemischten Szenarien erfolgt die DMC bei einer Zweierverbindung im Gesprächszustand zwischen der erstmöglichen IP-Adresse auf der A-Teilnehmerseite (IP-Telefon, HG 3575, HG 3500 (FUNCTION=HG3570) oder HG 3500 (FUNCTION=HG3550)) und der letztmöglichen IP-Adresse auf der B-Teilnehmerseite (ebenfalls HG 3500 (FUNCTION=HG3550), HG 3500 (FUNCTION=HG3570), HG 3575 oder IP-Telefon).

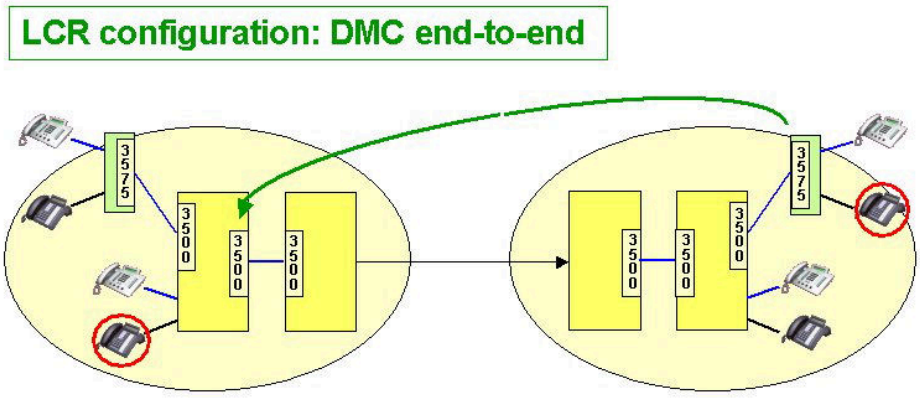


19.2.1.5 Domänenkonzept

Bei sehr großen Unternehmensnetzen muss das Netzwerk unter Umständen in mehrere Domänen aufgeteilt werden. Je nach der Konfiguration können DMC-Verbindungen innerhalb einzelner Domänen oder durchgehend über mehrere Domänen hinweg zugelassen werden.

Beispiel 1: DMC möglich von Domäne A auf Domäne B

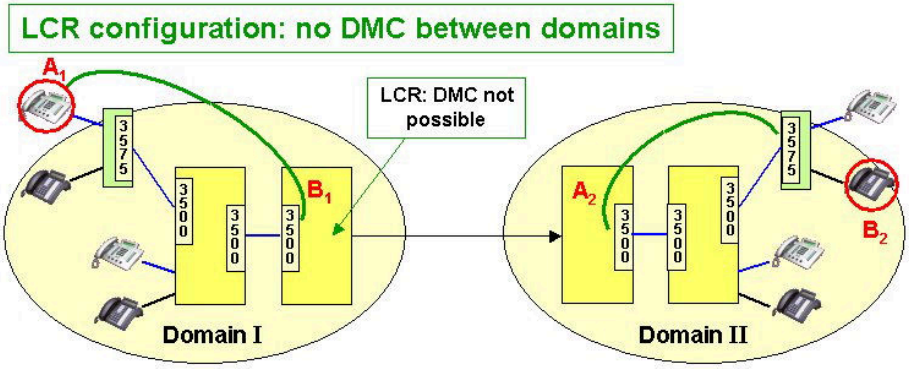
Hinweis: Für dieses Szenario ist keine spezielle Konfiguration erforderlich (Standard)



Beispiel 2: DMC nur innerhalb von Domäne A bzw. B möglich, nicht von Domäne A auf Domäne B

In diesem Fall müssen die Endpunkte der Verbindung zwischen den beiden Domänen als Domänengrenze gekennzeichnet werden.

Dies wird über ein entsprechendes Attribut im LCR bewerkstelligt (siehe Kapitel „Generierung“). Dieses Attribut muss in beiden Domänen für die LCR-Richtung zur jeweils anderen Domäne gesetzt werden.



19.2.1.6 DMC-Interworking mit HiPath 3000

Unterstützte Szenarien:

Szenario 1: Payload Switching von HiPath 3000 wird bei HG 3500 abgeschlossen

Bei diesem Szenario sind folgende zwei Anwendungsfälle abgedeckt:

1) beim Endpunkt im HiPath 4000-/OpenScape 4000-Netz handelt es sich um ein TDM-Gerät, oder

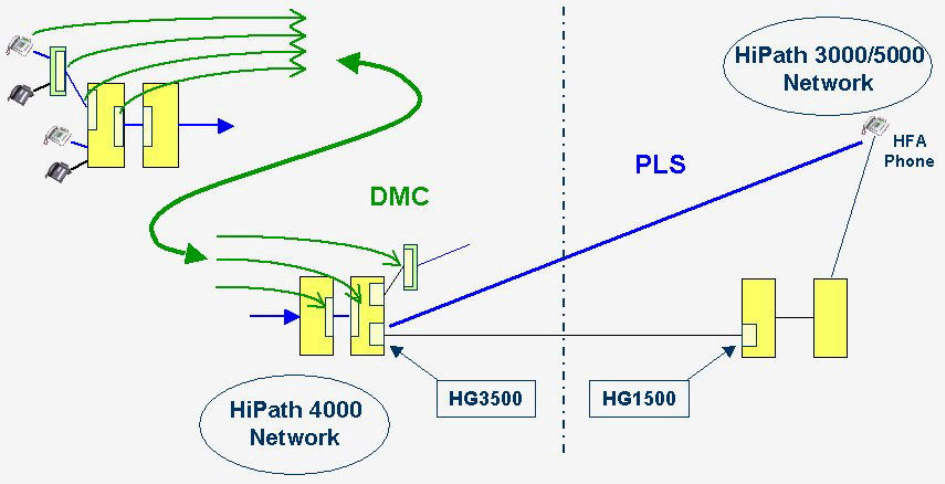
2) • DMC-Interworking zwischen OpenScape 4000 und HiPath 3000 ist nicht zugelassen (dieses Szenario lässt sich herbeiführen, indem man in der OpenScape 4000 für die Richtung zum HiPath 3000-Netz das LCR-Attribut Domänengrenze setzt).

Im ersten Fall setzt sich die Verbindung aus einer TDM-Verbindung auf der OpenScape 4000-Seite und einer IP-Verbindung zwischen dem HG 3500 und dem IP-Endpunkt auf der HiPath 3000-Seite zusammen.

Im zweiten Fall besteht die Verbindung zwischen den beiden Endpunkten im HiPath 4000-/OpenScape 4000 bzw. HiPath 3000-Netz aus folgenden Anteilen:

- einem DMC-Teil im HiPath 4000-/OpenScape 4000-Netz, und
- dem Payload Switching (PLS) im HiPath 3000-Netz, d.h. das Payload Switching wird bei der HG 3500 auf der OpenScape 4000-Seite abgeschlossen.

Dieser Fall ist im nachfolgenden Bild dargestellt.

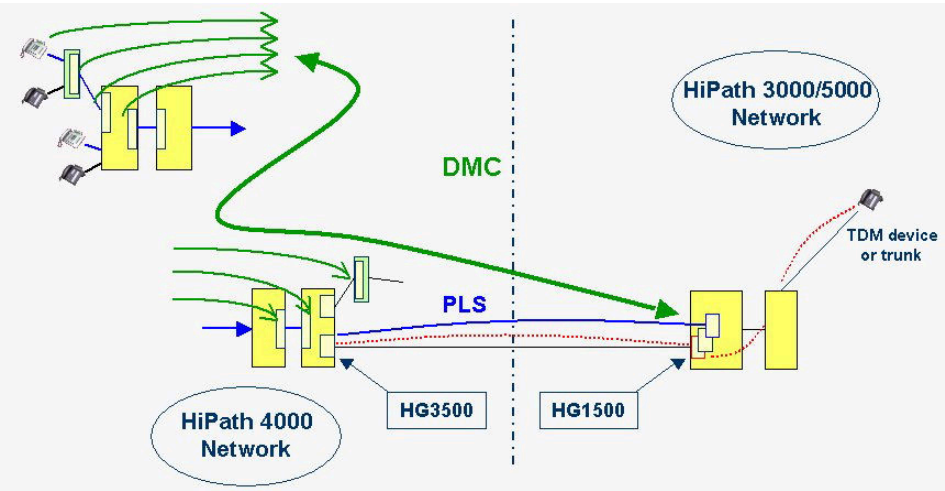


- DMC im HiPath 4000-/OpenScape 4000-Netz: Von der erstmöglichen IP-Adresse auf der A-Teilnehmerseite zur erstmöglichen IP-Adresse auf der B-Teilnehmerseite. Die Signalisierung der IP-Adressen von A und B erfolgt hierbei über CorNet-NQ (SETUP/CONNECT-Meldungen).
- PLS (Payload Switching) im HiPath 3000-Netz: Das IP-Gateway HG 3500 fungiert als Payload Switching HFA Proxy der HiPath 3000.

Szenario 2: Direct Media Connection von OpenScape 4000 wird bei HG 1500 abgeschlossen

DMC auf HG 1500 in HiPath 3000

Ist ein Interworking zwischen OpenScape 4000 und HiPath 3000 zugelassen und beim Endpunkt im HiPath 3000-Netz handelt es sich um ein TDM-Gerät, wird die DMC-Verbindung bei der HG 1500 abgeschlossen.

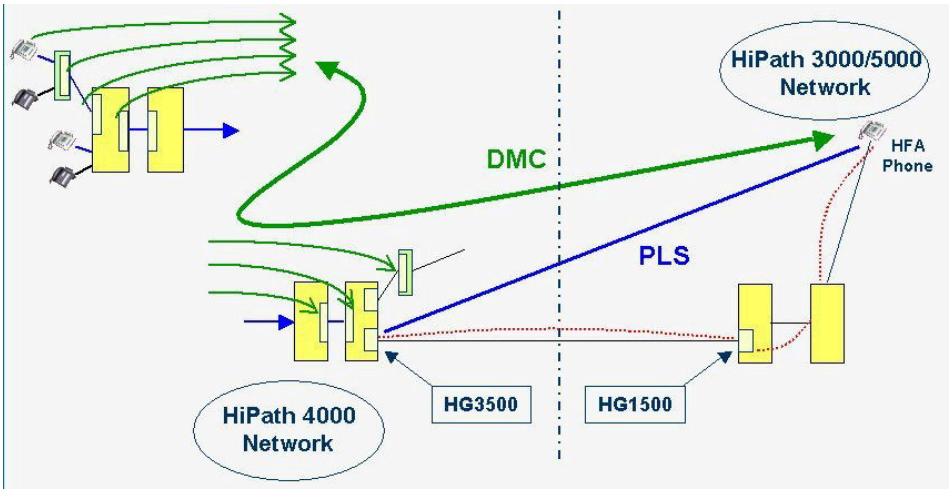


Der RTP-Strom zwischen der HG 1500 auf der HiPath 3000-Seite und der HG 3500 auf der OpenScape 4000-Seite gehört zur Master-Verbindung.

Szenario 3: Durchgängige Direct Media Connection zwischen HFA IP-Telefonen

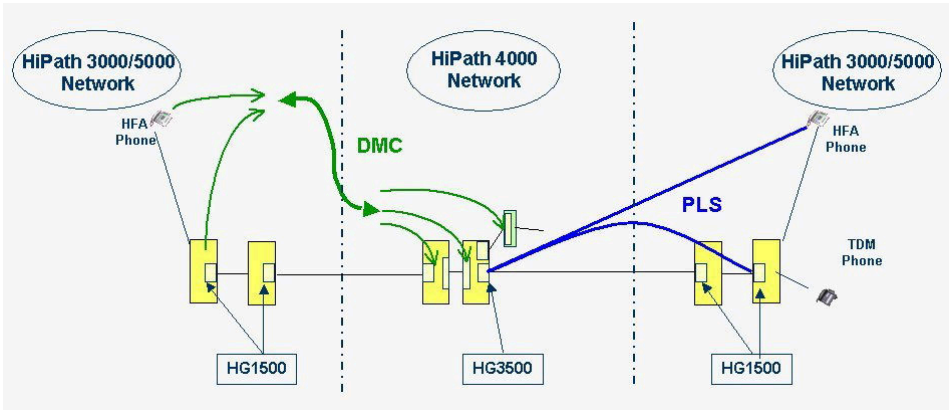
DMC auf HFA-Telefon in HiPath 3000

Ist ein Interworking zwischen OpenScape 4000 und HiPath 3000 zugelassen und beim Endpunkt im HiPath 3000-Netz handelt es sich um ein HFA-Telefon, kann eine durchgängige DMC-Verbindung hergestellt werden.



Der RTP-Strom zwischen dem HFA-Telefon auf der HiPath 3000-Seite und der HG 3500 gehört zur Master-Verbindung.

Szenario 4: OpenScape 4000 als Transitknoten zwischen zwei HiPath 3000-Knoten



In diesem Fall kann keine durchgehende DMC Verbindung zwischen den HiPath 3000 IP Geräten (IP phones oder HG1500) aufgebaut werden. Es bildet sich auf Seite des A Teilnehmers eine DMC bis zum weitesten entfernten OpenScape 4000 DMC Endpunkt (HG 3500 (FUNCTION=HG3550 oder HG3570) oder HG 3575). Diese DMC überspannt eine darunterliegende HiPath 3000 PLS Verbindung (nicht im Bild dargestellt) und die IP Anteile im HiPath 4000/OpenScape 4000 Netz.

Falls es keine IP Anteile im HiPath 4000/OpenScape 4000 Netz gibt, entfällt die DMC Verbindung , und die Payload wird auf der PLS Verbindung übertragen. Das trifft zu, wenn es sich nicht um ein HiPath 4000/OpenScape 4000 Netz oder eine IPDA Konfiguration handelt, sondern um eine einzelne OpenScape 4000, die auf beiden Seiten mit HiPath 3000 Anlagen oder Netzen verbunden ist. Eine DMC Verbindung auf der A Seite existiert also nur, wenn eine Optimierung notwendig ist.

Auf Seite des B Teilnehmers bildet sich eine Payload Switching Verbindung.

Es handelt sich also immer um eine Verbindung mit 2 IP hops.

19.2.2 Service Informationen

19.2.2.1 Leistungsmerkmale mit DMC

In der nachfolgenden Liste sind die Leistungsmerkmale aufgeführt, bei denen eine DMC-Verbindung hergestellt wird:

- Basic Call
- Basic Call mit internem Rerouting
- Basic Call mit Rerouting (NW)
- Rückfragegespräch (einschließlich Makeln und Ende der Rückfrage (Zurückholen des gehaltenen Teilnehmers))
- Übergabe im Gesprächszustand mit oder ohne Wegeoptimierung
- Übergabe im Rufzustand mit oder ohne Wegeoptimierung
- Sofortiger Wiederanruf
- Übergabe zum zentralen Vermittlungsplatz
- CFU (Call Forwarding Unconditional), CFNR (Call Forwarding No Reply) mit Forward Switching, Rerouting oder gemischt (Rerouting in Transitanlage)
- Rückruf (Message Waiting, Besetzt, Frei)
- Anrufübernahme im Team
- Gezielte Anrufübernahme
- Anruf auf Sammelanschluss
- Gesprächsaufbau aus einer Anwendung heraus (ACL Make Call)
- ACD-Anrufe
- Herabstufen einer Konferenz auf eine Zweierverbindung
- Anruf auf Keyset (Anruf wird an Zweitanschluss abgefragt)
- CHESE (Chef-/Sekretäreinrichung) (Anrufannahme durch Sekretärin)

19.2.2.2 Aktivierung von Leistungsmerkmalen bei aktiver DMC

Ist bei einer Zweierverbindung eine DMC aktiv und es wird ein Leistungsmerkmal aktiviert, so wird die DMC ausgelöst und das Gespräch über die Master-Verbindung abgewickelt.

Dies gilt für Leistungsmerkmale, die von einem der Gesprächsteilnehmer aktiviert werden, sowie für LMs, die von einem Dritten aktiviert werden (z.B. Anklopfen oder Aufschalten).

Ist die Ausführung des LMs beendet und das Gespräch wechselt wieder zu einer normalen Zweierverbindung, wird die DMC (außer für die oben aufgeführten LMs) nicht wieder aktiviert.

LM-Verhalten in Ausnahmesituationen:

- MFV-Handling
- Eine bestehende DMC wird ausgelöst, wenn ein Endpunkt die Aussendung von MFV-Signalen über die SIU (Signaling Unit) anstößt. Beispielsweise könnte ein HFA-Telefon die Aussendung von MFV-Signalen per Zugangscode anfordern.
- MVF-Übertragung über DMC
- MFV-Töne in DMCs werden erkannt und übertragen, etwa wenn der Ton von der OpenScape-4000-Anlage an der Amtsschnittstelle empfangen wird, oder wenn ein MFV-fähiger Anate-Teilnehmer selbst MVF-Signale sendet.

19.2.3 Generierung

19.2.3.1 DMC-Berechtigung

Die IP-Endpunkte müssen die Berechtigung zum Durchschalten von DMC bekommen. Dies wird mit Hilfe der folgenden AMO-Befehle bewerkstelligt:

- IP-Telefone:
- `AENDERN-SDAT:TLNNU=<Nebenstellen▶ nummer>,TYP=MERKMAL,EMERK=DMCERL;`
- NCUI:
- `AENDERN-STMIB:MTYP=NCUI2,LTU=xx,TYP=DMCDATA,DMCERL=JA;`
- STMI-Pool für IPDA:
- `AENDERN-SIPCO:TYP=DMCDATA,DMCERL=JA;`
- IP Trunking:
- `AENDERN-TDCSU:LAGE=<LTG-LTU-EBT- Satz),GER=HG3550IP,DMCERL=J;`

19.2.3.2 Maximale Anzahl von DMC-Verbindungen bei IP-Baugruppen

siehe „Gateways HG 3500 und HG 3575“, Abschnitt 2.6, „B-Kanäle“.

AMO-Befehle:

- NCUI:
- `AENDERN-STMIB:MTYP=NCUI2,LTU=xx,TYP=DMCDATA,DMCCONN=<Anzahl zugelassener DMC-Verbindungen>;`
- STMI - IP-Trunking:
- `AENDERN-CGWB:MTYP=CGW,LTU=xx,EBT=xx,TYP=DMCDATA,DMCCONN=<Anzahl zugelassener DMC-Verbindungen>;`

19.2.3.3 Sprachpausenerkennung (Voice Activity Detection, VAD)

Um Bandbreite zu sparen, sollte für IP-Verbindungen die Sprachpausenerkennung (VAD) aktiviert werden. Ist eine DMC-Verbindung aktiv, und die Sprachpausenerkennung ist eingestellt, so werden über die Master-Verbindung nur IDLE-Frames gesendet.

Die Sprachpausenerkennung wird mit Hilfe folgender AMO-Befehle aktiviert:

- Teilnehmer:
- `AENDERN-SDAT:TLNNU=<Nebenstellen▶ nummer>,TYP=DATEN1,CLASSMRK=VAD&EC&G711&G729OPT;`
- Digitale Leitungen:
- `AENDERN-TDCSU:LAGE=<LTG-LTU-EBT- Satz),CLASSMRK=VAD&EC&G711&G729OPT;`
- Analogleitungen:
- `AENDERN-TACSU:LAGE=<LTG-LTU-EBT-`

Satz),CLASSMRK=VAD&EC&G711&G729OPT;

- IP Trunking:
- Codecs und VAD können nicht mehr in der WBM geändert werden; jede Änderung muss über AMO CGWB vorgenommen werden. Allerdings ist es immer noch möglich, die aktuellen Einstellungen in der WBM unter **Explorers > Voice Gateway > Codec Parameter** (Explorer nnnn Sprachgateway nnnn Codec-Parameter) anzuzeigen.

  (Dasselbe gilt für HG 3575 IPDA - AMO STMIB)
- HFA: An beiden Enden der HFA-Master-Verbindung muss VAD einschalten werden.
- Für IP-Telefone: Die Sprechpausenunterdrückung muss in der WBM des Telefons unter **Administrator > Speech/Cloud > Codec Preferences** (Administrator nnnn Sprache/Cloud nnnn Codec-Voreinstellungen) aktiviert werden.

  Für HG3500:
  AENDERN-CGWB:MTYP=CGW,LTU=x,EBT=xx,TYP=ASC,VAD=JA;

19.2.3.4 Domänen

Bei sehr großen Unternehmensnetzen muss das Netzwerk unter Umständen in mehrere Areas (Domänen) aufgeteilt werden, wobei DMC jeweils nur innerhalb derselben Domäne und nicht domänenübergreifend möglich ist.

Hierfür muss an den Domänengrenzen ein entsprechendes LCR-Kennzeichen gesetzt werden. Ist ein solches Kennzeichen gesetzt, werden über den entsprechenden Punkt hinaus keine DMCs hergestellt.

AMO-Befehl:

AENDERN-LDAT:LRTG=<Richtungsnummer>,LATTR=<bestehende Attribute>&DMCENDE;

19.2.3.5 H.323 Stack bei IPDA-Baugruppen

Der H.323 Stack bei IPDA-Baugruppen ist mit Hilfe folgender AMO-Befehle zu konfigurieren:

- NCUI:
- AENDERN-STMIB:MTYP=NCUI2,TYP=H323,GWNAME=<String>;
- STMI:
- Diese Einstellungen können nicht über AMO durchgeführt werden. Bitte nutzen Sie das WBM der Baugruppe hierfür.

  Die korrekten Zahlenwerte entnehmen Sie bitte dem Konfigurationshandbuch für IPDA-Baugruppen.

  Weiterhin müssen die Codecs konfiguriert werden, die fuer die DMC benutzt werden (Master Connection Codecs siehe AMO SDAT / AMO TACSU / AMO TDCSU).
- NCUI:
- AE-STMIB:MTYP=NCUI2,LTU=xx,TYP=ASC,PRIO=PRIO1,CODEC=G729&G711;

```
AE-
STMIB:MTYP=NCUI2,LTU=xx,TYP=ASC,PRIO=PRIO2,CODEC=G711;
```

- STMI:
- ```
  AENDERN-
  CGWB:MTYP=CGW,LTU=xx,EBT=xx,TYP=ASC,PRIO=PRIO1,CODEC=G729;
  AENDERN-
  CGWB:MTYP=CGW,LTU=xx,EBT=xx,TYP=ASC,PRIO=PRIO2,CODEC=G711;
  ```

  WBM > Explorers > Voice Gateway > Codec Parameters (Administrator nnnn Sprache/Cloud nnnn Codec-Voreinstellungen)

19.2.3.6 Tipps zur Fehlerbeseitigung

Bei Problemen mit DMC-Verbindungen prüfen Sie bitte zunächst die in Abschnitt 2.3.1, „DMC-Berechtigung“ beschriebenen Aktivierungsschalter.

Ein weiterer zu prüfender Schalter ist der Diagnoseschalter 08 im CP2-Zweig von AMO DIAGS.

1) `DISPLAY-DIAGS:COMP=CP2;`

Denken Sie daran, dass der Schalter **S08 = ON** die DMC-Verbindungen systemweit deaktiviert. Deshalb sollte der Schalter in der Regel auf OFF gesetzt werden, um DMC zu aktivieren.

Sorgen Sie außerdem dafür, dass für die betroffenen Baugruppen genügend DMC-Ressourcen konfiguriert sind (siehe Abschnitt 2.3.2, „Maximale Anzahl von DMC-Verbindungen bei IP-Baugruppen“). Prüfen Sie auch, ob der Ressourcen-Manager konfiguriert/beteiligt ist.

Darüber hinaus können Sie überprüfen, ob die Komponenten zu verschiedenen Domänen gehören und DMC-Verbindungen zwischen Domänen zulässig sind.

Die Tabelle der unterstützten Leistungsmerkmale sollte ebenfalls überprüft werden (siehe Abschnitt 2.2, „Service Informationen“).

Die DMC-Verbindungen können durch Aktivieren des DIAGS-Schalters 09 in CP2 geprüft werden. Hierbei werden die Informationen zu DMC-Verbindungen im folgenden HISTA-Abschnitt angezeigt:

```
F4066 M8 N4058 NO ACT   BPA   CP       ADVISORY

      ALARM CLASS:CENTRAL:023

      FORMAT:49

      DMC
```

Der folgende Ablauf gewährleistet erfolgreiche DMC-Verbindungen:

Teilnehmer B:	STATE_NEW	=	init;	event = ACT_PROXY_DMC_START
Teilnehmer A:	STATE_NEW	=	active;	event = UP DMC_IND OK
```

Teilnehmer B:	STATE_NEW	=	active;	event = UP DMC_CONF

Hinsichtlich einiger DMC-bezogener Anrufe können auch die Explorer-Statistiken in der WBM der IPDA/Gateway-Baugruppen geprüft werden.

Hierbei kann die Anzeige von AMO ZAUSL nützlich sein. Im Ergebnis werden Zähler der DMC-Verbindungen angezeigt:

```
|N0059: NUM. OF ALL SUCCESS. DMC ATTEMPTS (ACT. OR
 PAS)..         0|
|N0060: NUM. OF ALL UNSUCCES.  DMC ATTEMPTS(ACT. OR
 PAS).          0|
|N0061: NUM. OF SUCCESSFUL DMC ATTEMPTS, BOTH PROX.
 INTR.          0|
|N0062: NUM. OF UNSUCCESSFUL DMC, BOTH PROXIES
 INTERNAL..         0|
|N0063: NUM. OF ALL UNSUCCES.  DMC ATTEMPTS(INSTANT
 DMC).          0|
```

Bei G711 werden die CN RTP-Pakete in Wireshark als „Payload Type: Comfort Noise“ angezeigt.

Bei G729 werden Sie als „Payload Type: ITU-T G729“ angezeigt (wie beim normalen RTP), wobei jedoch die Länge der Nutzlast in der Regel nur 2 Byte und die Gesamtpaketlänge 60 Byte beträgt.

Bei G723.1 wird CN in „field: frame size“ und „codec type: SID frame“ erkannt.

19.2.4 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	MTYP=CGW	d	Konfiguration von HG 3500
	MTYPE=CGW	e	Configuration of HG 3500
	TYP=DMCDATA	d	DMC-spezifische Daten konfigurieren
	TYPE=DMCDATA	e	Configure DMC specific data
	DMCCONN	d	Anzahl der DMC-Verbindungen
	DMCCONN	e	Number of DMC connections
	TYP=ASC,VAD=J/N	d	VAD in Senderichtung erlaubt / nicht erlaubt,Wert=JA / NEIN
	TYPE=ASC,VAD=Y/N	e	VAD enabled / not enabled in send direction, value = YES / NO
LDAT	LATTR	d	LCR Attribut, neuer Wert: DMCENDE = Ende der DMC Domaine

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	LATTR	e	LCR attribute, new value: DMCEND = end of DMC domain
SDAT	EMERK & AMERK	d	Teilnehmermerkmal, Wert: DMCERL = DMC erlaubt
	AATTR & DATTR	e	subscriber attribute, value: DMCALLWD = DMC allowed
	CLASSMRK	d	Classmark, Wert VAD = Voice Activity Detection
	CLASSMRK	e	Classmark, value VAD = Voice Activity Detection
SIPCO	TYP	d	Datentyp (Verzweigungsparameter), Wert: DMCDATA
	TYPE	e	type of data (branching parameter), value: DMCDATA
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO
STMIB	MTYP=NCUI2	d	Konfiguration der HG 3575
	MTYPE=NCUI2	e	Configuration of HG 3575
	TYP=DMCDATA	d	DMC-spezifische Daten konfigurieren
	TYPE=DMCDATA	e	Configure DMC specific data
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO
	DMCCONN	d	Anzahl der DMC-Verbindungen
	DMCCONN	e	Number of DMC connections
TDCSU	GER=HG3550IP	d	Integriertes IP-Gateway HG 3500
	DEV=HG3550IP	e	Integrated IP Gateway HG 3500
	DMCERL	d	DMC erlaubt, Wert = JA/NEIN
	DMCALLWD	e	DMC allowed, value = YES/NO
	CLASSMRK	d	Classmarks für IP Verbindungen, Wert VAD = Voice Activity Detection

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	CLASSMRK	e	classmarks for IP connections, value VAD = Voice Activity Detection
TACSU	CLASSMRK	d	Classmarks für IP Verbindungen, Wert VAD = Voice Activity Detection
	CLASSMRK	e	classmarks for IP connections, value VAD = Voice Activity Detection

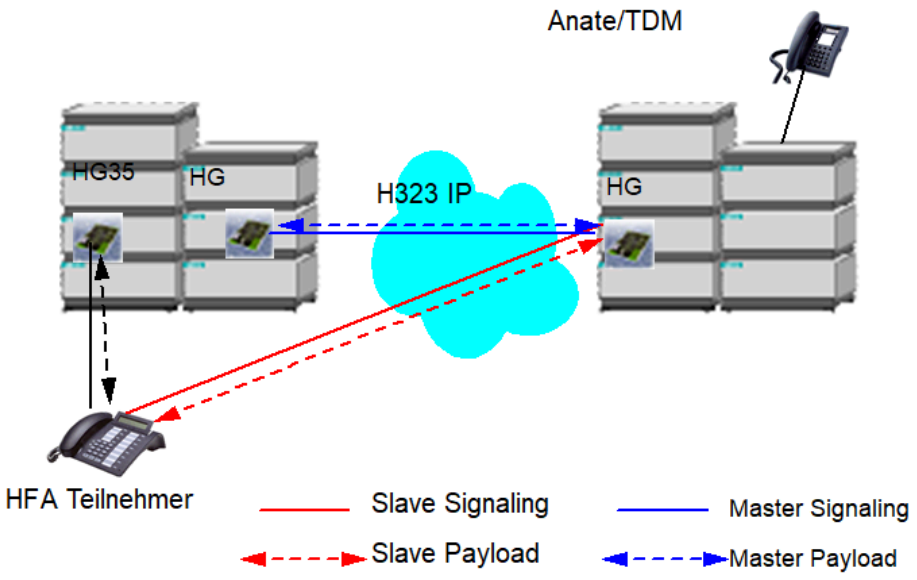
19.3 Direct Media Connect (DMC) in Verbindung mit SIP-Teilnehmern

19.3.1 Leistungsmerkmalbeschreibung

Eine wichtige Funktionalität auf der LAN-Seite ist „direkte Payload“ (DMC -> Direct Media Connect) zwischen den Gesprächsteilnehmern. Für alle SIP-Endpunkte kann diese Funktion aktiviert / deaktiviert werden.

Da SIP Endgeräte das H.323-basierte DMC-Verfahren nicht beherrschen, es aber trotzdem wünschenswert ist, zu anderen IP-Endgeräten und Gateways direkte Nutzdatenübertragung zu fahren (wegen der besseren Sprachqualität), beinhaltet die HG 3500 einen sogenannten „DMC-Proxy“. Dieses Leistungsmerkmal gibt es natürlich auch für die Common Gateway Baugruppe. Das heißt, das Gateway agiert, was DMC-Signalisierung betrifft, stellvertretend für das SIP-Endgerät und setzt die DMC-Signalisierung in SIP-Signalisierung um.

Für HFA-Teilnehmer wird die DMC-Verbindung in folgendem Diagram veranschaulicht:



DMC in Verbindung mit HFA-Teilnehmern

Das Diagram zeigt die Situation, dass ein HFA-Teilnehmer einen TDM-Teilnehmer in einem anderen Knoten über eine H323 IP-Verbindung ruft. Die Master-Verbindung für Signalisierung und Sprache wird über die HG 3500 (hier als HFA-Gateway eingerichtet) und die beiden HG 3500 (IP-Trunking-Gateways) aufrechterhalten. Die Slave-Verbindungen sind die DMC-Verbindungen vom ersten IP-Punkt (HFA-Teilnehmer) bis zum letzten IP-Punkt (HG 3500 IP-Trunking-Baugruppe) dieser Verbindung.

Als Teil der DMC-Signalisierung werden die Transportadressen (IP-Adressen/ Ports) für die Nutzdatenübertragung übermittelt. Der DMC-Proxy übermittelt hier nicht die eigene Transportadresse sondern die des angesprochenen SIP-Endgerätes um einen direkten RTP Strom zu dem SIP-Endgerät zu ermöglichen.

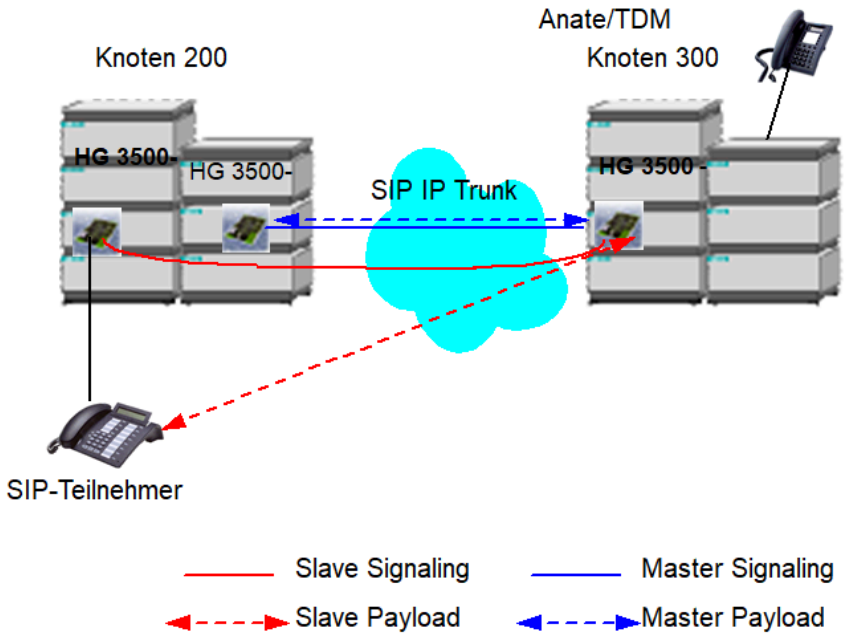
Da H.323 und SIP jeweils RTP für die Sprachübertragung verwenden, ist die Nutzdatenübertragung zwischen

- H323-Geräten,
- SIP- und HFA-Endgeräten,
- IPDA: Host System und IPDA Access Point,
- Common Gateways (IP-/SIP-Trunking) und HG 1500 Gateways

möglich.

Um zum SIP-Endgerät standard-konform einen direkten Nutzdatenkanal aufzubauen werden das SIP re-invite, und sofern es die Endgeräte unterstützen vorzugsweise auch das SIP-Update Verfahren verwendet (letzteres bedingt auch SIP-PRACK Unterstützung). Diese Verfahren ermöglichen das Umschalten einer Nutzdatenverbindung zu einem anderen Ziel. Im Unterschied zu bisherigen DMC-Endpunkten wird dabei nicht die „Master“-Nutzdatenverbindung zur OpenScape 4000 aufrechterhalten – d.h. die DMC-Nutzdatenverbindung ersetzt die Masterverbindung. Die „Master“-Signalisierung zur OpenScape 4000 wird aber sehr wohl aufrechterhalten.

Folgendes Diagramm dient zur Veranschaulichung:



HG 3500 als DMC Proxy

Erklärung:

Bild 26 „DMC in Verbindung mit HFA-Teilnehmern“: DMC-Signalisierung und Nutzdaten zwischen einem HFA-Telefon und einem HG 3500 Trunking-Gateway (siehe auch Kapitel 2, „Direct Media Connect (DMC) in Verbindung mit HFA-Teilnehmer“).

Bild 27 „HG 3500 als DMC Proxy“: DMC-Nutzdaten zwischen SIP-Telefon im Knoten 200 und einer HG 3500-Trunking im Knoten 300. DMC-Signalisierung ist aber zwischen DMC-Proxy im HG 3500 und HG 3500-SIP-Trunking.

Man unterscheidet den DMC-Proxy von dem DMC-Endpunkt. Letzterer ist Endpunkt für die DMC-Signalisierung und den DMC-Nutzdatenkanal (RTP). Man versteht sowohl Gateways (HG 3500, HG 3575) als auch Endgeräte als DMC-Endpunkte. Im Diagram sind also HG 3500-Trk im Knoten 300 und das SIP-Telefon im Knoten 200 DMC-Endpunkte.

Man bemerke, dass die HG 3500 in diesem Beispiel an keiner Nutzdatenverbindung beteiligt ist. Es wird allerdings trotzdem ein DSP für die Verbindung vorgehalten für den Fall, dass eine Leistungsmerkmalaktivierung die DMC beendet und einen Rückfall auf die Master-Verbindung bewirkt. Bei Beendigung der DMC, muss erneut per SIP-re-invite eine Master Nutzdatenverbindung ausgehandelt werden, da diese zum SIP-Endgerät nicht existiert.

Da die SIP-Endgeräte nicht selber DMC-fähig sind, spricht man ab HiPath 4000 V3.0 nicht mehr von DMC-Verbindungen sondern allgemeiner von Ende-zu-Ende Nutzdatenverbindungen (englisch: end-to-end payload connection, auch abgekürzt: e2epc).

Nicht dargestellt ist der Aufbau der Master-Verbindung, der zunächst zu einer Master Nutzdatenverbindung zwischen rufendem SIP-Endpunkt und HG 3500 führt (gefordert um Ansagen und Töne der OpenScape 4000 dem SIP-Endpunkt zu übermitteln). DMC wird mit der Rufannahme (Connect) der gerufenen Seite initiiert.

Es wird selbst bei einem Ruf zwischen zwei SIP-Endgeräten das oben beschriebene Verfahren verwendet, d.h. eine H.323-basierte DMC wird von HG 3500 zu HG 3500 (bzw. intern, falls beide Endgeräte an dem selben Gateway registriert sind) aufgebaut. Eine direkte Verbindung zwischen OpenScape 4000 SIP-Endgeräten ohne DMC ist zur Zeit nicht möglich.

19.3.2 Einschränkung

Wichtig: Bei Anschaltung eines Faxadapters an eine HG 3500 (SIP-Subscriber) muss DMC für dieses Device abgeschaltet werden (nur so kann eine Übertragung mit T.38 stattfinden). Möchte man DMC für dieses Gerät dennoch anschalten, muss der Codec fix auf G.711 eingestellt werden (Faxübertragung mit G.711, nicht T.38).

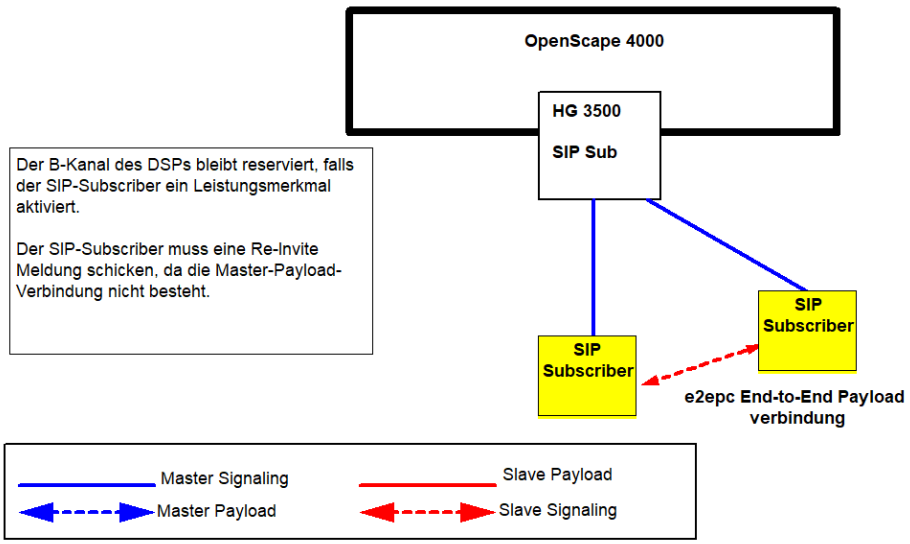
19.3.3 Szenarien

Die Diagramme in den folgenden Abschnitten sollen die möglichen Szenarien darstellen, bei denen ein SIP-Endgerät an e2epc beteiligt ist, beispielsweise

DMCen zu HFA- und SIP-Teilnehmer im eigenen (oder auch in anderen) Knoten, und DMCen zu IPDA und IP-Trunking Baugruppen - letztere als DMC-Endpunkte agierend.

19.3.3.1 SIP-Teilnehmer an gleicher OpenScape 4000

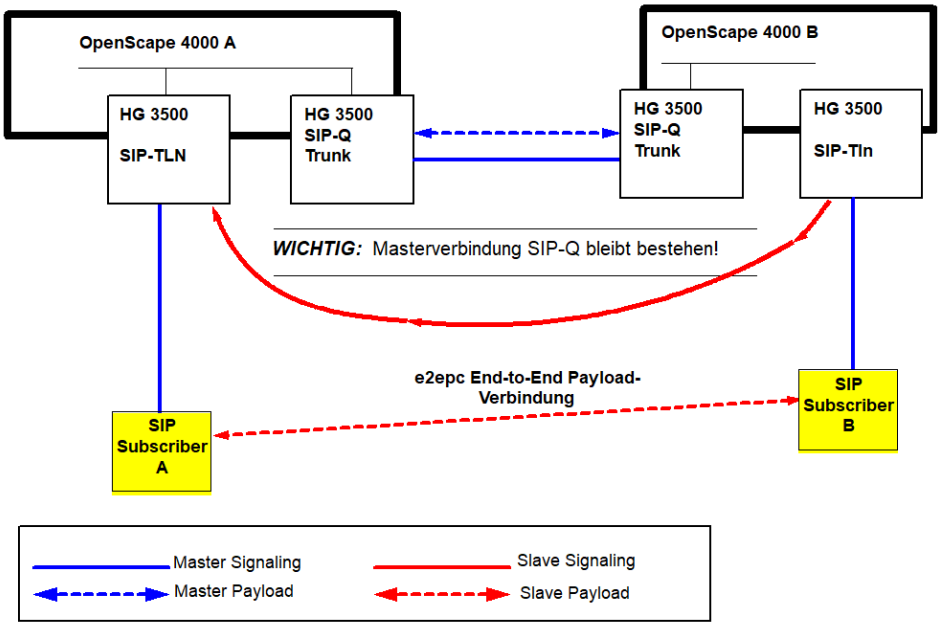
DMC-Signalisierung zwischen den HG 3500 (bzw. intern, falls beide am selben Gateway), e2epc zwischen den Teilnehmern, welche die Master Nutzdatenverbindung zum Gateway ersetzt.



19.3.3.2 SIP-Teilnehmer an einer anderen OpenScape 4000

Slave-Signalisierung an HG 3500 SIP-Teilnehmerbaugruppe, Slave-Payload zum SIP-Subscriber.

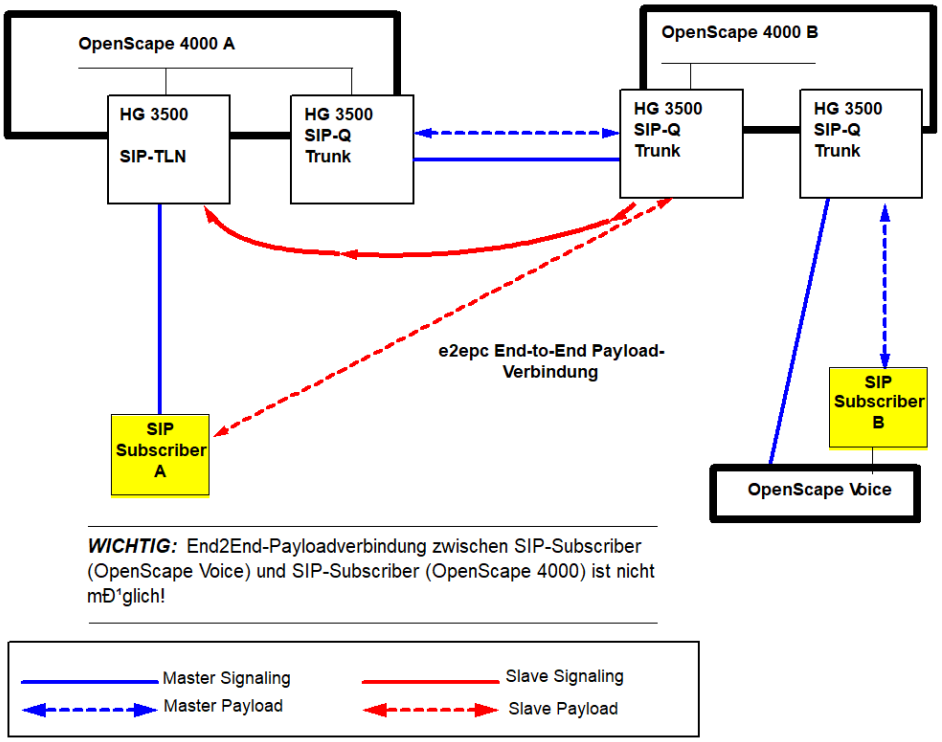
SIP-Subscriber A baut eine Verbindung zu OpenScape 4000 A auf. OpenScape 4000 A routet den Anruf über eine Trunking-Verbindung auf OpenScape 4000 B. OpenScape 4000 B baut anschließend eine Verbindung zum SIP-Subscriber B auf. OpenScape 4000 B baut eine DMC zwischen dem SIP-Subscriber B und dem SIP-Subscriber A auf, was eine End-to-End Payload-Verbindung zur Folge hat.



19.3.3.3 SIP-Teilnehmer an einer OpenScape Voice

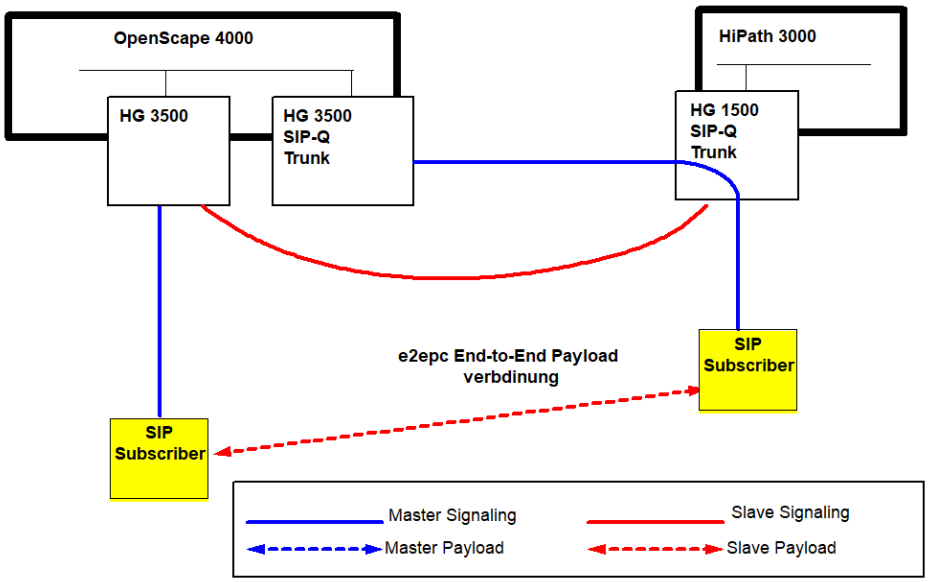
Slave-Signalisierung an HG 3500 SIP-Teilnehmerbaugruppe, Slave-Payload zum SIP-Subscriber.

SIP-Subscriber A baut eine Verbindung zu OpenScape 4000 A auf. OpenScape 4000 A routet den Anruf über eine Trunking-Verbindung auf OpenScape 4000 B. OpenScape 4000 B routet nun den Anruf über eine weitere Trunking-Verbindung zur OpenScape Voice. OpenScape Voice baut dann eine Verbindung zum SIP-Subscriber B auf. OpenScape 4000 B baut eine DMC zwischen dem SIP-Trunking Gateway B und dem SIP-Subscriber A auf, was eine End-to-End Payload-Verbindung zur Folge hat.



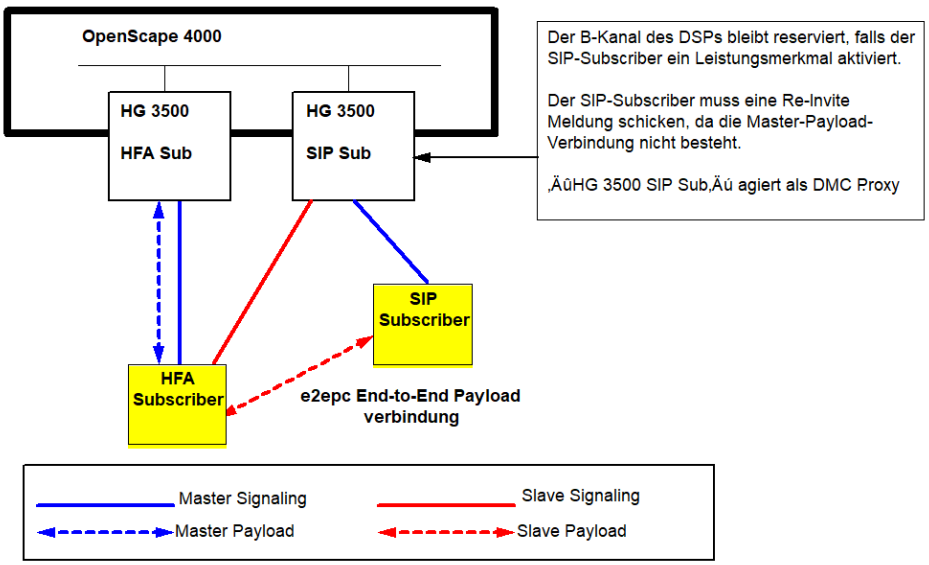
19.3.3.4 SIP-Teilnehmer an HiPath 3000

DMC-Signalisierung zwischen HG 3500 (SIP-Subscriber) und HG 1500 (initiiert durch OpenScape 4000), e2epc zwischen den SIP-Subscribern.



19.3.3.5 HFA-Teilnehmer an gleicher OpenScape 4000

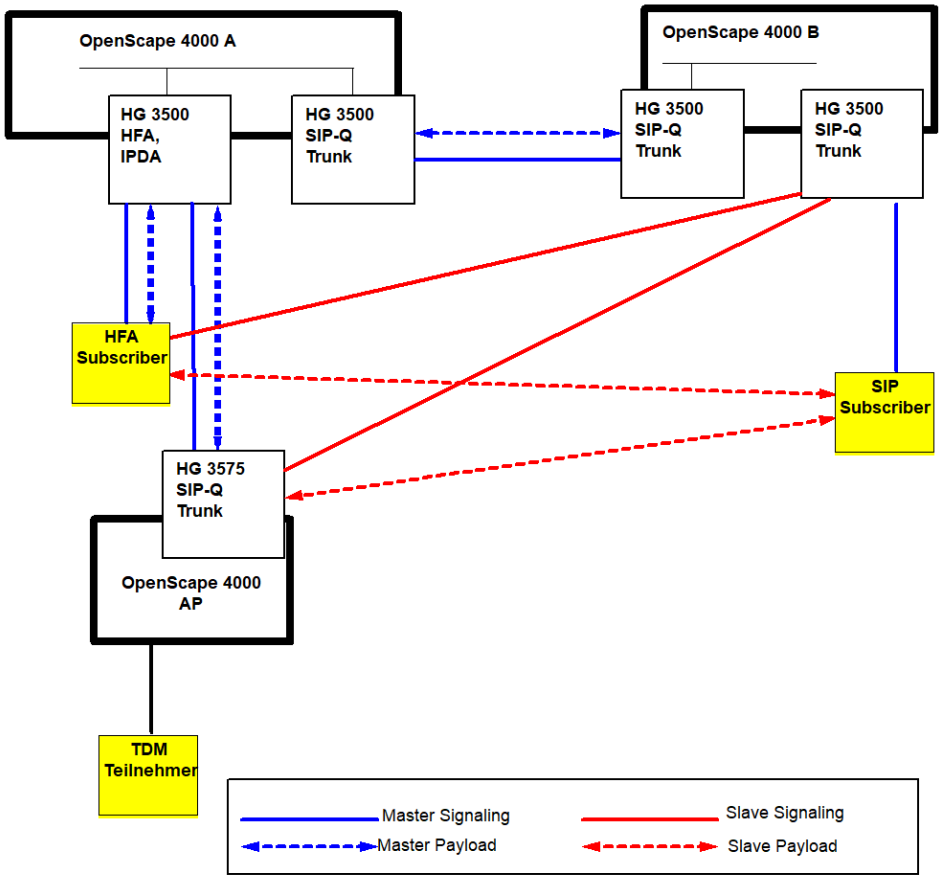
DMC-Signalisierung zwischen HG 3500 und HFA-Subscriber, e2epc zwischen den Teilnehmern. Zur HG 3500 (HFA-Subscriber) bleibt eine Master Nutzdaten-verbindung bestehen.



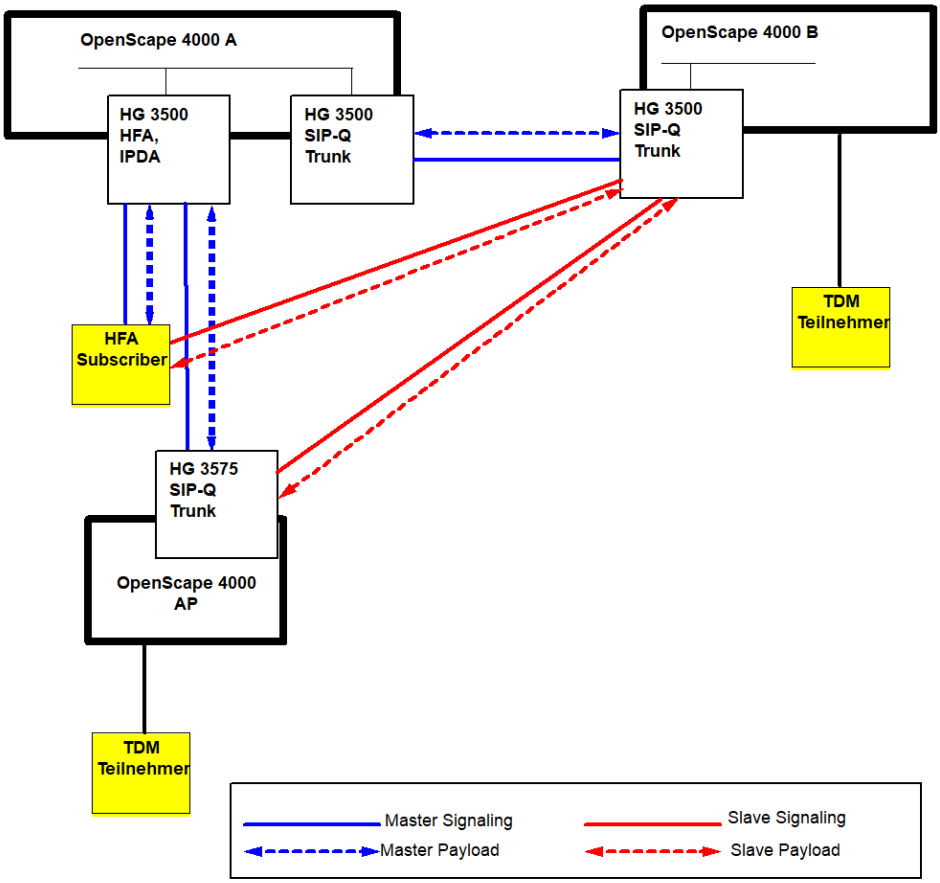
19.3.3.6 HFA-Teilnehmer an einer anderen OpenScape 4000

Beispiel 1: End-to-End Payload zwischen HFA- und SIP-Subscriber (oder HG 3575- und SIP-Subscriber)

Bei den HG 3500 Trunking-Baugruppen sind keine speziellen Maßnahmen erforderlich. OpenScape 4000 B baut eine DMC zwischen einem SIP- und einem HFA-Subscriber auf, was eine End-to-End Payload-Verbindung zur Folge hat.

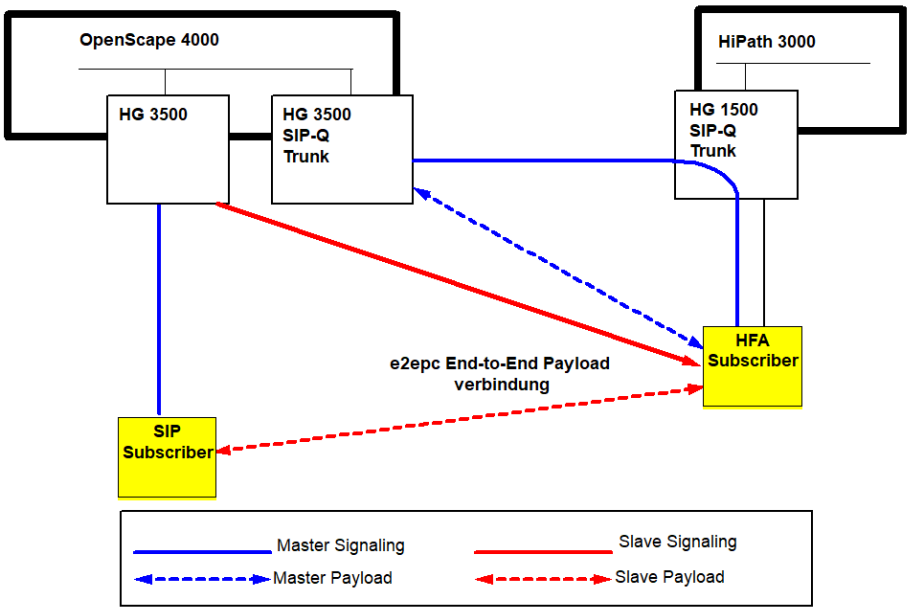


Beispiel 2: End-to-End Payload zwischen HFA- und SIP-Leitung (oder HG 3575- und SIP-Leitung)



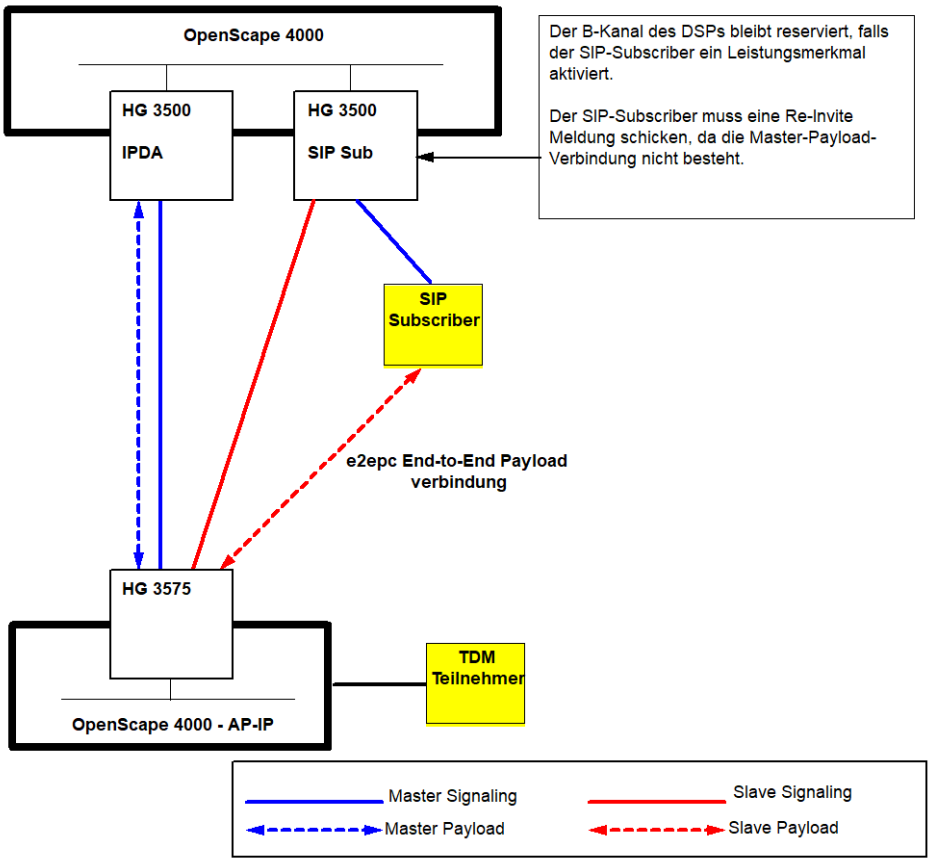
19.3.3.7 HFA-Teilnehmer an HiPath 3000

Master-Signalisierung über HG 1500, Master-Payload zwischen HFA-Subscriber und benachbarter HG 3500, Slave-Signalisierung und Payload zwischen HFA-Subscriber und Ursprungs-HG 3500.



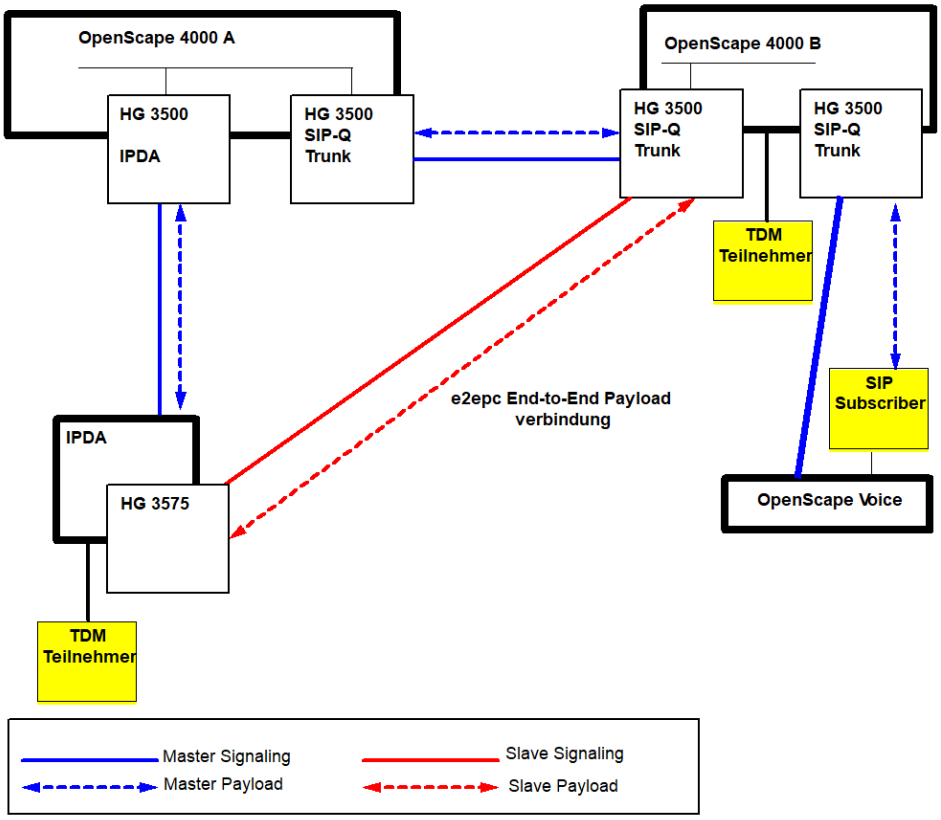
19.3.3.8 TDM-Teilnehmer/Netzwerk an einem abgesetzten Shelf einer OpenScape 4000

DMC-Signalisierung zwischen HG 3500 und HG 3575, e2epc zwischen SIP-Subscriber und HG 3575.



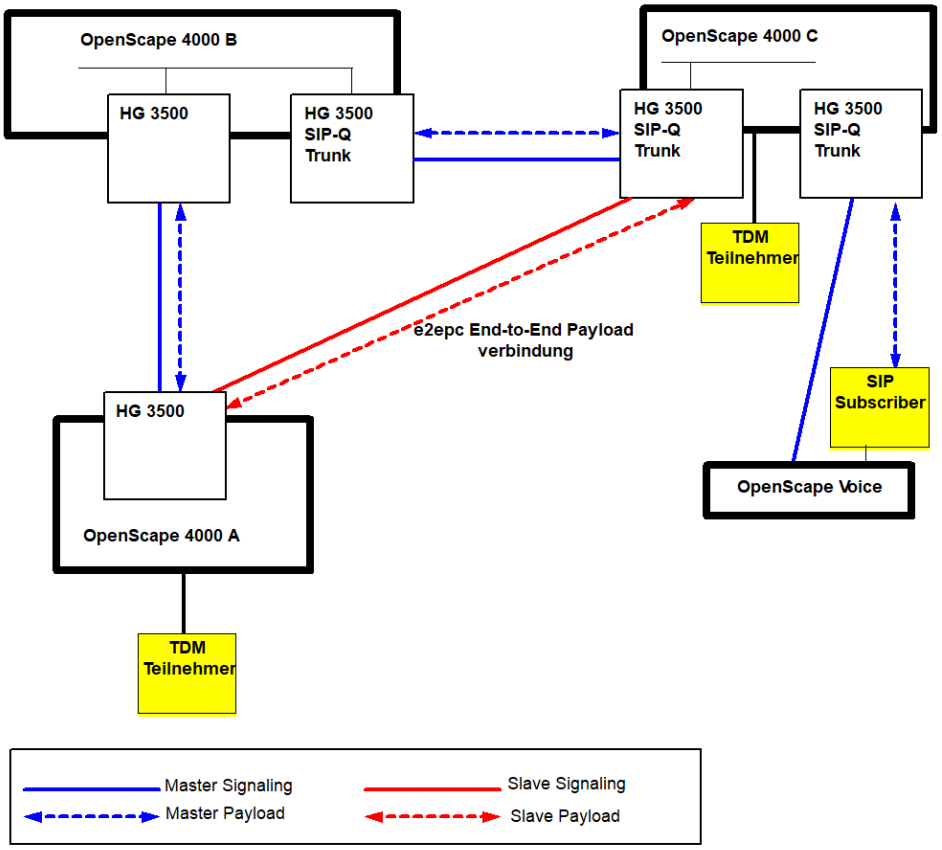
19.3.3.9 TDM-Teilnehmer/Netzwerk an einer anderen OpenScape 4000 hinter einem abgesetzten Shelf

Slavesignalisierung und Payload zu HG 3575.



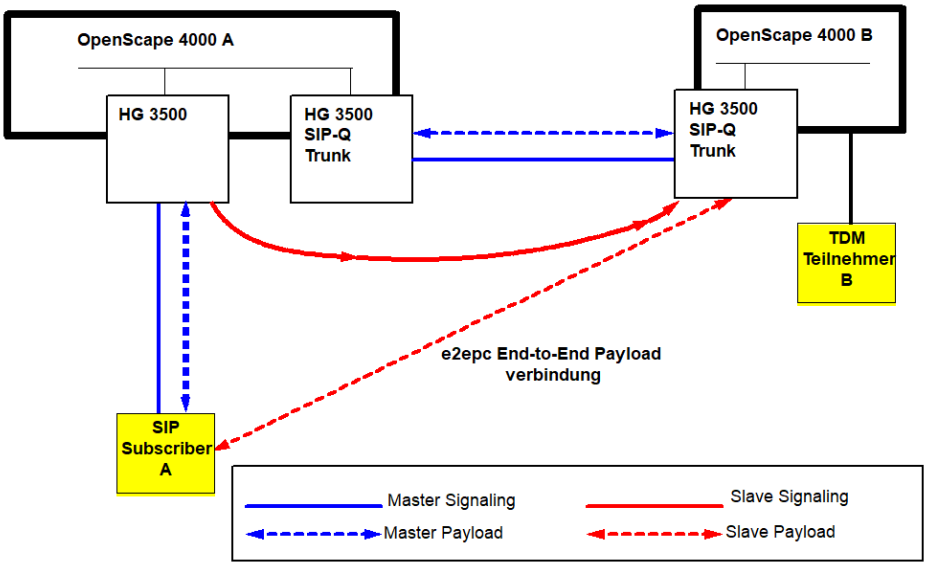
19.3.3.10 TDM-Teilnehmer an einer anderen OpenScape 4000

Beispiel 1: Slave-Signalisierung und Payload zu HG 3500



Beispiel 2: DMC Signalisierung zwischen HG 3500 (SIP-Subscriber) und HG 3500 (Trunk), e2epc zwischen SIP-Subscriber und HG 3500.

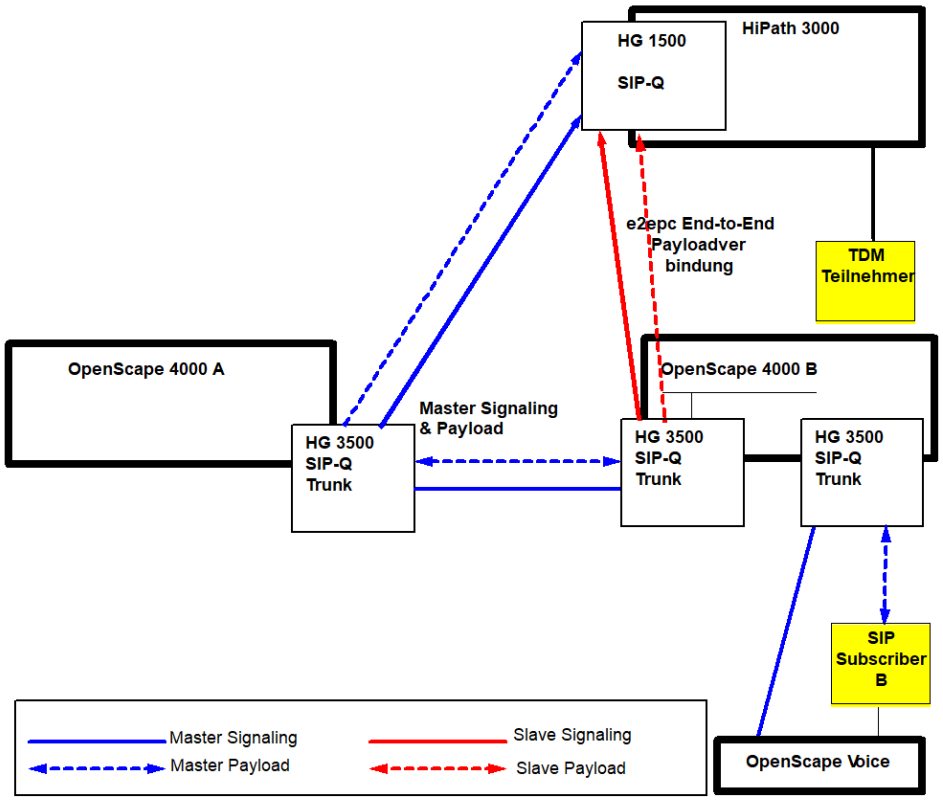
SIP-Subscriber A baut eine Verbindung zu OpenScape 4000 A auf. OpenScape 4000 A routet den Anruf über eine Trunking-Verbindung auf OpenScape 4000 B. OpenScape 4000 B baut anschließend eine Verbindung zum TDM-Teilnehmer B auf. OpenScape 4000 B baut eine DMC zwischen HG 3500 in OpenScape 4000 B und der HG 3500 (SIP-Subscriber/DMC-Proxy) in OpenScape 4000 A auf. OpenScape 4000 A stellt sicher, dass zwischen SIP-Subscriber A und der HG 3500 in OpenScape 4000 B eine End-to-End Payloadverbindung (e2epc) aufgebaut wird.



19.3.3.11 TDM-Teilnehmer an HiPath 3000

Master-Signalisierung und -Payload zwischen HG 1500 und benachbarter HG 3500, Slave-Signalisierung und -Payload zwischen HG 1500 und Ursprungs-HG 3500.

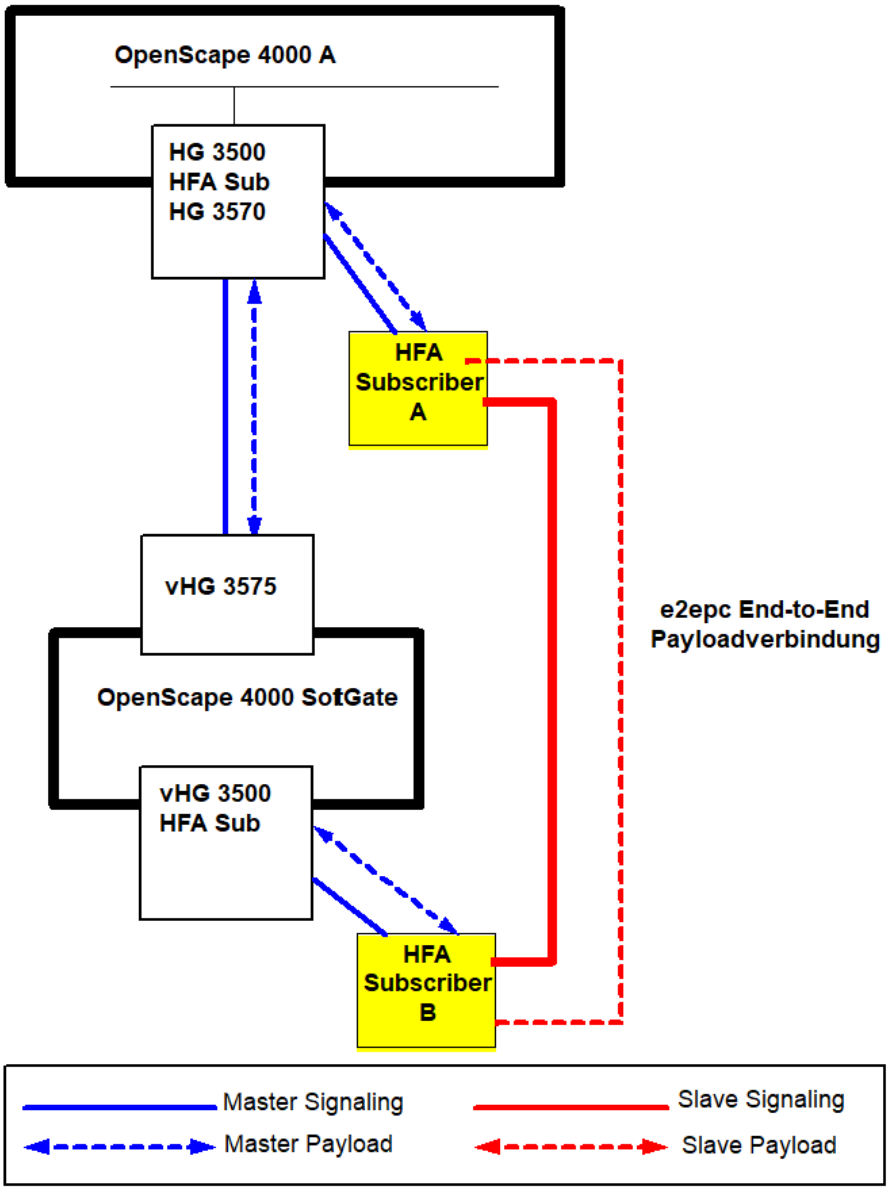
TDM-Teilnehmer an HiPath 3000 baut eine Verbindung zu OpenScape 4000 A auf. OpenScape 4000 A routet den Anruf über eine Trunking-Verbindung zu OpenScape 4000 B. OpenScape 4000 B routet nun den Anruf über eine weitere Trunking-Verbindung zur OpenScape Voice. OpenScape Voice baut dann eine Verbindung zum SIP-Subscriber B auf. OpenScape 4000 B baut eine DMC zwischen HG 3500 in OpenScape 4000 B und der HG 1500 in HiPath 3000 auf.



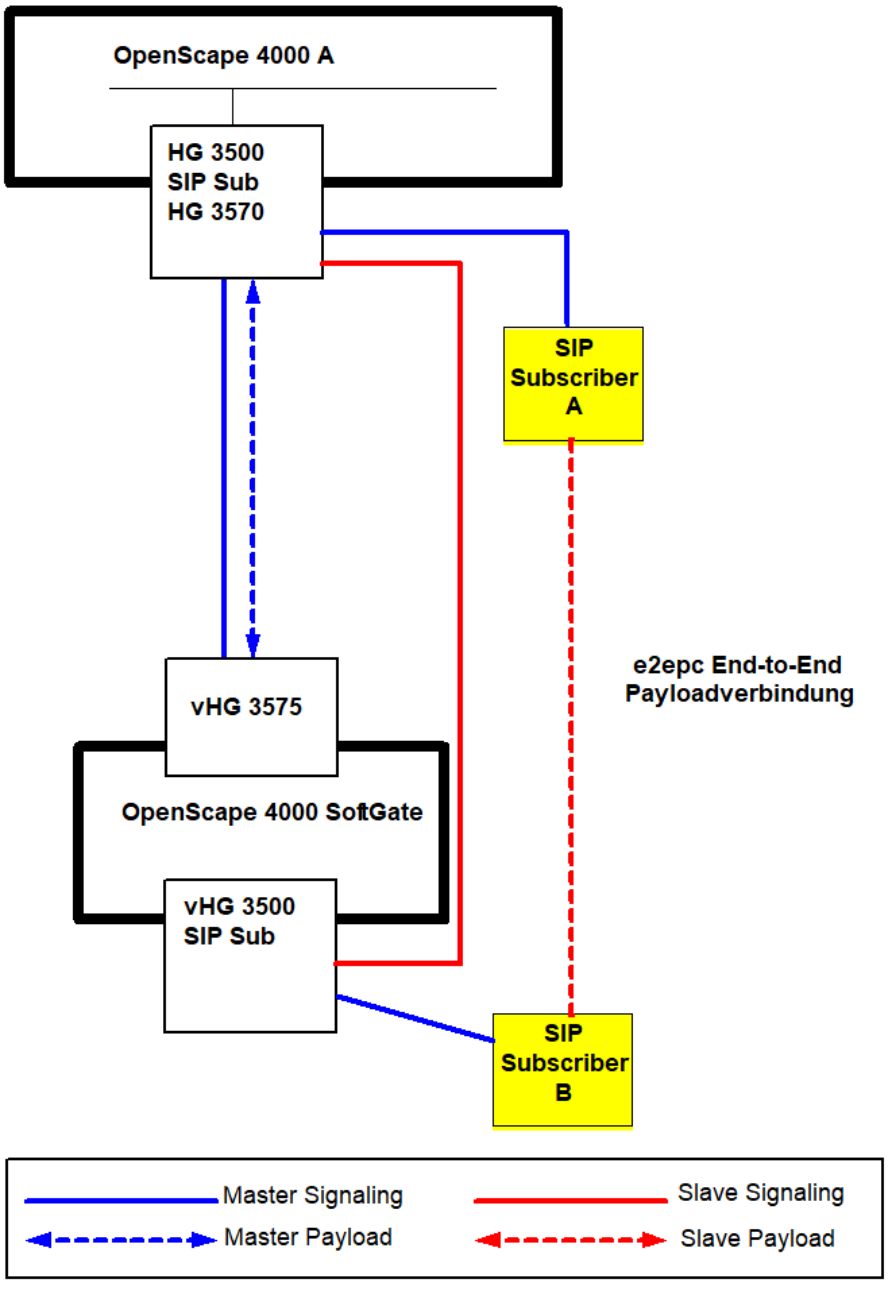
19.4 Direct Media Connect (DMC) in Verbindung mit OpenScape 4000 SoftGate

Wichtig: Für SIP-Subscriber: Ist DMC nicht aktiv, wird die Payload zwischen dem SIP-Subscriber und seiner HG 3500 (bzw. vHG 3500) ausgestauscht. Ist DMC aktiv, findet der Austausch der Payload **ausschließlich** über den end-to-end Payload-Pfad statt.

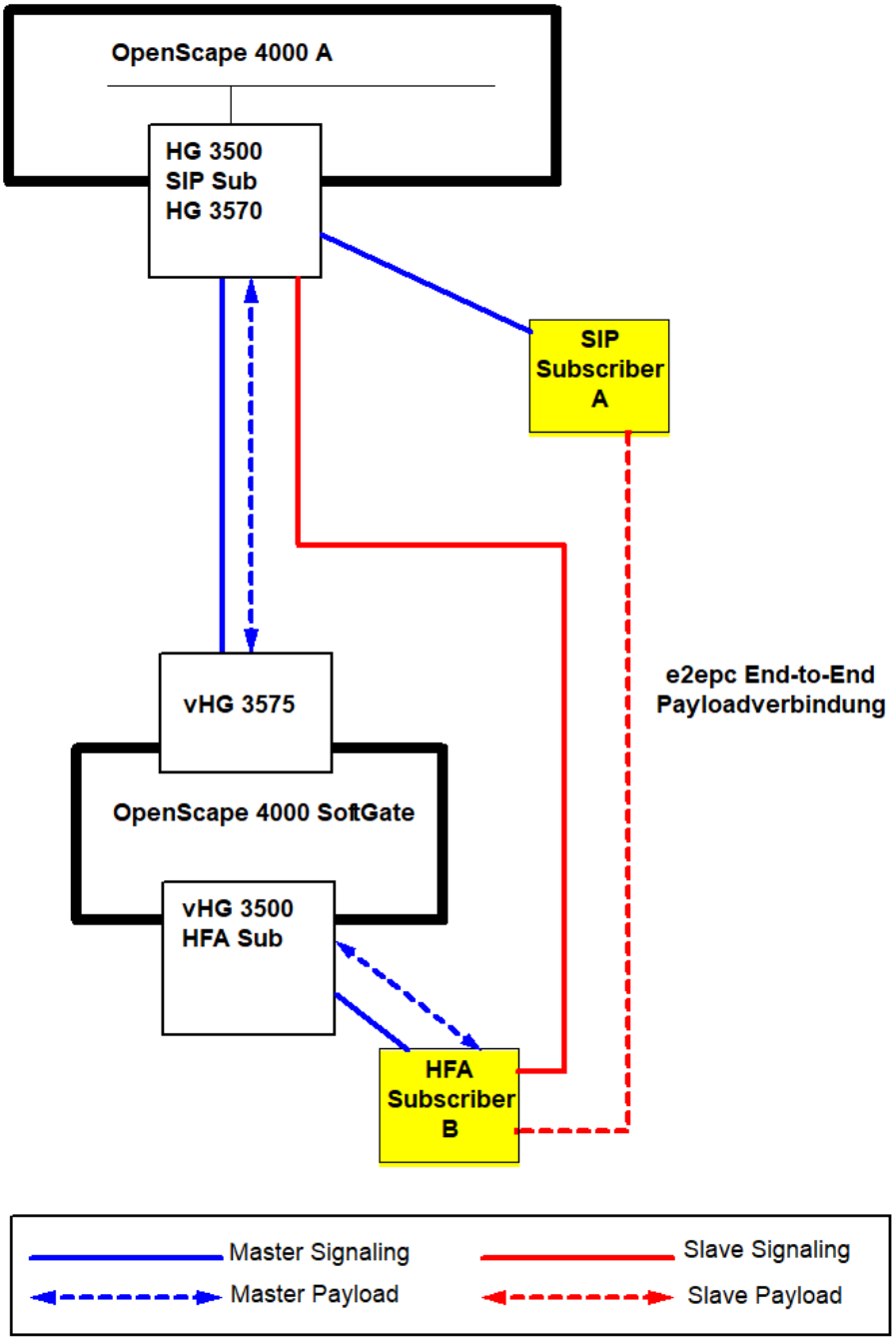
Beispiel 1: HFA-Subscriber A an OpenScape 4000 A ruft HFA-Subscriber B am OpenScape 4000 SoftGate



Beispiel 2: SIP-Subscriber A an OpenScape 4000 A ruft SIP-Subscriber B am OpenScape 4000 SoftGate

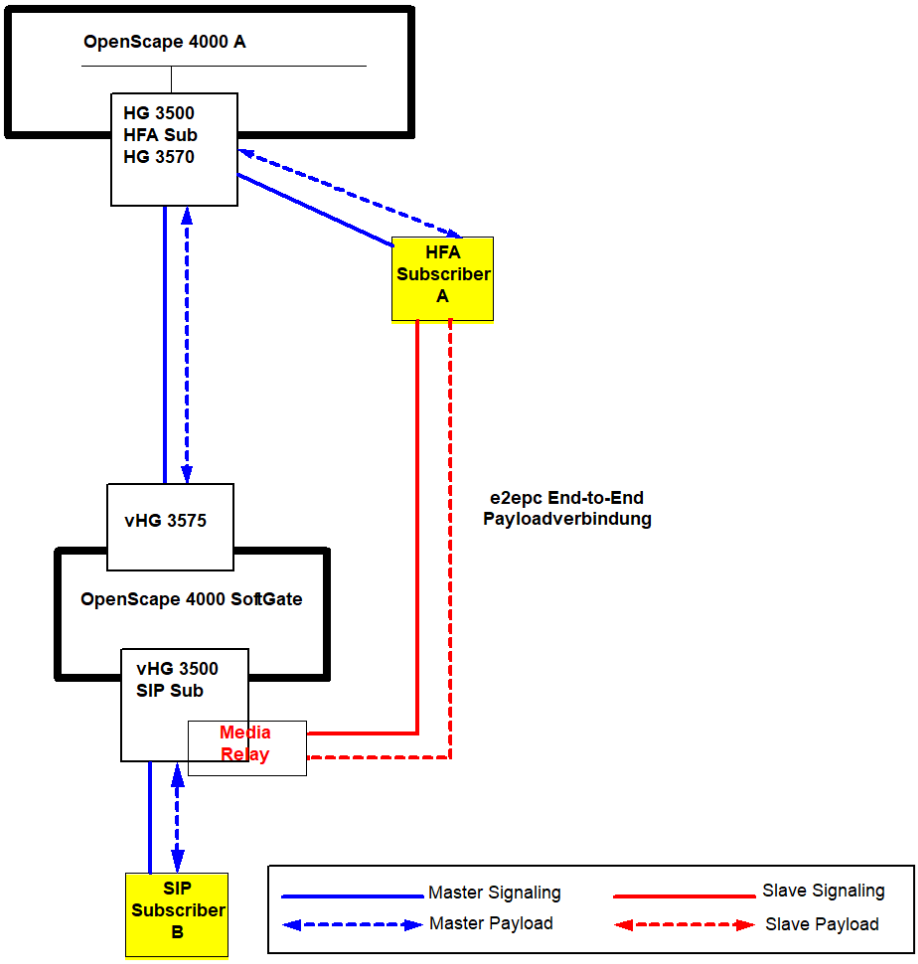


Beispiel 3: SIP-Subscriber A an OpenScape 4000 A ruft HFA-Subscriber B am OpenScape 4000 SoftGate

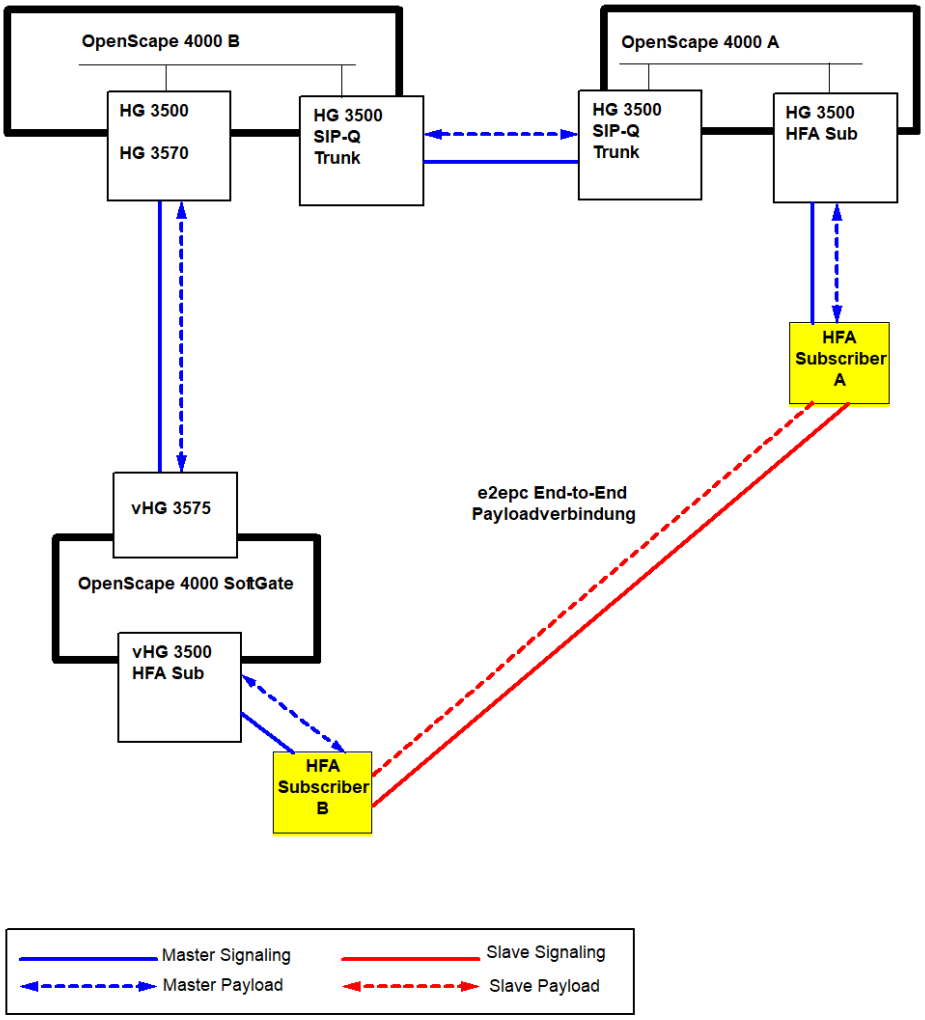


Beispiel 4: HFA-Subscriber A an OpenScape 4000 A ruft SIP-Subscriber B am OpenScape 4000 SoftGate

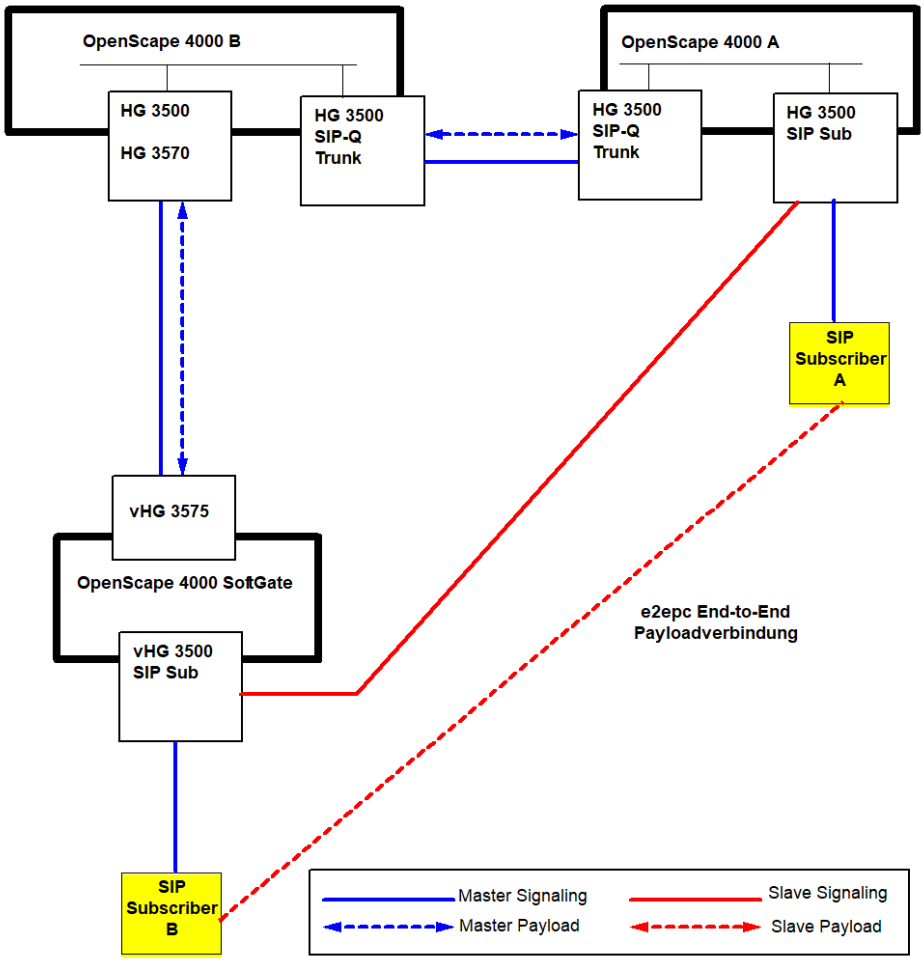
Kommuniziert ein SIP-Device oder SIP native Trunk am OpenScape 4000 SoftGate mit einem DMC-Endpoint (nicht DMC-Proxy!), dann wird immer ein Media Relay am OpenScape 4000 SoftGate dazwischen geschalten. Dies entspricht einem RTP-Proxy der den Media-Stream (RTP) immer über das OpenScape 4000 SoftGate leitet.



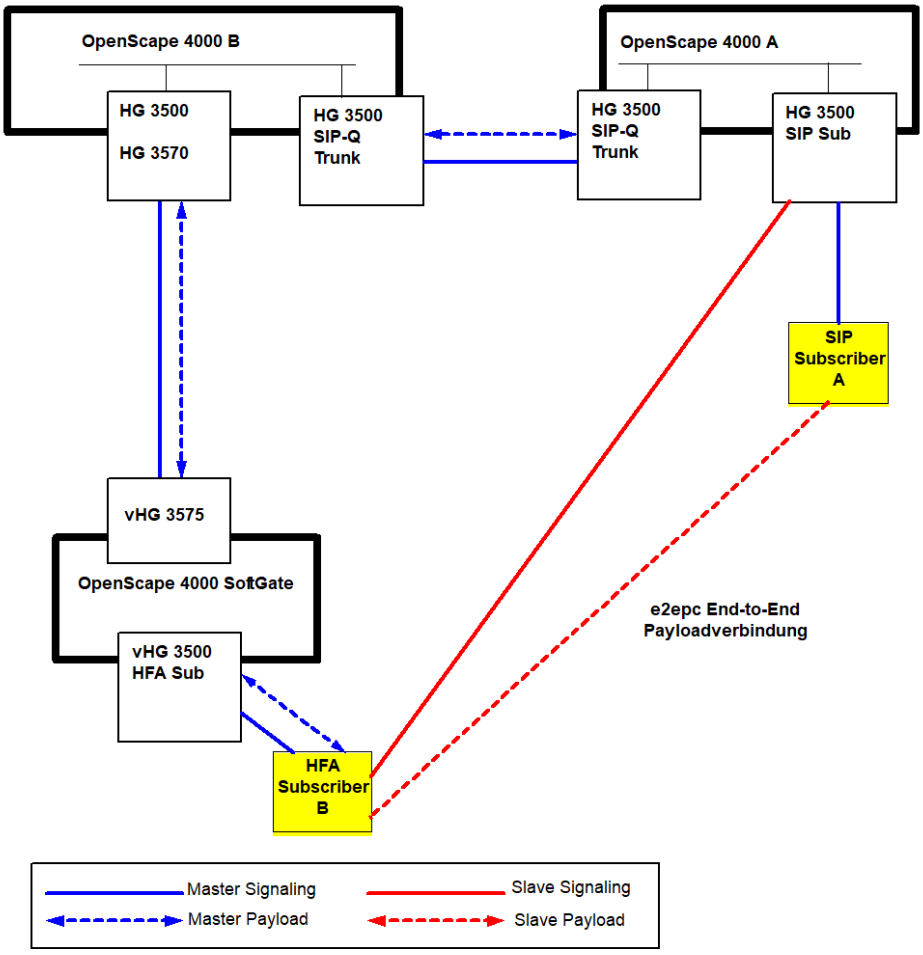
Beispiel 5: HFA-Subscriber A an OpenScape 4000 A ruft HFA-Subscriber am OpenScape 4000 SoftGate



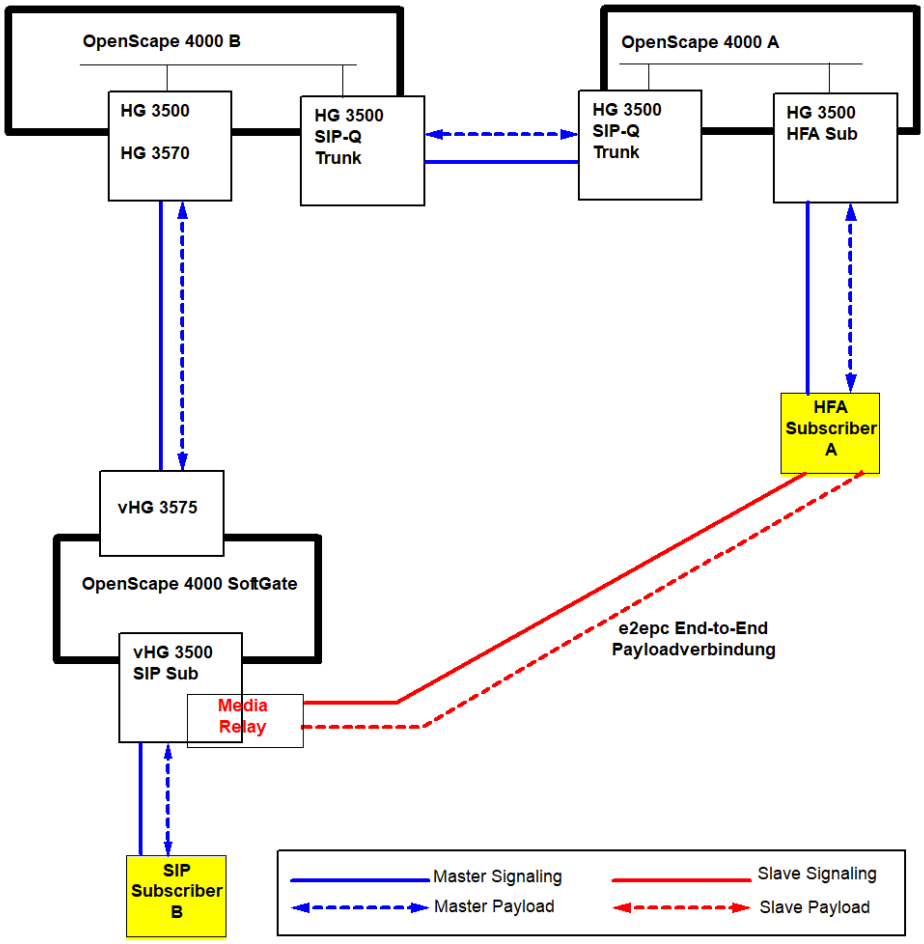
Beispiel 6: SIP-Subscriber A an OpenScape 4000 A ruft SIP-Subscriber am OpenScape 4000 SoftGate



Beispiel 7: SIP-Subscriber A an OpenScape 4000 A ruft HFA-Subscriber B am OpenScape 4000 SoftGate



Beispiel 8: HFA-Subscriber A an OpenScape 4000 A ruft SIP-Subscriber B am OpenScape 4000 SoftGate


OpenScape 4000 B
HG 3500
HG 3570
HG 3500
SIP-Q
Trunk
OpenScape 4000 A
HG 3500
SIP-Q
Trunk
HG 3500
HFA Sub
HFA
Subscriber
A
vHG 3575
OpenScape 4000 SoftGate
vHG 3500
SIP Sub
Media
Relay
e2epc End-to-End
Payloadverbindung
SIP
Subscriber
B
Master Signaling
Slave Signaling
Master Payload
Slave Payload

20 T.38 Fax

20.1 Definition

Der T.38-Faxstandard ist ein Protokoll, das die Faxübertragung über IP-Netzwerke in Echtzeit ermöglicht.

20.2 Leistungsmerkmalbeschreibung

T.38 Fax wird in Szenarien mit Common Gateway, OpenScape 4000 SoftGate, IPDA NCUI und IPDA STMI unterstützt.

20.2.1 Wichtige Hinweise

Wichtig: Bei Anschaltung eines Faxadapters an eine HG 3500 (SIP-Subscriber) muss DMC für dieses Device abgeschaltet werden (nur so kann eine Übertragung mit T.38 stattfinden). Möchte man DMC für dieses Gerät dennoch anschalten, muss der Codec fix auf G.711 eingestellt werden (Faxübertragung mit G.711, nicht T.38).

Wichtig: T.38 Fax-Streams werden für SPE nicht unterstützt

Wichtig: Auf Grund von Timing-Vorgaben des T.38 Standards, wird bei Konfiguration/Verwendung von T.38 End-to-End DMC zwischen den OpenScape 4000 Gateways (minimierte IP-Hops) benötigt. Im Falle von mehreren IP-Hops kann die Fax-Übertragung bei manchen Faygeräten fehlschlagen. Eine entsprechende Liste der Faxgeräte finden Sie in der Release Note.

Wichtig: Die Anzahl der zur Verfügung stehenden T.38 Fax-Kanäle für parallele Faxverbindungen ist 60 pro STMI. Das Limit von 60 ist unabhängig vom STMI-Typ (weder STMI2/STMI4 noch 60/120 Kanäle spielen eine Rolle). Weitere Faxe werden dann mit G.711 Clear Channel übertragen.

Wichtig: Wenn STMI4/NCUI4 Baugrupen verwendet werden, ist eine Fax-/Modemtonerkennung mit G729 Codec möglich und das Gateway schaltet autoamtisch nach G711. STMI2/NCUI2+ Baugruppen haben nicht genug Leistung um diese Umschaltung durchzuführen.

Wichtig: Wenn T.38 mit AP 1120 verwendet werden soll, muss G.711 als Sprachcodec konfiguriert werden, d.h. immer wenn

ein Modem oder Fax an einem AP 1120 angeschlossen wird, muss im AP 1120 als Sprachcodec G.711 eingestellt werden (keine Kompression möglich).

20.2.2 Einschränkungen

20.2.2.1 Verzögerungsprobleme im Szenario mit 2 und mehr IP-Hops und bestimmten Faxgeräten

Wenn die Faxübertragung über zwei oder mehr IP-Hops stattfindet, ist die Roundtrip-Verzögerung bei einigen (hauptsächlich älteren) Faxgeräten zu hoch, wenn T.38 verwendet wird. Es gibt zwei Fehlerkategorien. Im ersten Fall schlägt die Verhandlung fehl und die Faxübertragung startet überhaupt nicht. Im zweiten Fall wird die erste Seite ordnungsgemäß übertragen und empfangen, aber sie wird nicht rechtzeitig bestätigt. Dies führt dazu, dass auf dem Faxgerät ein Kommunikationsfehler angezeigt und keine zweite Seite übertragen wird.

Für die ursprünglichen Faxgeräte ist keine Lösung vorgesehen.

- Für die T.38-Konfiguration/-Nutzung ist ein End-to-End-DMC zwischen HP4K-Gateways (minimierte IP-Hops) aufgrund von Zeitanforderungen gemäß T.38-Standard erforderlich. Im Falle mehrerer IP-Hops könnte die Faxübertragung bei einigen Faxgeräten fehlschlagen. Canon FAX-L100 Canon FAX-L120 Panasonic Fax UF-595 Panasonic Fax UF-495

Lösung für betroffene Faxgeräte: Ersetzen alter Faxgeräte oder Verwendung des G711-Transparentmodus anstelle von T.38

- Wenn T.38 mit AP1120 verwendet werden soll, darf G.711 ausschließlich als Sprach-Codec verwendet werden, d. h. immer für den Fall, dass ein Modem oder Faxgerät mit einem AP1120 verbunden ist, muss der einzig zulässige Codes im AP1120 auf G.711 (keine Komprimierungsoption) eingestellt sein.

Wichtig: Wenn RFCFMOIP = ja / RFCDTMF = nein verwendet wird, gibt es mit dem MTX SIP-Adapter ein bekanntes Problem: Wenn der RFC2833 für Fax/Modem und für DTMF aktiviert ist, sendet GW Telefonereignis 32-36, 49 in der Einladung und MTX antwortet mit Telefonereignis 0-15 im 200ok. In diesem Fall wird RFC in GW insgesamt deaktiviert, aber der MTX sendet DTMF als RFC2833-Ereignisse. Daher gehen DTMF-Töne verloren.

20.2.2.2 DMC-Problem mit AP1120

Wenn G.729 als prio1-Codec eingestellt ist und das sendende Faxgerät mit dem AP1120 verbunden ist, kann es vorkommen, dass der Master-Anruf zwischen GW und AP1120 auf G.711 umgeschaltet wird, bevor das DMC eingerichtet wird. Der AP1120 erkennt den CNG und wechselt in den Datenmodus. Wenn das Faxgerät einen Anruf annimmt, wird der DMC mit G.729 eingerichtet. (Das GW sendet G.729 und der AP1120 fährt mit G.711 fort, da die Masterverbindung bereits in den Datenmodus geschaltet wurde). Nach dem Erkennen des CED-Tons auf der Empfängerseite wird ein OLC mit

G.711 an den AP1120 gesendet. Der AP1120 reagiert nicht ordnungsgemäß auf dieses OLC, da ein Wechsel zu G.711 (auf dem Masterkanal) bereits stattgefunden hat. Das GW selbst kann nicht in G.711 wechseln, da die Bestätigung durch den AP1120 fehlt. Daher sendet das GW weiterhin G.729-Pakete.

Anmerkung: Immer wenn ein Modem oder Faxgerät mit einem AP1120 verbunden ist, muss der einzig zulässige Code im AP1120 auf G.711 eingestellt sein.

20.2.2.3 DMC nicht mit MTX41xx eingerichtet

Wenn das Absende-Faxgerät in einem DMC-Szenario mit einem MTX41xx-Adapter verbunden und T.38 aktiviert ist, wird das aktivierte DMC häufig abgelehnt.

Der MTX41xx wechselt in die Standardkonfiguration in T.38, nachdem ein CNG-Ton erkannt wurde. Wenn das Absende-Faxgerät mit dem MTX41xx-Adapter verbunden ist, ist die Wahrscheinlichkeit groß, dass der erste CNG-Ton erkannt wird, bevor die Empfänger-Faxgeräte einen Anruf annehmen und der DMC eingerichtet wird. Für den Fall, dass der Masterkanal zwischen MTX41xx und SoftGate auf T.38 vor Eingang der DMC-Anfrage neu konfiguriert wurde, wird der DMC daher abgelehnt.

Abhilfe In MTX41xx gibt es den Parameter defaultMachineDetectionCngToneDetection. Wenn dieser Parameter deaktiviert wurde, wechselt der MTX41xx erst nach Erkennen von V.21-Flags in T.38.

Anmerkungen

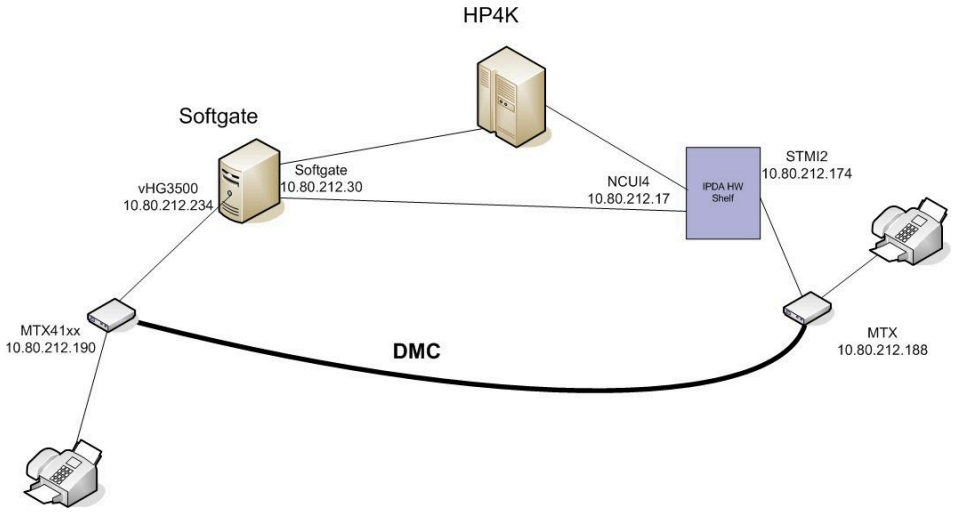
1) Wenn die CNG-Tonerkennung deaktiviert ist, findet der Wechsel zu T.38 später statt. Andererseits erkennt der Mediatrix-Adapter die V.21-Flag ausschließlich auf der SCN-Seite. Das bedeutet, dass der Adapter auf der Absenderseite das Fax sehr spät erkennt (Commerzbank-Problem). Es ist wichtig, dass das Fax auf der Empfängerseite erkannt wird.

Dieses Problem kann nur auftreten, sofern MTX41xx mit dem SoftGate verbunden ist.

1) Der Parameter „USE Previous Media Negotiation“ besteht nur in der DGWv2.0-Loadware aus Mediatrix. Daher muss auf den MTX41xx-Geräten ein Upgrade von SIPv5.0 auf die DGWv2.0-Loadware durchgeführt werden. Die Tests werden derzeit mit der DGWv2.0-Loadware durchgeführt.

20.2.2.4 Der Parameter „USE Previous Media Negotiation“ muss eingestellt sein

Wenn eine Zusammenarbeit zwischen MTX4104 (verbunden mit SoftGate) und MTX4104 (verbunden mit CGW) stattfindet, muss der Parameter „USE Previous Media Negotiation“ in MTX aktiviert sein.



Szenario mit im MTX 10.80.212.188 deaktiviertem T.38

Im oben aufgeführten Szenario ist T.38 im MTX 10.80.212.188 deaktiviert. Daher wird der DMC zugelassen. In allen anderen Komponenten ist T.38 aktiviert.

Angenommen, der Parameter „USE Previous Media Negotiation“ ist nicht eingestellt: Zuerst wird ein DMC zwischen beiden MTX41xx-Adaptern eingerichtet. Nachdem erkannt wurde, dass ein Faxgerät verbunden ist, sendet das MTX 10.80.212.190 eine erneute T.38-Einladung, die mit „488 Not Acceptable“ vom vHHG3500 10.80.212.234 abgelehnt wird. Der Grund dafür ist, dass es nicht möglich ist, Leistungsmerkmale in einem DMC-Kooperationsszenario auf dem CGW neu zu verhandeln. Nach Ablehnung des T.38 sendet Mediatrix eine erneute G.711-Einladung. Diese erneute Einladung wird ebenfalls aus dem oben angegebenen Grund abgelehnt. Nach der zweiten Ablehnung stellt MTX41xx den Anruf ein.

Wenn der Parameter „USE Previous Media Negotiation“ eingestellt ist, fährt MTX41xx mit G.711 fort, nachdem der „488 Not Acceptable“ für die erneute T.38 Einladung eingegangen ist, und die Faxübertragung funktioniert.

20.2.3 Common Gateway

T.38 ist möglich bei

- IP-Trunking-Verbindungen (H323 und H323A)
- SIP-Trunking-Verbindungen (SIP-Q und native SIP)
- DMC-Verbindungen von/zu IPDA-STMI/HG 3570

20.2.4 OpenScape 4000 SoftGate

Folgende Szenarien werden von OpenScape 4000 SoftGate unterstützt:

- Analoge Faxgeräte an Mediatrix 41xx in Verbindung mit einer virtuellen HG 3500 (SIP-Teilnehmerschnittstelle).
- Fax von Zentrale an Mediatrix 44xx in Verbindung mit einer virtuellen HG 3500 (SIP-Amtsschnittstelle).

- Fax von SIP-Provider/OpenScape Xpression in Verbindung mit einer virtuellen HG 3500 (SIP-Amtsschnittstelle).
- Fax von einem anderen OpenScape 4000/HiPath 4000 System in Verbindung mit einer virtuellen HG 3500 (SIP/SIP-Q-Amtsschnittstelle).
- Fax von einem anderen OpenScape 4000 SoftGate, IPDA NCUI oder IPDA STMI.

Alle Schnittstellen unterstützen die Umschaltung auf T.38 basierend auf Tonauswertung.

20.2.5 IPDA

Folgende Szenarien werden von IPDA unterstützt:

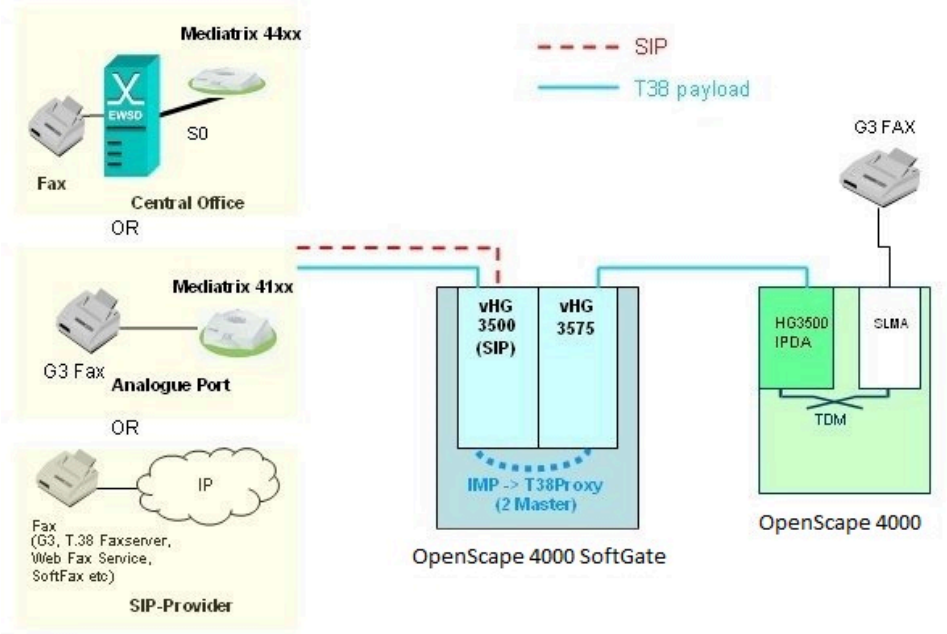
- Analoge Faxgeräte in Verbindung mit SLMA im Host- oder Access-Point-Baugruppenrahmen.
- Analoge Faxgeräte an Mediatrix 41xx in Verbindung mit HG 3500 (SIP-Teilnehmerschnittstelle).
- Fax von Zentrale in Verbindung mit der TDM-Amtsbaugruppe.
- Fax von SIP-Provider in Verbindung mit HG 3500 (SIP-Amtsschnittstelle).
- Fax von einem anderen OpenScape 4000/HiPath 4000 System in Verbindung mit HG 3500 (SIP-Amtsschnittstelle)
- Fax von einem anderen OpenScape 4000 SoftGate, IPDA NCUI oder IPDA STMI.

NCUI und IPDA STMI unterstützen die Umschaltung auf T.38 basieren auf Tonauswertung auf der Master- und der DMC-Slave-Verbindung.

20.3 Szenarien

Die Nutzung von T.38 ermöglicht auch auf dem Masterkanal. Die folgenden Abbildungen zeigen einige von OpenScape 4000 unterstützte Szenarien:

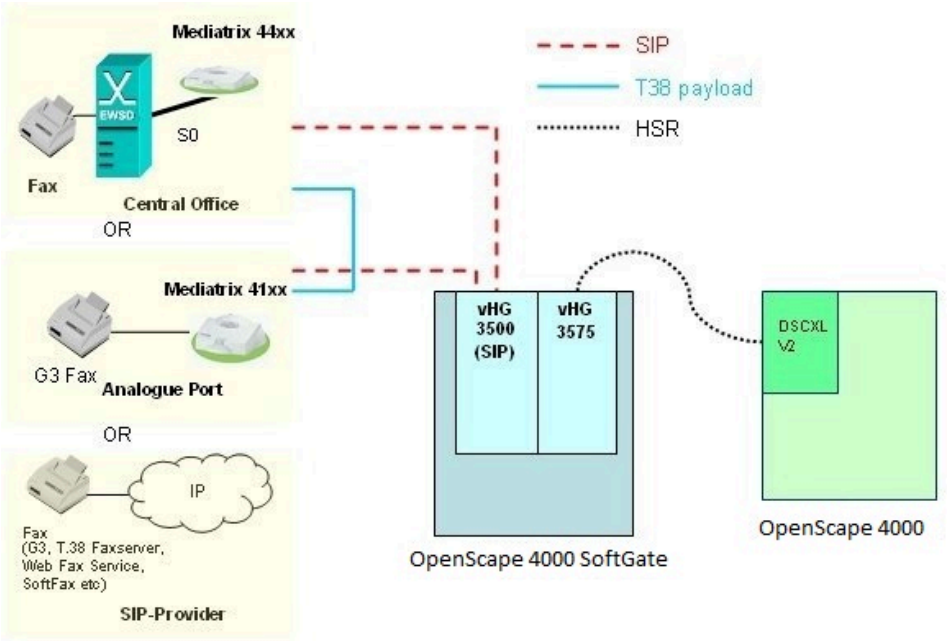
Szenario 1: OpenScape 4000 SoftGate - OpenScape 4000 Hostsystem



OpenScape 4000 SoftGate - OpenScape 4000 Hostsystem

Dieses Szenario zeigt einen typischen Faxanruf von einem kleinen Standort über OpenScape 4000 SoftGate an den Hauptstandort. In der Regel wird die Verbindung als Gesprächsverbindung hergestellt. Nach der Tonerkennung wird eine Umschaltung auf T.38 eingeleitet.

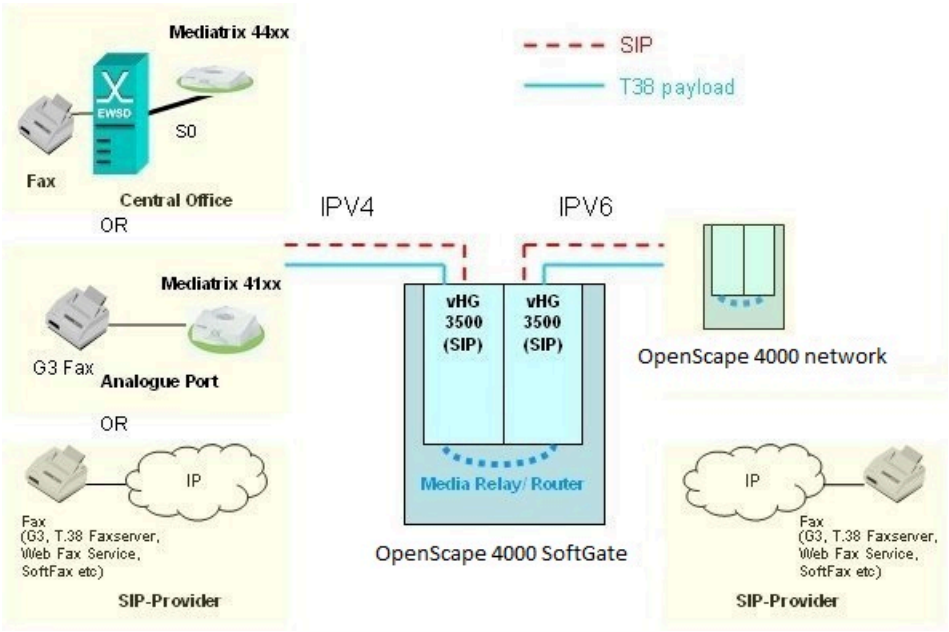
Szenario 2: Fax zwischen SMP-fähigen Endpunkten



Fax zwischen SMP-fähigen Endpunkten

Dieses Szenario zeigt einen Faxanruf zwischen SMP (SIP Message Proxy)-fähigen Endpunkten. Das Protokoll wird ohne Beteiligung des OpenScape 4000 SoftGate direkt zwischen den Endgeräten ausgehandelt.

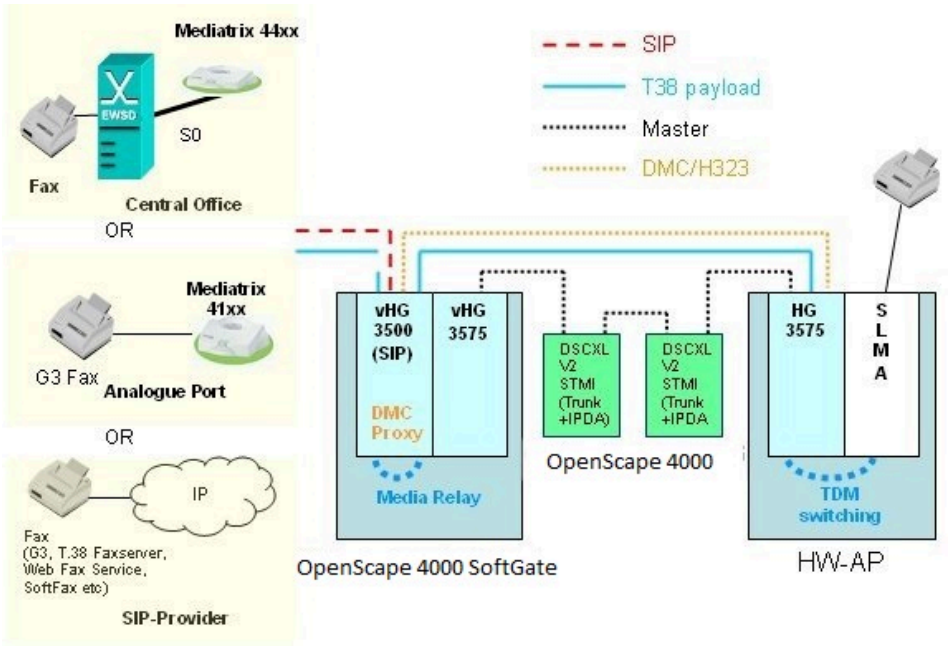
Szenario 3: Media-Routing in IPv6-Szenarien



Media-Routing in IPv6-Szenarien

Dieses Szenario zeigt einen Faxanruf zwischen IPv4 und IPv6. Die Konvertierung zwischen IPv4 und IPv6 wird vom OpenScape 4000 SoftGate durchgeführt, das als Media Relay fungiert.

Szenario 4: Media-Relay-Szenario mit DMC (Direct Media Connection)



Media-Relay-Szenario mit DMC

Dieses Szenario zeigt einen Faxanruf von einem OpenScape 4000 SoftGate über ein OpenScape 4000-Netzwerk (SIP-Q oder TDM) an einen Hardware-Access-Point.

Eine DMC-Verbindung wird eingeleitet. Falls die Faxtöne erkannt werden, bevor die DMC-Verbindung hergestellt ist, wird der DMC-Verbindungsaufbau abgebrochen und stattdessen der Masterkanal verwendet. Das OpenScape 4000 SoftGate installiert ein Media Relay zwischen SIP und H323.

20.4 Serviceinformationen

Folgende T.38-Leistungsmerkmale werden mit OpenScape 4000 SoftGate bereitgestellt:

- Codec-Wechsel bei bestehender Verbindung
- Sowohl das Mediatrix AP 41xx als auch die SIP-Provider schalten ohne Signalisierung zwischen den Codes G.729 und G.711 um. Somit wird die payloadbasierte Umschaltung bei bestehender Verbindung aufseiten des Empfängers unterstützt.
- Verbesserter Jitterbuffer
- Mit HiPath 4000 V6 wird ein größerer Puffer für T.38-Übertragungen bereitgestellt. Die Umschaltung der Puffergröße erfolgt während einer Pause (Idle) im Mediastream.
- Nutzung von RFC2833 für Fax
- RFC2833 für Faxtöne wird nicht empfohlen, aber nach wie vor unterstützt. Diese Option ist jedoch standardmäßig deaktiviert. Bei einer Aktualisierung der Software wird der zuvor konfigurierte Wert übernommen.

Wichtig: In einigen Szenarien kann die Nutzung von RFC2833 für Faxtöne Probleme verursachen. In diesem Fall muss die Option deaktiviert werden. Die ist bei den folgenden Konfigurationen der Fall: - Ein Mediatrix 41xx-Adapter wird an ein Hardware-Gateway angeschlossen und im selben System ein AP1120 Cornet IP-Adapter eingesetzt. Für den Aufbau einer DMC-Verbindung zwischen diesen beiden Adaptern muss RFC2833 für Fax deaktiviert werden. - Ein SIP-Service-Provider ohne Unterstützung für RFC2833 wird an ein Hardware-Gateway angeschlossen.

20.4.1 OpenScape 4000 SoftGate

- SIP
- Mit OpenScape 4000 SoftGate kann T.38 direkt ab dem Beginn einer Übertragung, also mit dem ersten SIP-Invite, genutzt werden.
- H323/DMC
- DMC verwendet den vorhandenen Mechanismus zur Unterstützung einer Umschaltung auf T.38 (aktiv und passiv).

20.4.2 IPDA (NCUI/STMI)

Bei IPDA können zwei hauptsächliche Faxverbindungen unterschieden werden:

- DMC (NCUI/STMI als Endpunkt) und
- Master-Aufrufe.

Master/Slave-Verbindung

Die Masterverbindung wird vom Host-System, die Slaveverbindung (DMC) hingegen von der Baugruppe selbst gesteuert.

Da IPDA-Masterverbindungen nicht von H323 gesteuert werden, erkennen IPDA-Endpunkte T.38 mittels Tonauswertung. Jeder IPDA-Endpunkt sendet eine Nachricht an DNIL in der SWU mit dem Hinweis, dass T.38 möglich ist. Wenn dies der Fall ist, wird die DMC-Verbindung abgewiesen. Nach Erhalt der Nachrichten sendet DNIL eine T.38-Pfadumschaltungsnachricht an die Endpunkte.

Einschränkungen

- Wenn keine T.38-Ressourcen verfügbar sind, wird als Alternative G.711 verwendet. Die Ressourceneinschränkung wird an DNIL signalisiert. Diese Einschränkung gilt für alle Hardware-Gateways.
- QoS-Überwachung
- Die QoS-Überwachung auf dem T.38-Kanal (dem ehemaligen Sprachkanal) wird so an T.38 angepasst, dass T.38 immer als „gute Qualität“ gilt. Daher werden keine BAD_QUALITY-Nachrichten generiert.
- Bandbreitenmanagement
- Die beanspruchte Bandbreite hängt vom ausgewählten Redundanzfaktor und der Faxübertragungsgeschwindigkeit ab. Für T.38 ist kein besonderes Bandbreitenmanagement vorgesehen; es gelten die Einstellungen für G.711 mit einer Paketgröße von 30 ms.

  Diese Einschränkungen gilt auch für Nicht-IPDA-Verbindungen.

20.5 Generierung (Beispiel)

Die folgenden Parametereinstellungen wurden einer funktionsfähigen Konfiguration entnommen und gelten für alle in diesem Kapitel beschriebenen Szenarien (siehe Kapitel 3, „Szenarien“).

```
TOSPL = 184 (184) TOSSIGNL = 104 (104)
UDPPRTLO = 29100 (29100) UDPPRTHI = 29999 (29999)
T38FAX = YES (YES) REDRFCTN = YES (YES)
RFCFMOIP = NO(NO) RFCDTMF = YES (YES)
PRIO1 : CODEC = G711A VAD = NO RTP-SIZE = 30
PRIO2 : CODEC = G729A VAD = NO RTP-SIZE = 20
PRIO3 : CODEC = G723 VAD = NO RTP-SIZE = 30
PRIO4 : CODEC = NONE VAD = NO RTP-SIZE = 20
PRIO5 : CODEC = NONE VAD = NO RTP-SIZE = 20
PRIO6 : CODEC = NONE VAD = NO RTP-SIZE = 20
PRIO7 : CODEC = G729AB VAD = YES RTP-SIZE = 20
```

20.6 Relevante AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
CGWB	T38FAX	d	Schaltet T.38 generell ein oder aus. Weitere Parameter, zur Konfiguration der T.38-Funktionalität befinden sich im WBM.
	T38FAX	e	Switches T.38 on or off generally. Further parameters for configuring the T.38 functionality are to be found in the WBM.
	RFCFMOIP	d	Schaltet RFC 2833 für Fax/Modem-Töne ein oder aus. Steht der Parameter auf JA, so werden die Fax/Modem-Töne als RFC 2833-Events übertragen. Der Parameter hat nur Einfluss auf die Tonübertragung, also auf den Sprachkanal. Somit ist er nur in der Phase vor dem Start des T.38-Stacks relevant. Der Parameter muss im gesamten System auf den gleichen Wert gesetzt wird.
	RFCFMOIP	e	Switches RFC 2833 for fax/modem tones on or off. If the parameter is set to YES, the fax/modem tones are transmitted as RFC 2833 events. The parameter influences only the tone transmission, that is, the speech channel. Thus, it is only relevant within the phase before the T.38 stack is started. The parameter must be set to the same value in the entire system.
	REDRFCTN	d	Schaltet RFC 2198 ein oder aus. Steht der Parameter auf JA, so werden die RFC 2833-Events redundant übertragen. Der Parameter hat nur Auswirkungen, wenn RFC 2833 eingeschaltet ist (RFCFMOIP=JA). Der Parameter muss im gesamten System auf den gleichen Wert gesetzt wird.

AMO	Parameter	Sprache/ Language	Beschreibung/ Description
	REDRFCTN	e	Switches RFC 2198 on or off. If the parameter is set to YES, the RFC 2833 events are transmitted in redundant fashion. The parameter is only effective when RFC 2833 is switched on (RFCFMOIP=YES). The parameter must be set to the same value in the entire system.

21 IP-Endgeräte

21.1 Unterstützte IP-Endgeräte

Die folgenden IP-Endgeräte (HFA) werden unterstützt:

- OpenStage HFA
- OpenScape Desk Phone IP 35G HFA
- OpenScape Desk Phone IP 55G HFA
- optiPoint 410/420 CorNet IP
- AP 1120 CorNet-IP (nur HG 3500)
- AC-Win IP
- OpenScape Personal Edition HFA
- OpenScape UC Web Embedded Client
- OpenScape Desk Phone CP100/110/200/210/400/410/600/700/710 HFA

IMPORTANT: Die freigegebenen SIP-Endgeräte finden Sie im Abschnitt "SIP-Konnektivität" > Kapitel 2, "SIP-Abonnent".

21.2 Baugruppen

IP-Endgeräte können auf folgenden Baugruppen mit Ethernet-Schnittstelle konfiguriert werden:

- STMI2 (Q2316-X)
- STMI2 (Q2316-X10)
- STMI4 (Q2324-X500)
- STMI4 (Q2324-X510)
- STMIX (Q2343-X)
- vHG 3500 mit OpenScape 4000 SoftGate

Wichtig: Ab V10R0 wird die Unterstützung für STMI2 nicht mehr angeboten. Der Ersatz für STMI2 ist STMIX.

Wichtig: Das folgende Dokument bezieht sich der Einfachheit halber nur auf die STMI-Baugruppe. Dieser Begriff wird allgemein für alle geeigneten Baugruppen verwendet. Der Begriff „HFA-Port“ wird im Folgenden zur Beschreibung eines IP-Ports verwendet, an den alle IP-Systemtelefone angeschlossen werden können.

21.3 optiPoint-IP-Endgeräte

21.3.1 Allgemeine Informationen

An ein optiPoint IP Endgerät können Sie über die entsprechenden Adapter, die im Telefon stecken müssen bzw. bereits integriert sind, weitere Endgeräte anschließen:

- Der USB-Adapter (OPTIUSB) ist in den meisten optiPoint 410 Telefonen bereits hardwaremäßig integriert.
- Um einen PC per USB-Adapter als Simple Dialer anschließen zu können, wird jedes optiPoint 410 bereits beim Konfigurieren grundsätzlich mit der „Control Adapter“ Funktionalität versehen.

Sie können an ein optiPoint 410 IP Telefon maximal 2 Beistellgeräte anschließen. Dies müssen Sie mit dem Parameter **BEIGER** angeben. Weitere Beistellgeräte können zwar eingerichtet werden, gehen aber nicht in Betrieb.

Wichtig: Analoge Endgeräte erfordern eine lokale Speisung der optiPoint mittels Steckernetzteil. Die landesspezifischen und übertragungstechnischen Einstellungen erfolgen zentral über `AMO ZAND:TYP=OPTISET,TAABLKZ=<string>`.

21.3.2 optiPoint 410/420

21.3.2.1 Endgerätetypen

Es gibt verschiedene optiPoint 410 Telefontypen, die sich durch ihren Funktionsumfang und die Ausbaumöglichkeiten unterscheiden. Nachfolgende Tabelle gibt einen Überblick:

optiPoint Telefontypen	Anzahl Funktions-tasten	Display *) beleuchtet	Anzahl Adapter-Einbau-plätze	Anzahl mögl. Beistell-geräte	USB 1.1 *) Master	Headset Anschluss
optiPoint 410 entry	8	nein	0	0	nein	nein
optiPoint 410 economy	12	ja	0	0	nein	nein
optiPoint 410 standard	12	ja *)	2	2	ja	ja
optiPoint 410 advance	19	ja *) 4 Zeilen	1	2	ja *)	ja
optiPoint 420 advance (je Label max. 12 Zeichen)	18	ja *) 4 Zeilen	1	2	ja *)	ja

Alle optiPoint 410 unterstützen die Speisung nach „Power over LAN“ (Cisco oder IEEE 802.3af). Ein Einsatz eines Steckernetzteiles parallel dazu ist möglich.

21.3.2.2 Adapter und Zusatzgeräte

Folgende optiPoint Adapter und Zusatzgeräte können am optiPoint 410 Systemtelefon betrieben werden:

Gerätetyp	Funktion	AMO-Parameter
optiPoint USB Adapter (bereits im Telefon integriert)	zum Anschluss von Standard S0-Datenendgeräten	OPTIUSB
optiPoint key module	Beistellgerät mit 15 freiprogrammierbaren Funktionstasten und 1 Shift-Taste)	BEIGER
optiPoint 420 key module	Beistellgerät mit 13 Tasten mit Electronic Key Labelling Funktionalität, davon 12 frei programmierbar (je Label max. 12 Zeichen) (und 1 Shift-Taste)	BEIGER
optiPoint signature module	Beistellgerät mit Chipkartenleser (SmartCardReader)	TAWL
OpenStage Belegtlampenfeld	Belegtlampenfeld mit 90 beleuchteten, freiprogrammierbaren Tasten	OPTIBLF
optiPoint Display Modul	zum Bereitstellen der LDAP/WAP und ENB Funktion, sowie der JAVA VM	---
optiPoint recorder adapter	zum Anschluss eines Zweithörers oder eines externen Recorders	---
optiPoint acoustic adapter	zum Anschluss von Zubehör (Lautsprecher, Mikrofon, Headset, ...)	---

Der OPTIUSB („optiPoint USB adapter“) wird automatisch beim Einrichten eines funktionalen Endgerätes eingerichtet, sofern nicht bereits vorhanden.

Ein physikalischer Adapter ist nicht erforderlich, da die Funktion je nach Endgerät bereits fest implementiert ist.

Wichtig: Mit dem Kommando ABFRAGEN-SBCSU:TLNNU=number; werden alle eingerichteten Adapter, d.h. sowohl die explizit eingerichteten als auch die automatisch eingerichteten, angezeigt.

21.3.2.3 Module bei optiPoint-Endgeräten

- Es ist maximal ein „optiPoint signature module“ je optiPoint-Endgerät möglich.

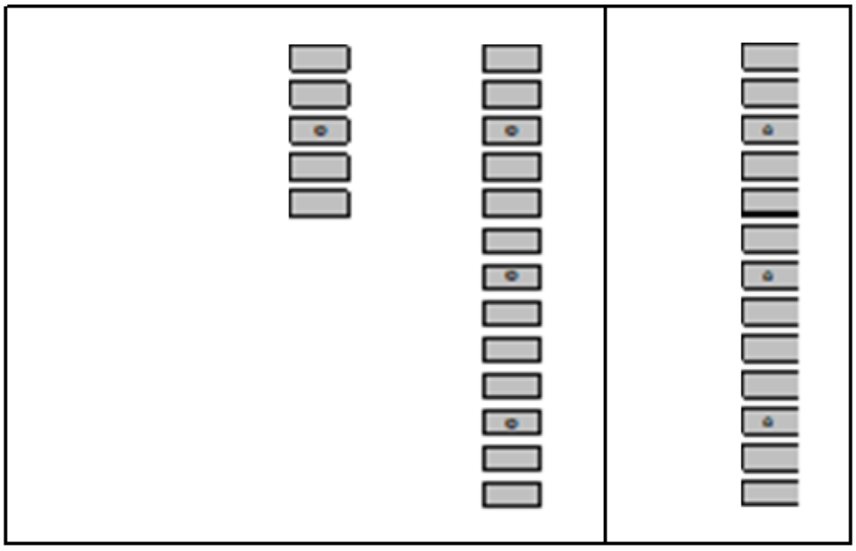
- Ein „optiPoint 420 key module“ darf nur im spannungslosen Zustand an ein optiPoint 410 angebracht werden.
- Für das „optiPoint display module“ ist keine eigene Konfiguration im System notwendig.

Wichtig: Grundsätzlich muss bei einer Konfiguration mit „optiPoint acoustic adapter“ bei dem derKontakt genutzt werden soll ein passendes Steckernetzteil angeschlossen werden.

- Es kann maximal ein „optiPoint display module“ am optiPoint 410 angeschlossen werden.
- Ein „optiPoint display module“ muss immer direkt als erstes Beistellgerät am optiPoint 410 angeschlossen werden.

21.3.2.4 Tastenlayout bei optiPoint-Endgeräten

Die Anordnung der Tasten eines optiPoint 410 advance und optiPoint 420 advance sind nicht identisch.



Tastenanordnung optiPoint 420 advance und optiPoint 420 key module

21.3.3 OpenStage WL3/WL4

Das Telefon OpenStage WL3/WL4 ist die Weiterführung der Telefone für mobile Arbeitsplätze, die als Übertragungsmedium die WLAN-Technologie nutzen. Es wird von OpenScape 4000 als SIP-Telefon erkannt und behandelt.

Weitere Informationen zum OpenStage WL3/WL4 finden Sie im Intranet auf E-Doku: http://apps.g-dms.com:8081/techdoc > Product: OpenStage WL3/WL4.

Für die Konfiguration in der OpenScape 4000 siehe Abschnitt 8.4, „OpenStage WL3/WL4-Konfiguration“.

21.3.4 Weitere Adapter und Anschlüsse

21.3.4.1 OpenStage Belegtlampenfeld

Wichtig: Das Openstage Belegtlampenfeld ist auch am optiPoint 410/420 IP freigegeben.

Der Wert **OPTIBLF** für **DIGTYP** ist für das Belegtlampenfeld im AMO TAPRO eingeführt worden. Ein Layout mit diesem Typ muss für die Tasten-Layout-Konfiguration eines optiPoint Endgerätes mit BLF verwendet werden.

Die Tastenkonfiguration ist ähnlich zu der eines OpenStage Endgerätes mit Belegtlampenfeld. Es werden alerdings nicht 90 Tasten auf einem Beistellgerät konfiguriert, sondern 5 Beistellgeräte mit jeweils 18 Tasten, d.h. jede Spalte mit je 18 Tasten auf dem Belegtlampenfeld kann man sich als ein Beistellgerät vorstellen.

Konfiguration

Es muss eine Nummer für das Tastenlayout (z.B. **SNU=127**) dem **DIGTYP=OPTIBLF** zugewisen werden.

Beispiel:

```
AENDERN-TAPRO:SNU=127,DIGTYP=OPTIBLF,TD01=CH;
REGEN-TAPRO:TYP=STD,SNU=127;
```

1)
```
AENDERN-TAPRO:,127,OPTIBLF ,CH ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,
                           " ";
  AENDERN-
  TAPRO:,127,OPTIB1 ,FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ;
  AENDERN-
  TAPRO:,127,OPTIB2 ,FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ;
  AENDERN-
  TAPRO:,127,OPTIB3 ,FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ;
  AENDERN-
  TAPRO:,127,OPTIB4 ,FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ;
  AENDERN-
  TAPRO:,127,OPTIB5 ,FREI ,FREI ,FREI ,FREI ,FREI ,
                           FREI ,FREI ,FREI ,FREI ,FREI ,
```

```
                                FREI ,FREI ,FREI ,FREI ,FREI ,
                                FREI ,FREI ,FREI ;
AMO-TAPRO-111        TASTENPROGRAMMIERUNG DIGITE

REGENERIEREN DURCHGEFUEHRT;
```

Zusätzlich müssen im AMO SBCSU die Parameter **BEIGER=0** und **BLF=JA** für den Teilnehmer gesetzt sein.

21.3.4.2 optiPoint Recorder Adapter

Der Recorder Adapter ermöglicht den Anschluss eines analogen Aufzeichnungsgerätes oder eines Zweithörers an einem bestehenden optiPoint 410 Gerät.

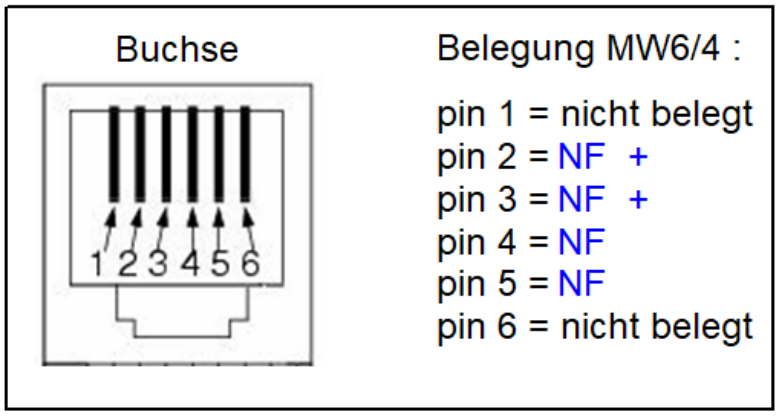
Wichtig: Dieser Adapter wird in der PBX nicht konfiguriert und besitzt somit in der Abfragemaske des AMO SBCSU keinen Parameterwert.

21.3.4.2.1 Anschluss für Aufzeichnungsgerät (Daten nicht veränderbar)

An der Buchse liegen die Signale des Handapperates (RX und TX) im Gesprächszustand gemeinsam an.

1) Impedanz: 6k Ohm

2)
- Frequenzbereich: 300 bis 3000 Hz (+/- 3dB)
- Pegel: 1,77Vrms an 600 Ohm

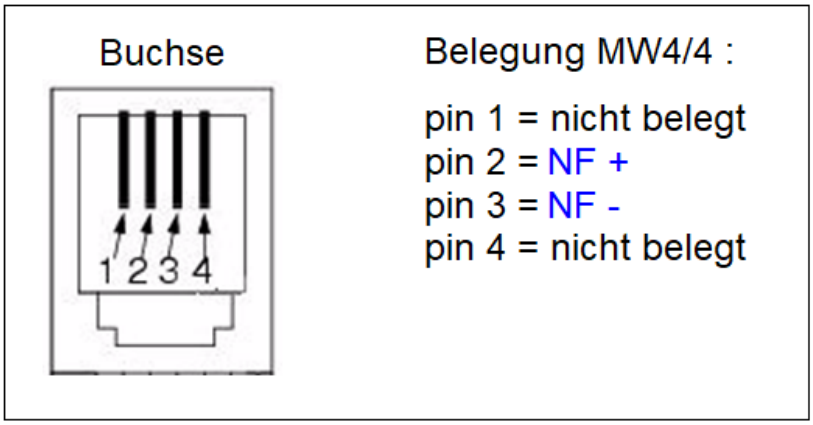


Belegung Recorder interface

21.3.4.2.2 ZweithörerAnschluss

Nach dem Anschluss eines Zweithörers ist dieser sofort benutzbar und die Lautstärke richtet sich an die des Telefons in dem der Adapter sich befindet.

Die Lautstärke für diesen Anschluss ist nicht getrennt einstellbar.



Belegung ZweithörerAnschluss

21.3.4.3 optiPoint Acoustic Adapter

Der Acoustic Adapter ermöglicht den Anschluss eines externen Microphones und Lautsprechers sowie eines Headsets (schnurlos oder drahtgebunden) an einem bestehenden optiPoint 410 Gerät. Zudem bietet der Adapter zwei potentialfreie Kontakte.

Wichtig: Dieser Adapter wird in der PBX nicht konfiguriert und besitzt somit in der Abfragemaske des AMO SBCSU keinen Parameterwert.

21.3.4.4 Mikrofon und Lautsprecher Anschluss

An diesem Anschluss kann mittels eines Y-Kabels ein Beistellmicrofon und eine aktiv Lautsprecherbox betrieben werden.

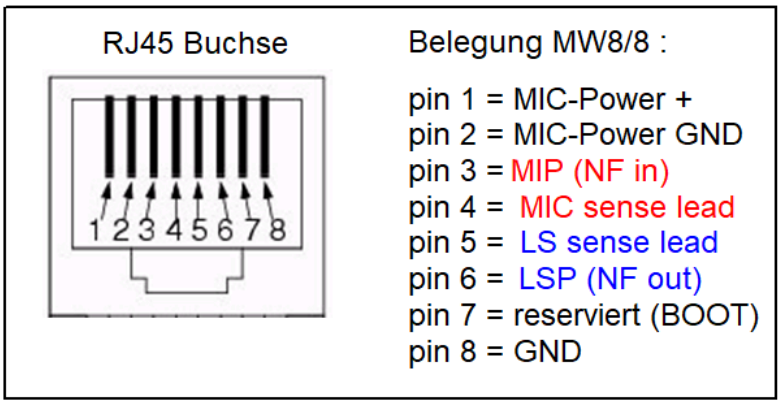
Wichtig: Sind externe Geräte angeschlossen, so sind die jeweiligen internen deaktiviert. Eine Konfigurationsänderung in der PBX ist nicht erforderlich.

---

1) Die Lautstärke kann wie für das Telefon verändert werden.

2) • Der externe Lautsprecher muss einen eigenen Verstärker und Stromversorgung besitzen

.



Belegung Mikrofon/Lautsprecher Anschluss

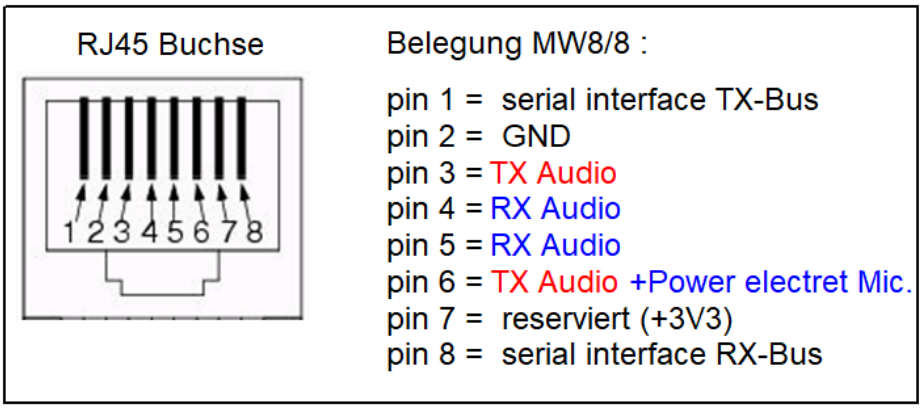
21.3.4.5 Headset Anschluss

An diesem Anschluss können Kopfsprechgarnituren mit und ohne Taste, sowie auch schnurlose oder drahtgebundene Garnituren eingesetzt werden.

Wichtig: Wird eine Kopfsprech-Garnitur ohne HW Indikation (d.h. Stecken/Ziehen wird von der HW n i c h t erkannt) eingesetzt, so muss diese durch Drücken der SG Taste (SprechGarnitur, durch AMO TAPRO zugewiesen) bekannt gemacht werden. Im AMO SBCSU muss der Parameter KOPFSG auf OHNEIND und TASTSG entsprechend der Funktion gesetzt werden

---

Ein Headset mit MW4/4 Anschluss benötigt einen Adapter:



Belegung Headset Anschluss

21.3.4.6 Kontakt Anschluss

Der Kontakt „Klingel“ wird beim erhalten einer Alert-Meldung für das Endgerät aktiviert.

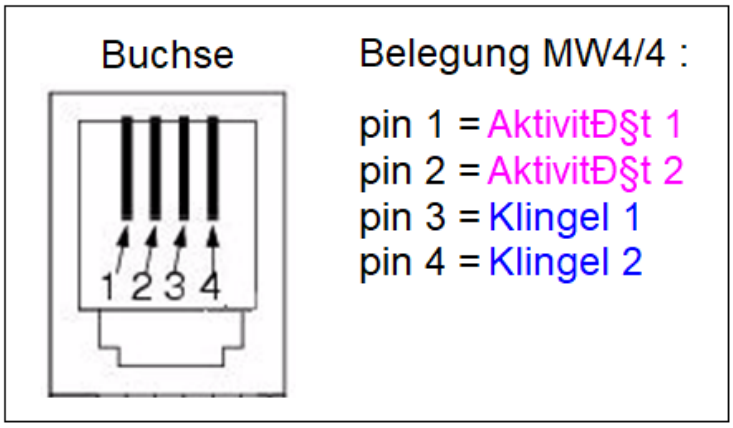
Der zweite Kontakt „Aktivität“ läßt sich durch Drücken der mittels AMO TAPRO konfigurierten Tasten (BUSYLAMP oder DOOROPEN) aktivieren. Dabei wird beim ersten Drücken der Taste „BUSYLAMP“ der Kontakt geschlossen und beim zweiten Drücken wieder geöffnet. (Analog dazu wird die LED der zugehörigen Taste gesetzt und auch wieder rückgesetzt)

Wichtig: Dieser Adapter wird in der PBX nicht konfiguriert, muss aber vorhanden sein, um die Funktion Türoffner und Besetzlampe mittels Tasten nutzen zu können.

---

1) Die Kontakte sind zum Telefon hin galvanisch getrennt

2)
- Belastbarkeit der Kontakte bei AC: 24V / 5W
- Belastbarkeit der Kontakte bei DC: 60V / 5W



Belegung Kontakt Anschluss

Wichtig: Für die Funktion Klingelkontakt muss ein externes Netzteil vorhanden sein. (Nicht nötig, wenn nur Headset oder Mikrofon/Lautsprecher genutzt werden.)

21.4 OpenStage IP-Endgeräte

Die OpenStage-Endgeräte-Familie ist für den Betrieb an OpenScape 4000 freigegeben. Die genauen Endgerätetypen entnehmen Sie bitte den enstprechenden Freigabemitteilungen.

21.4.1 Hardware und allgemeine Leistungsmerkmale

Siehe Datenblatt zu den OpenStage-Endgeräten (http://apps.g-dms.com:8081/techdoc/de/P31002S2000D101010029/index.htm).

Wichtig: Es gibt keine Adapter für OpenStage-Endgeräte.

Wichtig: Die beiden Key Module, Application Module, Display Module, Belegtlampenfeld und Adapter der optiPoint Endgerätefamilie können nicht zusammen mit OpenStage verwendet und betrieben werden. Die einzige Ausnahme bildet das externe Netzgerät (L30250-F600-A190-A191-A192) zur Speisung der Telefone.

21.4.2 Tastenbelegung

OpenStage-Endgeräte haben fest beschriftete Tasten (so genannte Fixed Keys). Daher müssen die richtigen Tastenstandards zugewiesen werden. Die Tasten 1-8 müssen den Beispielen in Abschnitt 8.5, „OpenStage Konfiguration“ entsprechen. Ab Taste 9 beginnen die variablen Tasten.

Auch für das Endgerät selber kann eine Shift-Taste programmiert werden.

21.4.3 Beistellgeräte (Key Module)

Ein OpenStage-Endgerät kann maximal 2 Beistellgeräte (Key Module) haben. Mit der Shift-Taste kann zwischen 2 Eben umgeschaltet werden.

Gerätetyp	Funktion	AMO-Parameter
OpenStage key module	Beistellgerät mit 15 freiprogrammierbaren Funktionstasten (und 1 Shift-Taste)	BEIGER

Shift-Taste

Wenn an einem optiPoint Beistellgerät die Shift-Taste gedrückt wird, so wirkt sich das immer auf alle Beistellgeräte aus, d.h. es werden auch am 2. bis 4. Beistellgerät die Shift-Ebene umgeschaltet.

Bei einem OpenStage-Endgerät/-Beistellgerät ist das anders. Hier wirkt sich jeder Shift-Tasten-Druck nur auf das Gerät aus an dem die Taste gedrückt wurde.

21.4.4 OpenStage in Verbindung mit optiClient

Die folgenden Einrichtungs-Hinweise und geschilderten Einschränkungen gelten vorübergehend für die erste Version des Release 2. Ein verbessertes Handling wird so schnell wie möglich bereitgestellt.

- Das openStage vom Typ „nn“ muss mit einem Tastenstandard „openStage nn“ eingerichtet werden.
- Änderungen der Tastenbelegung an einem Endgerät (AMO TAPRO) dürfen nicht durchgeführt werden, wenn der optiClient aktiv ist.
- Das individuelle Einrichten von Tastenbelegungen durch den Teilnehmer darf für die Kombination optiClient/openStage **nicht** freigegeben sein.

- Wenn der Teilnehmer vorher die Kombination optiClient/optiPoint benutzt hat, ist er über die sichtbar veränderte Tastenbelegung im optiClient zu informieren. Diese ist durch die feste Tastenbelegung bei openStage Telefonen bedingt.

Wenn die genannten Einschränkungen nicht beachtet werden, ist die korrekte Tastenbelegung im Wechsel zwischen optiClient und OpenStage nicht gewährleistet. Im Fehlerfall kann dies nur durch Löschen und Neu-Einrichtung des Anschlusses repariert werden.

Neuen Anschluss mit optiClient/openStage einrichten:

Neu-Einrichten des openStage Telefons mit dem dazugehörigen Tastenstandard plus der Konfiguration eines optiClient (OPTIIP&API).

In der Applikation optiClient ist in den Einstellungen das Device „optipoint 420 advance“ zu aktivieren.

Bestehende Konfiguration optiClient/optiPoint ersetzen durch optiClient/ openStage:

1) Regenerieren der Teilnehmer-Daten
2) Anschluss vollständig löschen
3) Hinweis: das Löschen ist notwendig, da zur Zeit nur so der sogenannte Hintergrundspeicher für Tastenbelegungen gelöscht werden kann. Geschieht dies nicht, ist eine richtige Tastenbelegung sowohl beim optiClient als auch beim openStage nicht gewährleistet. Es hängt von der Vorgeschichte am Anschluss (z.B. ob verschiedene Endgeräte gesteckt waren usw) ab, ob der Hintergrundspeicher gelöscht werden muss.
4) Endgerät kann jetzt getauscht werden
5) Neu-Einrichtung des Anschlusses mit dem openStage Telefon mit dem dazugehörigen Tastenstandard plus der Konfiguration eines optiClient (siehe oben)
6) oder Endgerät jetzt tauschen

21.4.5 Belegtlampenfeld

Leistungsmerkmalbeschreibung

Das OpenStage Belegtlampenfeld ist ein seitlich am Telefon zu montierendes Beistellgerät, das Ihnen 90 beleuchtete, freiprogrammierbare Tasten bietet.

Diese Tasten können Sie, wie am Telefon, nach Ihren Wünschen belegen.

Serviceinformation

- Es kann maximal 1 OpenStage Belegtlampenfeld an einem OpenStage-Endgerät angeschlossen.
- Nur interne Ziele können programmiert werden.

Konfiguration (Beispiel)

Einrichtung des Belegtlampenfeldes:
`AENDERN-TAPRO:SNU=61,DIGTYP=OST30BLF;`

Relevant AMOs

AMO	Parameter	Sprache/ Language	Beschreibung/ Discription
TAPRO	DIGTYP	d	OST30BLF - OpenStage 30 BLF OST40BLF - OpenStage 40 BLF OST60BLF - OpenStage 60 BLF (entkoppelte Freigabe)
	DIGTYP	e	OST30BLF - OpenStage 30 BLF OST40BLF - OpenStage 40 BLF OST60BLF - OpenStage 60 BLF (decoupled release)

21.5 OpenScape Desk Phone IP 35G/55G HFA

Das OpenScape Desk Phone IP 35G HFA und das OpenScape Desk Phone IP 55G HFA sind für den Betrieb an OpenScape 4000 freigegeben (ab OpenScape 4000 V7 R1).

21.5.1 Hardware und allgemeine Leistungsmerkmale

Siehe Datenblatt zu den OpenScape Desk Phone IP 35G/55G HFA-Endgeräten.

21.5.2 Tastenbelegung

Die OpenScape Desk Phone IP 35G/55G HFA Endgeräte haben fest beschriftete Tasten (so genannte Fixed Keys). Daher müssen die richtigen Tastenstandards zugewiesen werden (siehe Abschnitt 8.6, „OpenScape Desk Phone IP Konfiguration“). Ab Taste 9 beginnen die variablen Tasten.

21.5.3 Beistellgeräte

Am OpenScape Desk Phone IP 35G HFA kann **kein** Key Modul angeschlossen werden.

Am OpenScape Desk Phone IP 55G HFA können bis zu 2 Key Module mit elektronischen Labels angeschlossen werden.

Tabelle 89: OpenScape Key Modul 55

Gerätetyp	Funktion	AMO-Parameter
OpenScape Key Modul 55	Key Modul mit 12 freiprogrammierbaren Funktionstasten auf maximal. 2 Ebenen	BEIGER

21.6 OpenScape Desk Phone CP HFA

Die OpenScape Desk Phones CP100, OpenScape Desk Phones CP200/205 HFA und die OpenScape Desk Phones CP400/600 HFA sind für den Einsatz an OpenScape 4000 (ab OpenScape 4000 V8 R1) und OpenScape Desk Phones CP700/700X ab OpenScape 4000 V10R0 freigegeben.

Die OpenScape Desk Phones CP110, OpenScape Desk Phones CP210 HFA und die OpenScape Desk Phones CP410 HFA sind für den Einsatz an OpenScape 4000 (ab OpenScape 4000 V8 R2) und OpenScape Desk Phones CP710 ab OpenScape 4000 V10R1 freigegeben.

21.6.1 Hardware und allgemeine Merkmale

Siehe das Datenblatt der OpenScape Desk Phone CP100/110/200/210/400/410/600/700/710 HFA-Endgeräte.

21.6.2 Tastenbelegung

Die OpenScape Desk Phone-Endgeräte haben fest beschriftete Tasten (so genannte Fixed Keys). Aus diesem Grund müssen die richtigen Standardtastenbelegungen zugewiesen werden (siehe Abschnitt Abschnitt 8.7, "Desk Phones CP-Konfiguration").

21.6.3 Tastenmodule

Es ist **nicht** möglich, ein Tastenmodul an das OpenScape Desk Phone CP100/110/200/205/210 HFA anzuschließen.

Am OpenScape Desk Phone CP 400 können bis zu 2 Key Module mit Papierbeschriftungen angeschlossen werden.

Am OpenScape Desk Phone CP 600 können bis zu 2 Key Module mit elektronischen Beschriftungen angeschlossen werden.

An das OpenScape Desk Phone CP700 HFA können bis zu zwei Tastenmodule (KM600) mit elektronischen Etiketten angeschlossen werden.

An das OpenScape Desk Phone CP700X HFA können bis zu vier Tastenmodule (KM600) mit elektronischen Etiketten angeschlossen werden.

An das OpenScape Desk Phone CP410/CP710 HFA können bis zu vier Tastenmodule (KM410) mit Papieretiketten angeschlossen werden.

An das OpenScape Desk Phone CP410/CP710 HFA können bis zu vier Tastenmodule (KM710) mit elektronischen Etiketten angeschlossen werden.

Table 90: OpenScape-Tastenmodule

Gerätetyp	Funktion	AMO-Parameter
OpenScape Key Module KM400	Key Modul mit 16 freiprogrammierbaren Funktionstasten auf maximal. 2 Ebenen	BEIGER

Gerätetyp	Funktion	AMO-Parameter
OpenScape Key Module KM600	Key Modul mit 12 freiprogrammierbaren Funktionstasten auf maximal. 2 Ebenen	BEIGER
OpenScape Key Module KM410	Tastenmodul mit 16 frei programmierbaren Funktionstasten (auf max. 2 Ebenen)	BEIGER
OpenScape Key Module KM710	Tastenmodul mit 12 frei programmierbaren Funktionstasten (auf max. 2 Ebenen)	BEIGER

21.7 Serviceinformation

- Ein IP Endgerät muss nicht nur im System eingerichtet werden, sondern es müssen auch am Endgerät selbst entsprechende Konfigurationen vorgenommen werden.
- Wenn SPE bei den IP-Endgeräten aktiviert ist, muss ein externer NTP-Server für die Zeitsynchronisation verwendet werden. Hierfür **darf nicht** der OpenScape 4000 Assistant verwendet werden. Die Performance der Hardware/Software des OpenScape 4000 Assistant ist hierfür nicht ausreichend.
- Ein SoftClient wird wie ein entsprechendes optiPoint Telefon konfiguriert (ein Tausch eines optiPoint IP Telefon gegen einen Softclient ist somit möglich).
- Die LAN Port Einstellungen am Telefon sind immer so zu wählen, dass ein „Duplex Missmatch“ vermieden wird.
- OpenStage-Endgeräte haben keine Adapter
- Eine Host/Client-Konfiguration ist nur mit OpenStage-Endgeräten möglich.

21.8 Generierung IP-Endgeräte

Detaillierte Informationen zu HFA finden Sie im Dokument .

Bei allen Generierungen ist zu beachten, dass auch am Endgerät selbst Einstellungen nötig sind.

So sind zum einem die Netzwerk relevanten Daten zu konfigurieren, wobei diese bei entsprechender Konfiguration des Telefons auch via DHCP automatisch bezogen werden können (Werksseitig als Default):

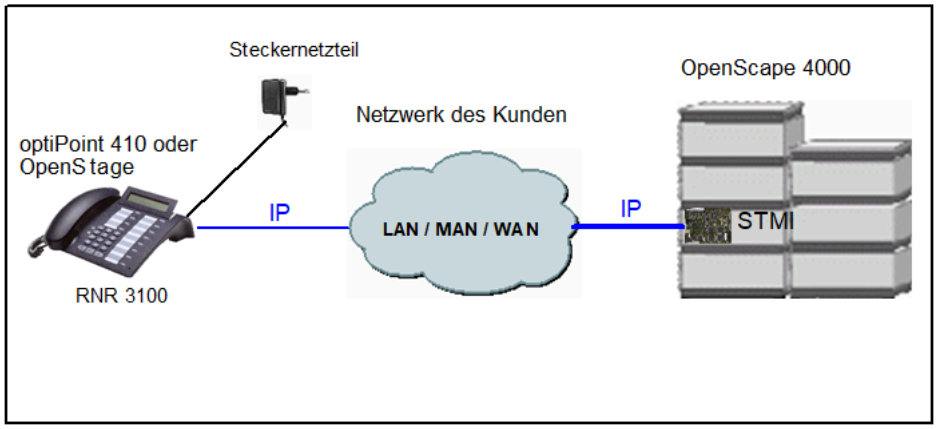
- **Terminal IP Address (TLN IP)**
- **Terminal Mask (Netzmaske)**
- **Standard-Gateway**
- (VLAN ID)

Zum anderen die zwingend erforderlichen Systemparameter für den HFA Betrieb:

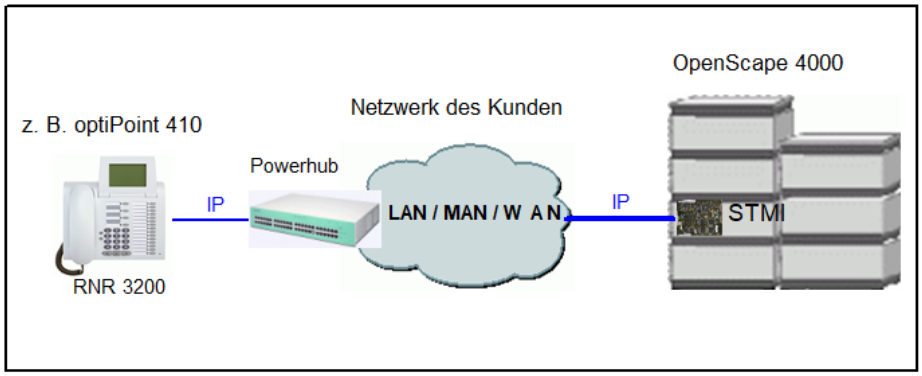
- **PBX Address**
- **Subscriber Number**

21.8.1 HFA (IP) Endgerät an STMI

Wichtig: Für OpenStage 60/80, OpenScape Desk Phone CP600 und OpenScape Desk Phone IP 55. D.h. dass die Werte, die mit AMO ACTDA/AMO KCSU konfiguriert wurden, nicht ausgewertet werden.



HFA (IP) Endgerät mit Steckernetzteil



HFA (IP) Endgerät mit Powerhub Stromversorgung

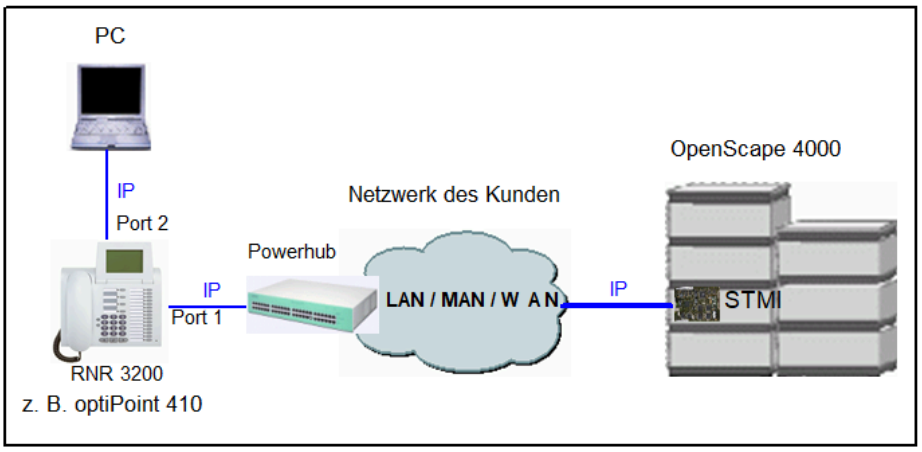
Sie richten ein HFA (IP) Telefon an STMI wie folgt ein:

1) `EINR-SBCSU:TLNNU=<number>,ART=OPTI,`**`ANSCHL=IP2`**`,LAGE=<ltg-ltu-ebt-satz>,`
`GERKON=OPTIIP``,COS1=<number>,COS2=<number>,`**`LCOSS1`**`=<number>,`

`LCOSS2=<number>,LCOSD1=<number>,LCOSD2=<number>,VBZ=<number>,`
`WABE=0,SNU=<number>,`**`[IPPASSW=<Passwort>],KOPFSG=MITIND`**`;`

Wichtig: Für OpenStage und Desk Phone IP: **KOPFSG=MITIND** muss konfiguriert sein damit die richtige Meldung im Display erscheint, wenn die Kopfsprechgarniturtaste gedrückt wird, obwohl keine Kopfsprechgarnitur angeschlossen ist.

21.8.2 PC hinter HFA (IP) Endgerät



PC und HFA Endgerät mit „single wire to the desk“

Sie richten ein HFA Endgerät an STMI wie folgt ein:

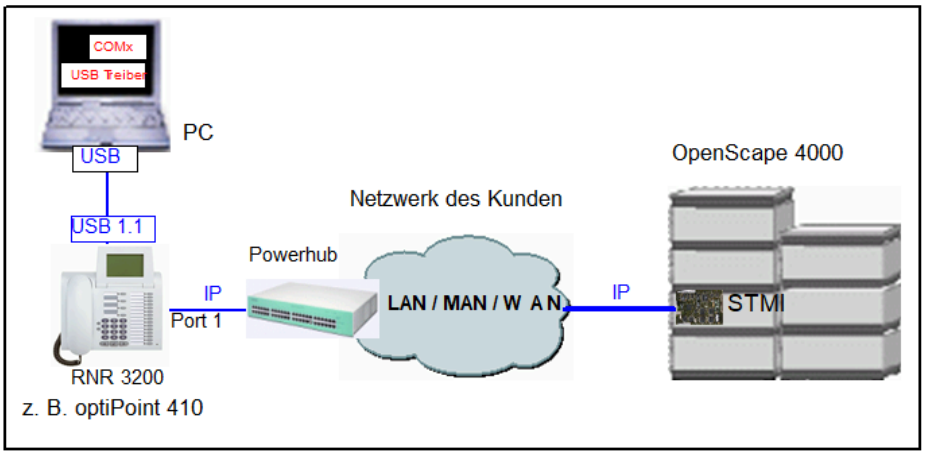
1) `EINR-SBCSU:TLNNU=<number>,` **`ART=OPTI,ANSCHL=IP2,`** `LAGE=<ltg-ltu-ebt-satz>,` **`GERKON=OPTIIP,`** `COS1=<number>,COS2=<number>,LCOSS1=<number>,LCOSS2=<number>,LCOSD1=<number>,LCOSD2=<number>,VBZ=<number>,WABE=0,SNU=<number>,` **`[IPPASSW=<Passwort>]`**

Wichtig: Für OpenStage und Desk Phone IP: KOPFSG=MITIND muss konfiguriert sein damit die richtige Meldung im Display erscheint, wenn die Kopfsprechgarniturtaste gedrückt wird, obwohl keine Kopfsprechgarnitur angeschlossen ist.

Für den PC ist keine spezielle OpenScape 4000-Konfiguration erforderlich, sondern Sie müssen lediglich die Port-Einstellungen am Telefon mit denen auf der PC-Netzwerkkarte abstimmen.

Wichtig: Anschaltung eines PC ohne 802.1p/q an ein optiPoint 410, an dem 802.1p/q aktiviert ist, ist nicht möglich. Die 802.1p/q Einstellungen sind am Telefon und im AMO zu tätigen, sowie den LAN Komponenten.

21.8.3 HFA (IP) Endgerät und USB für Simple Dialer



HFA-Endgerät und USB für Simple Dialer

Sie richten ein HFA (IP) Telefon an STMI wie folgt ein:

1) `EINR-SBCSU:TLNNU=<number>,ART=OPTI,`**`ANSCHL=IP2`**`,LAGE=<ltg-ltu-ebt-satz>,`
`GERKON=OPTIIP``,COS1=<number>,`**`COS2=<number>`**`,LCOSS1=<number>,`
`LCOSS2=<number>,LCOSD1=<number>,LCOSD2=<number>,VBZ=<number>,`
`WABE=0,SNU=<number>,`**`[IPPASSW=<Passwort>]`**

> **Wichtig: Für OpenStage und Desk Phone IP: KOPFSG=MITIND** muss konfiguriert sein damit die richtige Meldung im Display erscheint, wenn die Kopfsprechgarniturtaste gedrückt wird, obwohl keine Kopfsprechgarnitur angeschlossen ist.

Es sind keine weiteren Konfigurationsschritte nötig.

21.8.4 OpenStage WL3/WL4-Konfiguration

Gerätekonfiguration

OpenStage WL3/WL4 müssen als UFIP-SIP-Geräte konfiguriert sein:

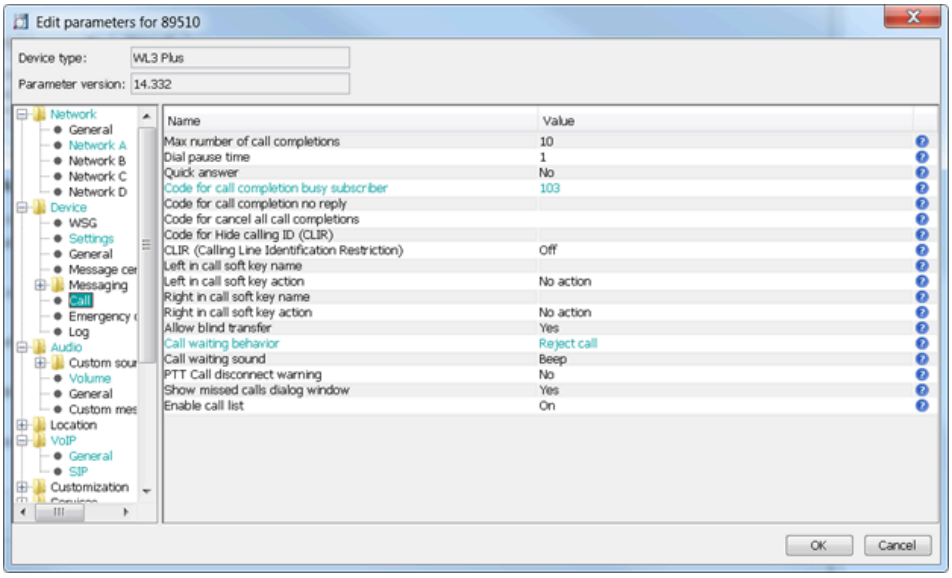
```
ADD-SBCSU:STNO=44511,OPT=OPTI,CONN=IP2,PEN=1-99-5-6,DVCFIG=UFIP,
TSI=1,COS1=310,COS2=310,LCOSV1=1,LCOSV2=1,LCOSD1=1,LCOSD2=1,DPLN=0,ITR=0,
SSTNO=N,COSX=0,SPDI=0,IDCR=N,STD=0,INS=Y,ALARMNO=0,RCBKB=N,RCBKNA=N,
CBKBMAX=5,HEADSET=N,HSKEY=NORMAL,CBKNAMB=Y,TEXTSEL=ENGLISH,HMUSIC=0,COMGRP=0;
```

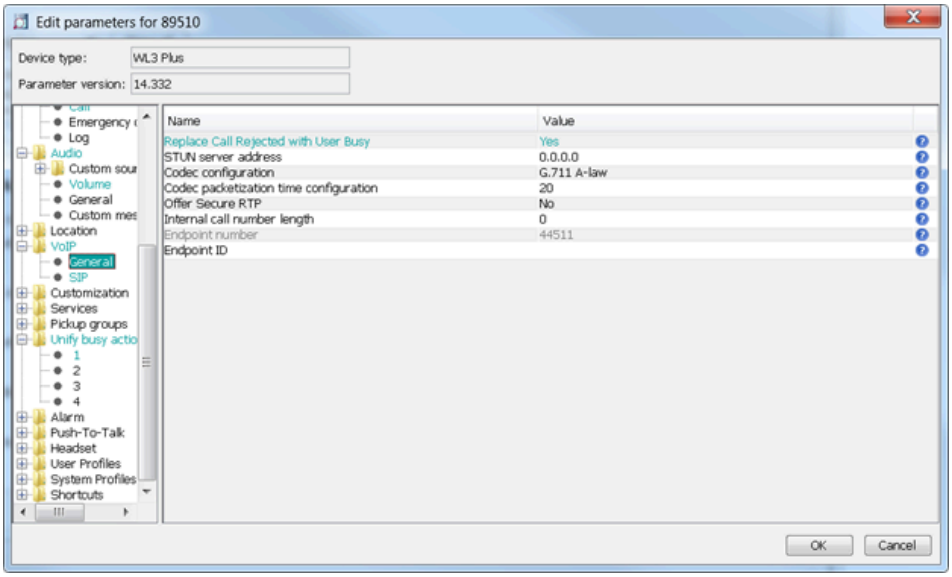
CHANGE-SDAT:STNO=44510,TYPE=ATTRIBUT,AATTR=MBCHL;

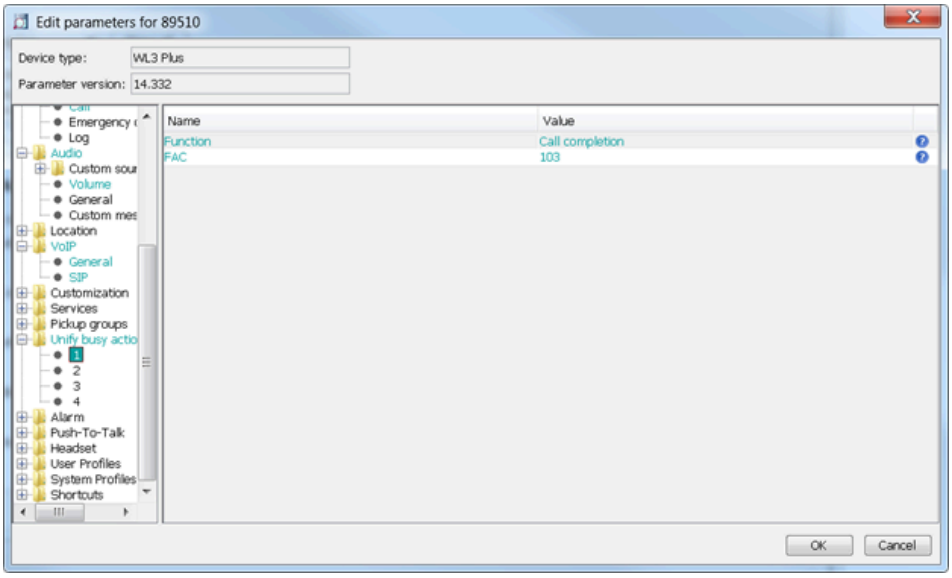
> **NOTICE:** WL3/WL4 Central Speed Dialing für OpenScape4000 wird unterstützt.

Damit Sie das Leistungsmerkmal „Rückruf bei Besetzt“ mit dem WL3/WL4 nutzen können, überprüfen Sie, ob für WABE eine vorhandene CBKKY DAR konfiguriert wurde. Falls nicht, können Sie es folgendermaßen hinzufügen:
`ADD-WABE:CD=103,DAR=CBKKY,CHECK=N;`

Dieser WABE-Leistungsmerkmal-Zugriffscode muss für WL3/WL4-Stationen über bekannte Methoden konfiguriert werden (siehe WL3/WL4-Dokumentation). Nachfolgend finden Sie WL3-Screenshots als Beispiel:







21.8.5 OpenStage Konfiguration

Ein OpenStage HFA-Terminal wird konfiguriert wie in Abschnitt 8.1, "HFA (IP)-Terminal am STMI".

Tastenbelegung

Ein standardmäßiges Tastenlayout wird in AMO TAPRO in jedem Fall für OS15/OS20/OS40/OS60/OS80 HFA vordefiniert.

Table 91: Standardmäßiges Tastenlayout für OS15/OS20/OS40/OS60/OS80 HFA

OpenStage	Tastenlayout (STD in AMO TAPRO)
OpenStage 15	60
OpenStage 20	55
OpenStage 40	56
OpenStage 60	57
OpenStage 80	58

Beispiele für Tastenstandards bei den verschiedenen OpenStage Varianten

```
DIS-TAPRO:TYPE=STD,STD=55&56&57&58&60;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                   |
+-----+---------+-------------------------------------------------------------+
|  55 | OPENST20| "OPENSTAGE - OS20                                    "      |
|     |         |  1 SPKR-FIX  2 FIX       3 MUTE-FIX   4 SNR-FIX   5 FWD-FIX  |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX                           |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT  |
```

```
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT    5 VACANT   |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT   10 VACANT   |
|     |         | 11 VACANT   12 VACANT                                          |
+-----+---------+----------------------------------------------------------------+
|  56 | OPENST40| "OPENSTAGE - OS40                                        "     |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 SNR-FIX    5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT               |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT   17 VACANT   18 VACANT                           |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
+-----+---------+----------------------------------------------------------------+
|  57 | OPENST60| "OPENSTAGE - OS60                                        "     |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 FIX        5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
```

```
|     |         | 11 VACANT   12 VACANT                                          |
+-----+---------+----------------------------------------------------------------+
|  58 | OPENST80| "OPENSTAGE - OS80                                        "     |
|     |         |  1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX   4 FIX        5 FWD-FIX |
|     |         |  6 RLS-FIX   7 CH-FIX    8 MB-FIX     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT   17 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                          |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT    2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT    7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT   12 VACANT                                          |
+-----+---------+----------------------------------------------------------------+
|  60 | OPENST15| "OPENSTAGE 15                                             "    |
|     |         |  1 SPKR-FIX   2 FIX       3 FIX        4 FIX        5 FIX     |
|     |         |  6 FIX        7 CH-FIX    8 MB-FIX     9 NAME      10 NAME    |
|     |         | 11 NAME      12 VACANT   13 VACANT    14 VACANT    15 VACANT  |
|     |         | 16 VACANT                                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |  1 LINE       2 LINE      3 LINE       4 LINE       5 LINE    |
|     |         |  6 LINE       7 LINE      8 LINE       9 LINE      10 LINE    |
|     |         | 11 LINE      12 LINE     13 LINE      14 LINE      15 LINE    |
|     |         | 16 LINE      17 LINE     18 LINE                             |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT    12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT    12 VACANT                                         |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |  1 VACANT     2 VACANT    3 VACANT     4 VACANT     5 VACANT  |
|     |         |  6 VACANT     7 VACANT    8 VACANT     9 VACANT    10 VACANT  |
|     |         | 11 VACANT    12 VACANT                                         |
+-----+---------+----------------------------------------------------------------+
```

SHIFT Taste

Bei OpenStage-Endgeräten kann auch am Endgerät eine UMSCHALTTASTE konfiguriert werden (bisher war dies nur auf den Beistellgeräten möglich). Dies geschieht mit dem AMO TAPRO oder über das Service-Menü am Endgerät selber.

AENDERN-TAPRO:TLNNU=<teilnehmernummer>,TDxx=SHIFT;

IMPORTANT: xx mus größer als 08 sein, da die ersten 8 Tasten fest definiert sind. Erst ab der 9. Taste kann man die Tasten beliebig belegen!

21.8.6 OpenScape Desk Phone IP Konfiguration

Ein OpenScape Desk Phone IP Endgerät wird wie im Abschnitt 8.1, „HFA (IP) Endgerät an STMI“ beschrieben eingerichtet.

Tastenbelegung

Für OpenScape Desk Phone IP 35 G/55G HFA sind jeweils ein Tastenstandard im AMO TAPRO vorgeleistet.

Tabelle 92: Tastenstandard für OpenScape Desk Phone IP 35 G/55G HFA

Desk Phone	Tastenstandard (SNU im AMO TAPRO)
OpenScape Desk Phone IP 35 G HFA	62
OpenScape Desk Phone IP 55 G HFA	63

Außerdem gibt es im AMO TAPRO für den Parameter DIGTYP die Werte **DPIP35** bzw. **DPIP55**.

- OpenScape Desk Phone IP 35 G HFA
- Das OpenScape Desk Phone IP 35 G HFA hat 3 frei programmierbare Tasten (9,10,11), die per Tastenstandard defaultmäßig mit den Funktionen **Trennen**, **Wahlwiederholung** und **Anrufliste** vorbelegt sind.
- OpenScape Desk Phone IP 55 G HFA
- Das OpenScape Desk Phone IP 55 G HFA hat 8 frei programmierbare Tasten (9 - 16) mit elektronischer Tastenbeschriftung. Zusätzlich hat das Endgerät 4 Tasten unterhalb des Displays, sogenannte Softkeys, mit denen jeweils die Menüpunkte in der letzten Displayzeile ausgewählt werden können.

Wichtig: Die Tastenfunktionen der Softkeys, als auch die Tasten Phone, Call Log und Directory sind nur im Endgerät (lokal) belegt, und können daher über AMO weder administriert noch angefragt werden.

21.8.7 Desk Phones CP-Konfiguration

A CP100/ CP110/ CP200/ CP210/ CP400/ CP410/ CP600/ CP700/ CP700X/ CP710 HFA-Endgerät wird wie in Kapitel 8, “HFA (IP)-Endgerät bei STMI”beschrieben konfiguriert.

Tastenbelegung

Für CP100/CP110/ CP200/ CP210/ CP400/ CP410/ CP600/ CP700/CP710 HFA ist in AMO TAPRO jeweils eine Standard-Tastenbelegung vordefiniert.

Die CP410-Standardtastenbelegung sollte für OpenScape Desk Phone CP410 oder CP710 mit angeschlossenem KM410 (Tastenmodul mit 16 frei programmierbaren Funktionstasten) verwendet werden.

Die CP410-Standardtastenbelegung sollte für OpenScape Desk Phone CP700 oder CP710 mit angeschlossenem KM710 (Tastenmodul mit 12 frei programmierbaren Funktionstasten) verwendet werden.

Desk Phone CP	Tastenlayout (STD in AMO TAPRO)
OpenScape Desk Phone CP100	112
OpenScape Desk Phone CP200	109
OpenScape Desk Phone CP400	110
OpenScape Desk Phone CP600	111
OpenScape Desk Phone CP700/ CP710/CP410 (mit KM710)	113
OpenScape Desk Phone CP110	114
OpenScape Desk Phone CP410/ CP710 (mit KM410)	115

Beispielhafte Standard-Tastenbelegungen für die CP100-Variante:

```
<DISPLAY-TAPRO:TYPE=STD,STD=112;
DISPLAY-TAPRO:TYPE=STD,STD=112;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                   |
+-----+---------+-------------------------------------------------------------+
| 112 | CP100   |  "DESKPHONE CP100                                        "  |
|     |         |   1 SPKR-FIX  2 FIX       3 MUTE-FIX  4 FIX       5 FIX     |
|     |         |   6 FIX       7 CH-FIX    8 MB-FIX    9 VACANT   10 VACANT  |
|     |         |  11 VACANT                                                  |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT  |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT  |
|     |         |  11 VACANT   12 VACANT                                      |
+-----+---------+-------------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
```

```
DISPLAY COMPLETED;
```

Beispielhafte Standard-Tastenlayouts für die CP200-Variante:

```
 <DIS-TAPRO:STD,109;
DIS-TAPRO:STD,109;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                   |
+-----+---------+-------------------------------------------------------------+
| 109 | CP200   |  "DESKPHONE CP200                                          " |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 TRNS-FIX  5 HOLD-FIX |
|     |         |   6 CONF-FIX  7 CH-FIX    8 MB-FIX    9 CALLOG   10 VACANT   |
|     |         |  11 FWD      12 LNR                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                       |
+-----+---------+-------------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Beispiel für Standard-Tastenlayouts für CP400/CP600-Varianten:

```
 <DIS-TAPRO:TYPE=STD,STD=110&&111;
DIS-TAPRO:TYPE=STD,STD=110&&111;
H500:  AMO TAPRO STARTED
+-----+---------+-------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                   |
+-----+---------+-------------------------------------------------------------+
| 110 | CP400   |  "                                                         " |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 FIX       5 FIX      |
|     |         |   6 FIX       7 CH-FIX    8 FIX       9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FWD-FIX  20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX      25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT   30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
```

```
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                    |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                    |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                    |
+-----+---------+---------------------------------------------------------------+
| 111 | CP600   |  "                                                          "  |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 FIX       5 FIX      |
|     |         |   6 FIX       7 CH-FIX    8 FIX       9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FWD-FIX  20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX      25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT   30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                        |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT                                        |
+-----+---------+---------------------------------------------------------------+
AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Beispielhafte Standardtastenbelegungen für die CP700-Variante:

```
<DISPLAY-TAPRO:TYPE=STD,STD=113;
DISPLAY-TAPRO:TYPE=STD,STD=113;
H500:  AMO TAPRO STARTED
+-----+---------+---------------------------------------------------------------+
| STD | DIGTYP  | "SERVICE INFORMATION"          KEY LAYOUT                     |
+-----+---------+---------------------------------------------------------------+
| 113 | CP700   |  "DESKPHONE CP700                                           "  |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 TRANS-FIX  5 HOLD-FIX |
|     |         |   6 CONF-FIX  7 CH-FIX    8 MB-FIX    9 VACANT    10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT    15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FIX       20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX       25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT    30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                        |
```

```
|     + - - - - + - - - -
```

```
| 115 | CP410   |  "DESKPHONE CP410                                          "       |
|     |         |   1 SPKR-FIX  2 HS-FIX    3 MUTE-FIX  4 TRNS-FIX  5 HOLD-FIX |
|     |         |   6 CONF-FIX  7 CH-FIX    8 MB-FIX    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT   17 FIX      18 FIX      19 FWD-FIX  20 FIX      |
|     |         |  21 FIX      22 FIX      23 FIX      24 FIX      25 VACANT   |
|     |         |  26 VACANT   27 VACANT   28 VACANT   29 VACANT   30 VACANT   |
|     |         |  31 VACANT   32 VACANT                                       |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA1  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA2  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA3  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
|     + - - - - + - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
|     | OPTIA4  |   1 VACANT    2 VACANT    3 VACANT    4 VACANT    5 VACANT   |
|     |         |   6 VACANT    7 VACANT    8 VACANT    9 VACANT   10 VACANT   |
|     |         |  11 VACANT   12 VACANT   13 VACANT   14 VACANT   15 VACANT   |
|     |         |  16 VACANT                                                   |
+-----+---------+--------------------------------------------------------------+

AMO-TAPRO-111       PROGRAMMABLE KEY DEFINITION FOR DIGITAL TERMINALS
DISPLAY COMPLETED;
```

Die Werte CP100, CP110, CP200, CP400, CP410, CP600 und CP700 gelten auch in AMO TAPRO für den Parameter DIGTYP.

- OpenScape Desk Phone CP100/CP110 HFA

  Das OpenScape Desk Phone CP100, CP110 verfügt über drei programmierbare Funktionstasten (9,10,11), die jederzeit mit anderen Funktionen oder Telefonnummern umprogrammiert werden können.
- OpenScape Desk Phone CP200/ CP210 HFA

  Das OpenScape Desk Phone CP200, CP210 HFA verfügt über vier frei programmierbare Tasten (9,10,11,12), die in der Standardtastenbelegung mit den Funktionen **Anrufprotokoll**, **Nicht belegt**, **Weiterleitungstaste** und **Wahlwiederholung der letzten Nummer**.
- OpenScape Desk Phone CP400

  Das OpenScape Desk Phone C400 HFA hat 16 frei programmierbare Tasten (9 - 16 und 25 - 32). Zusätzlich hat das Endgerät vier Tasten auf der rechten Seite des Displays, sogenannte Softkeys, mit denen jeweils die Menüpunkte in der letzten Displayzeile ausgewählt werden können.
- OpenScape Desk Phone CP600/ CP410

  Das OpenScape Desk Phone C600, CP410 HFA hat sechzehn frei programmierbare Tasten (9 - 16 und 25 - 32) mit elektronischer Tastenbeschriftung. Zusätzlich enthält das Endgerät fünf Tasten auf der

rechten Seite des Displays, sogenannte Softkeys, mit denen jeweils die Menüpunkte in der letzten Displayzeile ausgewählt werden können.

- OpenScape Desk Phone CP700/ CP710

  Das OpenScape Desk Phone C700, CP710 HFA verfügt über sechzehn frei programmierbare Tasten (9 - 16 und 25 - 32) mit elektronischer Tastenbeschriftung.

  Darüber hinaus verfügt das Endgerät über 12 frei programmierbare Tasten mit LED, die sogenannten Softkeys. Die ersten 6 programmierbaren Tasten werden permanent auf dem linken Bedienfeld angezeigt. Die letzten 6 programmierbaren Tasten sind in den Favoriten verfügbar.

  IMPORTANT: Die Tastenfunktionen der Softkeys sind nur im Endgerät (lokal) belegt, und können daher über AMO weder administriert noch angefragt werden.

  NOTICE: Das OpenScape Desk Phone CP700/CP700X enthält die REDIAL KEY, die über das WBM konfiguriert werden kann.

Schlüsselwerte

Es folgen die logischen Schlüsselwerte für Schlüsselmodule.

	HAUPTGERÄT	DSS1	DSS2	DSS3	DSS4
Ebene 1	1 - 32	33-48	49-64	65-80	81-96
Ebene 2	180-211	97-112	113-128	129-144	145-160

NOTICE: Auch wenn das AMO für 4 zusätzliche Schlüsselmodule vorbereitet ist, unterstützt nur das CP600-Telefon 4 Add-ons. Das CP400-Telefon unterstützt 2 Add-ons.

Die CP410- und CP710-Telefone unterstützen 4 Tastenmodule (KM410 oder KM710).

21.9 Löschen am IP-Anschluss

21.9.1 Alle Geräte einer Rufnummer am IP-Anschluss löschen

Alle Endgeräte, die einer Rufnummer zugeordnet sind, löschen sie wie folgt (der optionale AUSART Parameter mit seinem Standardwert MV=„Ausschalten mit Vorsperre“ übernimmt dabei das sonst per AMO DSSU erforderliche vorherige Sperren der Endgeräte):

```
LOESCHEN-SBCSU:TLNNU=number,DIENST=ALLE[,AUSART=OV];
```

Wichtig: Sie dürfen das Endgerät mit der Hauptrufnummer erst dann löschen, wenn keine Geräte unter einer Nebenrufnummer mehr eingerichtet sind.

21.9.2 Non-Voice-Dienste am IP-Anschluss löschen

Einzelne NV-Dienste am IP-Anschluss löschen sie wie folgt (der optionale AUSART Parameter mit den Werten MV=„Ausschalten mit Vorsperre“ und OV=„Ausschalten ohne Vorsperre“ übernimmt dabei das sonst per AMO DSSU erforderliche vorherige Ausschalten aller Endgeräte und das anschliessende Wieder-Einschalten der noch verbliebenen Endgeräte):

```
LOESCHEN-SBCSU:TLNNU=number,DIENST=param [,AUSART=OV];
```

Wichtig: Wenn Sie beim Löschen des einen NV-Dienstes mit AUSART=KS (Keine Sperre) gearbeitet haben, dann müssen Sie anschließend die restlichen Endgeräte per DSSU wieder in Betrieb nehmen (insbesondere das Sprachendgerät, da Sie dieses ja nicht gelöscht haben).

21.9.3 Beistellgerät des IP-Endgerätes löschen

Sie löschen alle Beistellgeräte, die einem Telefon zugeordnet sind folgendermaßen:

```
AENDERN-SBCSU:TLNNU=number,ART=OPTI,BEIGER=0;
```

21.9.4 Busy Lamp Field am IP-Endgerät löschen

```
AENDERN-SBCSU:TLNNU=number,ART=OPTI,BLF=NEIN;
```

21.9.5 Adapter des IP-Endgerätes löschen

Wichtig: Dieser Abschnitt gilt nur für optiPoint- und optiClient-Endgeräte!

- Sie können den optipoint USB adapter nicht durch ein AMO Kommando löschen, er wird beim Löschen des letzten (funktionalen) S0-Gerätes am IP Anschluss automatisch mit gelöscht.

Glossar

A

Anrufübergabe nach Melden

A ist der Initiator der Anrufübergabe. A ist in einem Gespräch mit B und setzt B auf Halten. Dann baut A ein Rückfragegespräch zu C auf und leitet die Übergabe ein. Nach der Übergabe sind B und C verbunden.

B

Anrufübergabe ohne Melden

A ist der Initiator der Anrufübergabe. A ist in einem Gespräch mit B. A setzt B auf Halten. Dann baut A ein Rückfragegespräch zu C auf und übergibt den Anruf, bevor das Rückfragegespräch verbunden wird. Nach der Übergabe sind B und C verbunden.

C

CLIP

CLIP – Calling Line Identification Presentation (Rufnummernerkennung) – Die Nummer des Anrufers wird beim Angerufenen angezeigt.

CLIR

CLIR– Calling Line Identification Restriction Rufnummernunterdrückung) – Die Nummer des Anrufers wird beim Angerufenen angezeigt.

CNIP

CNIP – Calling Name Identification Presentation (Anrufernamenerkennung) – Der Name des Anrufers wird beim Angerufenen angezeigt.

CNIR

CNIR – Calling Name Identification Presentation (Anrufernamenunterdrückung) – Der Name des Anrufers wird beim Angerufenen nicht angezeigt.

CNOP

CNOP – Connected Name Identification Presentation (Namenserkennung des Angerufenen) – Der Name des Angerufenen wird beim Anrufer angezeigt.

CNOR

CNOR – Connected Name Identification Restriction (Namensunterdrückung des Angerufenen) – Der Name des Angerufenen wird beim Anrufer nicht angezeigt.

COLP

COLP – Connected Line Identification Presentation (Rufnummernerkennung des Angerufenen) – Die Nummer des Angerufenen wird beim Anrufer angezeigt.

COLR

COLR – Connected Line Identification Restriction (Rufnummernunterdrückung des Angerufenen) – Die Nummer des Angerufenen wird beim Anrufer nicht angezeigt.

CSTA/ACL-Monitoring

Das CSTA/ACL-Monitoring liefert den Gerätestatus von SIP-Teilnehmern für BLF WIN-Anwendungen (Belegtlampenfeld) oder andere präsenzbasierte Anwendungen.

D

DMZ

Der Name leitet sich von dem Begriff „entmilitarisierte Zone“ ab, einem Gebiet zwischen Nationalstaaten, in dem militärische Aktionen nicht erlaubt sind.

In der Computersicherheit ist eine DMZ (manchmal auch als Perimeter-Netzwerk bezeichnet) ein physisches oder logisches Subnetz, das die externen Dienste einer Organisation enthält und einem größeren, nicht vertrauenswürdigen Netzwerk, in der Regel dem Internet, aussetzt. Der Zweck einer DMZ ist es, dem lokalen Netzwerk (LAN) einer Organisation eine zusätzliche Sicherheitsebene hinzuzufügen. Ein externer Angreifer hat nur Zugriff auf Geräte in der DMZ und nicht auf andere Teile des Netzwerks.

I

Inbound-Proxy:

Servername/IP-Adresse des Trunking-Partners, von dem die Daten an das OpenScape 4000 gesendet werden.

IP-Hop

Ein IP-Hop bedeutet einmaliges Kodieren und Dekodieren.

M

MediaRelay

MediaRelay ist ein Media-Proxy des Media-Servers im OpenScape 4000 SoftGate, der über die Signalisierungssoftware des HG 3500 gesteuert wird.

O

Outbound-Proxy

Servername/IP-Adresse, an die alle ausgehenden Nachrichten/Daten als erster Knoten/Hop gesendet werden (z. B. Session Boarder Controller).

P

Proxy

Servername/IP-Adresse des Servers des Partners, an den die Anrufe weitergeleitet werden.

T

T.38

T.38 ist ein ITU-Standard für den Versand von Faxnachrichten über IP-Netzwerke in Echtzeit.

Abkürzungen

ACC	Access Point Connection Control
AP	Access Point
APE	Access Point Emergency
BRI	Basic Rate Interface (ISDN S0)
CGW	Common Gateway, z.B. HG 3500
CLA	Customer License Agent
CLM	Customer License Manager
CO	CentralOffice (Deutsche Telekom)
DLS	Deployment and License Server
DMC	Direct Media Connection (VoIP)
E2E	End-to-End
ERH	Endpoint Registration Handler
HFA	HiPath Feature Access
HSR	HiPath Signaling Router
HW	Hardware
ICMP	Internet Control Message Protocol
IMP	IPDA Media Proxy
IPDA	IP Distributed Architecture
ISDN	Integrated Services Digital Network
JRE	Java Runtime Environment
LS	Local Survivability
LW	Loadware
MEK	Master Encryption Key
MXGW	Mediatrix Gateway
MTU	Maximum Transmission Unit (maximale Übertragungsrate)
NAT	Network Address Translation
PBX	Private Branch Exchange
PEP	Proprietary Encryption Protocol (für IPDA-Signalisierung)
PSTN	Public Switching TDM Network

PXE	Preboot eXecution Environment
QDC	Quality of Service Data Collection
QoS	Quality of Service
SBC	Session Border Controller
SIP	Session Initiation Protocol
SPE	Signaling and Payload Encryption
SRSR	Small Remote Side Redundancy
SRTP	Secure Real Time Protocol
SSA	SIP Stack Adaptor
TLS	Transport Layer Security
VoIP	Voice over IP
WBM	Web Based Management

Index

A

Access Point 592, 595, 598, 717
Access Point Emergency 750
Adapter des IP-Endgerätes löschen 1337
Aktivierung des Leistungsmerkmals SPE 1192
Alle Geräte einer Rufnummer am IP-Anschluss löschen 1336
Allgemeines 454
Anlagenkapazität 536
Ansagen pro Access Point 546, 688
AP Emergency 750
- Access Points einrichten 769
- Access Points entfernen 773
- Administrative Umschaltung von Access Points 779
- Administrative Umschaltung von OpenScape 4000 SoftGates 779
- AP Emergency-Konfiguration verifizieren 784
- Arbeitsblätter-Konfiguration 794
- CC-AP löschen 763
- Display-Anzeige am Endgerät 774
- Emergency Gruppe ändern 764
- Emergency Gruppe einrichten 764
- Emergency Gruppe löschen 769
- FAQ - Häufig gestellte Fragen 813
- Hinweise für Netzwerkadministratoren 796
- Inbetriebnahme
  - CC-AP 783
  - Survivable OpenScape 4000 SoftGate 784
- Konfiguration 760
- Konfiguration von Backup & Restore am CC-AP 790
- Konfigurationsdaten 757
- Kurzanleitung 798
- Leistungsmerkmalbeschreibung 750
- Lizenzierung 759
- Löschen der gesamten Konfiguration 774
- Netzwerkadministratoren 796
- Normalbetrieb 756
- OpenScape 4000 Assistant Backup & Restore 784
- OpenScape 4000 im Kunden-LAN 760
- OpenScape 4000 SoftGate konfigurieren 769
- Rückschaltung in Normalbetrieb 756
- Software Update 758, 758, 758
- Survivability Unit am OpenScape 4000 SoftGate 754
- Survivability Unit im AP 3700 IP 754
- Szenarien 750
- Übernahme der AP-Notfallkonfiguration 784
- Umschalteverzögerung 775
- Umschaltung in den Emergency-Betrieb 755
- Unterstützung von Applikationen im Emergency-Betrieb 760
- Verbindung zwischen den Teilsystemen (Inseln) 758
- Verbindungsdaten 777
- Zeitsynchronisation 536, 759
- Zeitsynchronisation zwischen Host System und CC-AP 783
- Zeitsynchronisation zwischen Host System und Survivable OpenScape 4000 SoftGate 783
- Zuordnung von Access Points zur Survivability Unit 755

APE 750
Arbeitsblätter - IPDA-Konfiguration 724
Architektur 39

B

Bandbreitenbedarf 47
Bandbreitenbedarf pro Verbindung 48
Baugruppen 1309
Beistellgerät des IP-Endgerätes löschen 1337
Benutzeroberfläche bei Mobility-Sitzung 517

C

CLI HG 3500 200
CLI HG3500
- Zugriffskontrolle 201

CMI 678
Codec-Einstellungen 144
Codec-Standards 28
Codierung 47
Command Line Interface CLI in HG 3500 200

D

Daten-Verbindungen (Mediatrix 44xx) 316
Dienste 276
Different Time Zones (DTZ) 816
DMC
- HFA-Teilnehmer an OpenScape 4000 1282
- HFA-Telefon an einer anderen OpenScape 4000 1282
- HFA-Telefon an HiPath 3000 1284
- SIP-Teilnehmer an OpenScape 4000 1279
- SIP-Telefon an einer anderen OpenScape 4000 1279, 1280
- SIP-Telefon an HiPath 3000 1281
- TDM-Telefon an einer anderen OpenScape 4000 die über H323A Trunking angebunden ist 1286
- TDM-Telefon an einer anderen OpenScape 4000 (abgesetztes Shelf) 1285, 1285
- TDM-Telefon an HiPath 3000 1288

Durchschaltung 536
Durchschnitts-Delay für Daten (ms) (Parameter) 38
Durchschnitts-Delay für Sprache (ms) (Parameter) 37

E

Einrichtung von IPDA 547
Externe Music-On-Hold 674

F

FAQ - Häufig gestellte Fragen 741
Fax-Übertragung und -Erkennung 27
Fax/Modem over IP 27
FMoIP 27

G

Gatekeeper Einschränkungen 455
Gatekeeper Funktionalität 454
Gateways HG 3500 und HG 3575 24
Generierung IP-Endgeräte 1322

H

H323-/H323-Annex-Connectivity 1141
H323-Connectivity
    Überblick 1141
Hardware 295
HG 3500 24
    Baugruppentausch 57
HG 3575 24, 598
HG3500
    DLS-Client-Bootstrapping 99
    Ladekonzept 69
Hinweise für Netzwerkadministratoren 733
Hinweise zum 19" Access Point AP 3700 IP 603
HiPath Feature Access (HFA) 490

I

IP Distributed Architecture (IPDA) 534
IP-Adressänderungen 678
IP-Endgeräte 1309
IP-Overhead 48
IP-Ports 276
IP-Trunk-Konfiguration für SPE 1180
IPDA 534, 1194
IPDA unterschiedliche Zeitzonen
    Leistungsmerkmalbeschreibung 1101
IPDA-Verschiedene Zeitzonen
    Ändern von System-Zeit/Datum mit AMO DATE 825
    Generierungsbeispiel 817
    Leistungsmerkmalbeschreibung 816
    Löschen einer Zeitklasse 823
    Relevante AMOs 826
    Service Information 817
    Sommerzeitumschaltung löschen 825
    Zeitklassen einrichten 819
    Zuweisen der Zeitklassen zu einem AP-Shelf 822
    Zuweisen der Zeitklassen zu einem HFA-Teilnehmer 822
ISDN-S0-Daten (Mediatrix 44xx) 316

J

Jitter-Buffer-Typ (Parameter) 37

K

Konfiguration am IP-Endgerät 1189
Konfiguration der Signalisierungs- und Sprachverschlüsselung / SPE 1175

L

Laden neuer Loadware auf eine HG 3575 598
Large Enterprise Gatekeeper (LEGK) 454
Lastkalkulation 698
Laufzeit und dadurch bemerkbare Effekte 38
LEGK 454
Leistungsmerkmalbeschreibung 1155
Leistungsmerkmalbeschreibung Mobility-Sitzung 513
Leistungsmerkmale 63
Leitfaden für eine Installation eines IP-Features 455
Linkstatus-Abfrage 978, 1150
Load Balancing 390
Lokale Administration des Access Points am CLI mittels Terminal 717
Lokale Konfiguration eines Access Point 595
Löschen am IP-Anschluss 1336

M

Master Encryption Key 1195
Maximales Delay für Daten (ms) (Parameter) 38
Maximales Delay für Sprache (ms) (Parameter) 37, 37
Mediatrix 1204 Gateway 339
Mediatrix 41xx Gateway 332
Mediatrix 44xx Gateway (Daten) 316
Mediatrix 44xx Gateway (Sprache) 300, 307
Mediatrix Gateways - Hinweise zur Konfiguration 299
MEK 1195
MFV-Wähltonempfänger pro Access Point 546, 688
Microsoft Lync Communication Server
    Interworking 1046
Mobile HFA Logon 513
Modem-Übertragung und -Erkennung 27
Module bei optiPoint-Endgeräten 1312
MOH 355
Music on Hold 355
Music-On-Hold 674
MVF-Außerband-Signalisierung 1141

N

Nationale Zeichensätze für Textanzeigen pro Access Point 546
Native SIP
    Codecs 901
    Relevante AMOs 978, 1150

Netzwerk-Anforderungen 39
Netzwerkadministratoren 733
Notrufe von mehreren Standorten 967
NV-Dienste am IP-Anschluss löschen 1337

O

OpenScape 4000 Assistant
Common Gateway HG 3500 konfigurieren 981
IPGW löschen 983, 1153
IPGW-Baugruppendaten ändern 984, 1154
OpenScape 4000 SoftGate 289
OpenStage IP-Endgeräte 1317
optiPoint Acoustic Adapter spezifische Daten 1315
optiPoint Recorder Adapter spezifische Daten 1314
optiPoint-IP-Endgeräte 1309

P

Paket-Verlust / Delay-Präferenz (Parameter) 38
Parameter eines Access Points ändern 592
Payload - Aktivierung von Leistungsmerkmalen bei aktiver DMC 1270
Payload - DMC-Berechtigung 1271
Payload - Domänen 1272
Payload - Generierung 1271
Payload - H.323 Stack bei IPDA-Baugruppen 1272
Payload - Leistungsmerkmalbeschreibung 1260, 1260
Payload - Leistungsmerkmale mit DMC 1270
Payload - Maximale Anzahl von DMC-Verbindungen bei IP-Baugruppen 1271
Payload - Relevant AMOs 1274
Payload - Service-Informationen 1269
Payload - Sprachpausenerkennung (Voice Activity Detection
VAD) 1271
Payload Survivability 645
Display-Probleme auf VNR-Systemen 659
Protokoll 276

R

Referenztakt im Access Point 598
Ressourcenverwaltung 67
Rufszenarien 537

S

Samplingzeit 47
Schlüsselbegriffe 24
Security 67
Serviceinformation 1322
Serviceinformationen zu Mobility-Sitzungen 520
Signaling and Payload Separation 542
Signaling Survivability 829
Signalisierungs- und Sprachverschlüsselung (SPE) 1155
SIP-Carrier 926
SIP-Connectivity
DMC-Szenarien 1278
SIP-Konnektivität
SIP-Teilnehmer-Kommunikationsmatrix 865
SIP-Trunking Kommunikationsmatrix 865
Übersicht 865
Verwendete Baugruppen 870
SIP-Q
Trunking zwischen OpenScape 4000 und OpenScape Voice mit SIP-Q V2 985
SIP-Service-Provider 926
SIP-Teilnehmer
ändern 881
Anzeige 887
entfernen 881
konfigurieren 880
nicht registrierte SIP-Teilnehmer 887
Registrierte SIP-Teilnehmer 887
Relevante AMOs 890
SoftGate Upgrade 295
SPE: Konfiguration des externen Gateways 1180
Sprachen für Textanzeigen pro Access Point 546
Standard-Security Level 1177
STMI2/4-Baugruppenkonfiguration 880
Strombedarf 39
Systemanforderungen 39

T

Tastenlayout bei optiPoint-Endgeräten 1312
Teilnehmer-Gateway (Mediatrix 44xx) 320
Töne pro Access Point 546, 688
Trunking-Gateway (Mediatrix 44xx) 317

U

Überblick 289

V

Verkehrsbezogene Hinweise 55
Verschiedene Zeitzonen 816
Verschiedene Zeitzonen - Different Time Zones (DTZ) 546
Verteilung von Zertifikaten mit DLS 1212
Voraussetzungen 39, 1176

W

Web Based Management 1209

Z

Ziel dieses Dokumentes 23
Zugriff auf HiPath-Funktionen
Standby Board HG 3500 82

© 2025 Mitel Networks Corporation. Alle Rechte vorbehalten. Mitel und das Mitel-Logo sind Marken der Mitel Networks Corporation. Unify und damit verbundene Marken sind Marken der Unify Software and Solutions GmbH & Co. KG. Alle anderen hier genannten Marken sind Eigentum der jeweiligen Inhaber.