A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 V11

Gateways HG 3500 und HG 3575

06/2024

P31003-H31B0-M103-01-A9

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.

Inhalt

1 Einführung

Dieses Dokument beschreibt die Konfiguration der HG 3500/3575 Gateways und die dafür verfügbaren Werkzeuge.

Dieses Kapitel gibt einen Überblick über das Handbuch. Es beschreibt:

- die Zielgruppe für dieses Handbuch (siehe Section 2.1, "Zielgruppe")
- den Inhalt der einzelnen Handbuchkapitel (siehe Section 2.2, "Inhalt dieses Handbuchs")
- einen wichtigen Hinweis zu Internet Explorer (siehe Section 2.3, "Hinweis zu Internet Explorer")
- die verwendeten typografischen Konventionen (siehe Section 2.4, "Verwendete Konventionen")

1.1 Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die für die Einrichtung der HG 3500/3575 Gateways verantwortlich sind. Sie müssen bereits Erfahrung in der Administration von LANs haben und insbesondere über fundierte Kenntnisse in den folgenden Bereichen verfügen:

- Hardware für die Datenkommunikation
- Konzepte und Begriffe für Weitbereichsnetze (WAN)
- Konzepte und Begriffe für lokale Netze (LAN)
- Konzepte und Begriffe für das Internet

Sie sollten eine Einweisung in den folgenden Bereichen erhalten haben:

- Installation und Inbetriebnahme HG 3500/3575 Gateways
- Konfiguration der VoIP-Funktionen HG 3500/3575Gateways
- Einrichtung und kundengerechte Konfiguration der Datenkommunikationsparameter der HG 3500/3575 Gateways.

1.2 Inhalt dieses Handbuchs

Dieses Handbuch enthält eine vollständige Beschreibung der Verwaltungsmöglichkeiten für HG 3500/3575 Gateways und Hintergrundinformationen zu ausgewählten Themen.

Es erläutert die Verwaltung der HG 3500/3575 Gateways, nachdem sie in einem Baugruppenträger installiert wurden.

Die Ersteinrichtung muss zu Beginn der Verwaltung durchgeführt werden. Die vorbereitenden Verwaltungsschritte sind in Chapter 3, "Vorbereiten der Baugruppe" beschrieben.

Weitere Informationen zu HG 3500/3575 finden Sie im Servicehandbuch von OpenScape 4000 V10.

Die nachfolgenden Kapitel enthalten eine systematische Beschreibung der WBM-Benutzeroberfläche zur Konfiguration und Verwaltung der HG 3500/3575 Gateways.

1.3 Hinweis zu Internet Explorer

IMPORTANT: Wenn Sie Änderungen an den Sicherheitseinstellungen von Internet Explorer für eine WBM-Seite vorgenommen haben (z. B. durch Hinzufügen der zu den vertrauenswürdigen Websites), wird empfohlen, den Browser neu zu starten, damit die neuen Einstellungen korrekt verwendet werden.

1.4 Verwendete Konventionen

In diesem Handbuch werden die folgenden typographischen Konventionen verwendet:

Table 1: Typographische Konventionen

Konvention	Beispiel
`Courier`	Eingabe und Ausgabe Beispiel: Geben Sie als Dateinamen `LOKAL` ein. `Befehl nicht gefunden`
Kursivschrift	Variable Beispiel: *Name* kann bis zu acht Zeichen lang sein.
Kursivschrift	Weist auf Elemente der Benutzeroberfläche hin Beispiel: Klicken Sie auf *OK*. Wählen Sie im Menü *Datei* die Option *Beenden*.
Fett	Besondere Hervorhebung Beispiel: Beispiel: Dieser Name darf **nicht** gelöscht werden.
`<Courier>`	Tastenkombinationen Beispiel: `<STRG>+<ALT>+<ESC>`
>	Menüfolge Beispiel: Datei schließen **>**.
Verwendete Konventionen	Querverweis oder Hyperlink Zusätzliche Informationen

2 Vorbereiten der Baugruppe

Alle im WBM eingerichteten Konfigurationsdaten der Baugruppe müssen auf dem Backup-Server gesichert werden. Andernfalls würden bei einem Austausch der Baugruppe oder einer Aktualisierung der Loadware alle Konfigurationsdaten verloren gehen und die IP-Trunking-Verbindung könnte nicht mehr automatisch wiederhergestellt werden. Es muss sichergestellt sein, dass der Backup-Server erreichbar ist. Wenn der Backup-Server nicht erreichbar ist, werden die Konfigurationsdaten auch im Flash-Speicher der Baugruppe gesichert.

3 WBM

WBM steht für **W**eb **B**ased **M**anagement. Das WBM ist die Standard-Administrationsoberfläche der HG 3500/3575 Gateways.

Jeder PC mit TCP/IP-gestützter Netzwerkverbindung, auf dem ein kompatibler Web-Browser läuft, kann nach erfolgreicher Anmeldung am OpenScape 4000 Assistant auf die Bedienoberfläche des WBM zugreifen. Das WBM verfügt über einen integrierten Webserver, so dass das WBM über eine HTTPS-URL aufrufbar ist.

Sofern der Root-Administrator das WBM auf dem Gateway aktiviert hat, steht es über jede TCP/IP-Verbindung zur Verfügung, sowohl über das LAN als auch das WAN.

Die Benutzerschnittstelle des WBM steht nur auf Englisch zu Verfügung.

Hardware-Voraussetzungen:

Für den Betrieb des WBM benötigen Sie einen Standard PC oder Laptop mit einer Maus mit linker und rechter Maustaste.

Software-Voraussetzungen:

Das WBM besteht aus HTML/XSL-Seiten mit Frames. Sein Einsatz erfordert:

- Windows
- Microsoft Internet Explorer
- Im Microsoft Internet Konfiguration muss Folgendes eingestellt sein:
  - Aktivieren Sie die folgende Option: *Extras* > *Internetoptionen* > *Erweitert* > *Leeren des Ordners 'Temporary Internet Files' beim Schließen des Browsers*
  - Die Verbindung des Administrations-PC zum Gateway darf nicht über einen Proxyserver erfolgen. Die folgende Option sollte daher aktiviert werden: *Extras -> Internetoptionen -> Verbindungen -> LAN-Einstellungen: Einstellungen... -> Proxyserver: Umgehung des Proxyservers für die lokale Adresse*

  Andere Browser, die Frames und JavaScript unterstützen, sind möglicherweise ebenfalls mit dem WBM kompatibel. Browser, die keine Frames unterstützen, können nicht mit dem WBM verwendet werden.

Erstkonfiguration

Dieses Kapitel beschreibt die Erstkonfiguration des Gateways.

Vor Beginn der Konfiguration muss das Gateway entsprechend der Beschreibungen im Installationshandbuch installiert worden sein.

Die Grundkonfiguration des Gateways besteht aus vier Schritten:

1) Vorbereitende Arbeiten (siehe Section 4.1, "Vorbereitung der Konfiguration").
2) Das WBM aufrufen (siehe Section 4.2, "WBM starten und beenden").
3) Beenden der WBM-Sitzung.

Das WBM führt Sie Schritt für Schritt durch den Konfigurationsprozess. Nach Beendigung der Konfiguration kann die WBM-Sitzung beendet werden.

3.1 Vorbereitung der Konfiguration

Es ist empfehlenswert, die Konfiguration der HG 3500/3575 Gateways zu organisieren, bevor Sie damit beginnen, damit Sie sie ohne Unterbrechung durchführen können.

IMPORTANT: Stellen Sie sicher, dass dem Gateway die richtige IP-Adresse zugewiesen wurde, bevor Sie es mit dem Netzwerk verbinden.

3.2 WBM starten und beenden

Zugangsmöglichkeiten

Zum Starten des WBM für die HG 3500/3575 Gateways gibt es zwei Möglichkeiten. Zum einen über OpenScape 4000 Assistant, zum anderen direkt über einen Web-Browser und die URL des WBM. Der Zugang über OpenScape 4000 Assistant ist die am häufigsten benutzte Möglichkeit.

Themen in diesem Abschnitt

1) Section 4.2.1, "Über OpenScape 4000 Assistant starten" Section 4.2.2, "Über Web-Browser starten" Section 4.2.3, "WBM-Sitzung beenden"

3.2.1 Über OpenScape 4000 Assistant starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1) Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort am OpenScape 4000 Assistant an.
2) Wählen Sie in der Baumstruktur *OpenScape 4000 Assistant* **>** *Expertenmodus* **>** *Gateway-Dashboard*. Das Fenster *Gateway-Dashboard* mit den vorhandenen Baugruppen wird angezeigt:
3) Klicken Sie in der Zeile der gewünschten STMI-/NCUI-Baugruppe in der Spalte 'Remote-Zugang' auf *[WBM] [N/A]*. Der Webserver für die HG 3500/3575 Gateways wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.

NOTICE: Im Browser kann die Meldung erscheinen, dass ein Problem mit dem Sicherheitszertifikat der Website besteht. Klicken Sie in diesem Fall auf *Laden dieser Website fortsetzen*.

4) Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Die Startseite des WBMs wird angezeigt:
5) In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die HG 3500/3575 Gateways verwalten.

3.2.2 Über Web-Browser starten

Benutzerkonto

Für das WBM steht Ihnen die Benutzerkennung 'Administrator' zur Verfügung. Diese Kennung bietet Ihnen Zugang zu den Konfigurationseinstellungen.

Der Standard-Benutzername lautet **TRM** und das Standard-Kennwort **HICOM** (wie im AMO STMIB konfiguriert). Diese Standardeinstellungen sollten von Ihnen im AMO STMIB geändert werden.

WBM-Sitzung starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1) Öffnen Sie Ihren Web-Browser.
2) Geben Sie in die Adresszeile des Web-Browsers die URL des WBM ein. Der Webserver für die HG 3500/3575 Gateways wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.
3) Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Das Anmeldefenster der HG 3500/3575 Gateways wird angezeigt:
4) Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf *Anmelden*. Die Startseite des WBMs für HG 3500/3575 wird angezeigt:
5) In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die HG 3500/3575 Gateways verwalten.

3.2.3 WBM-Sitzung beenden

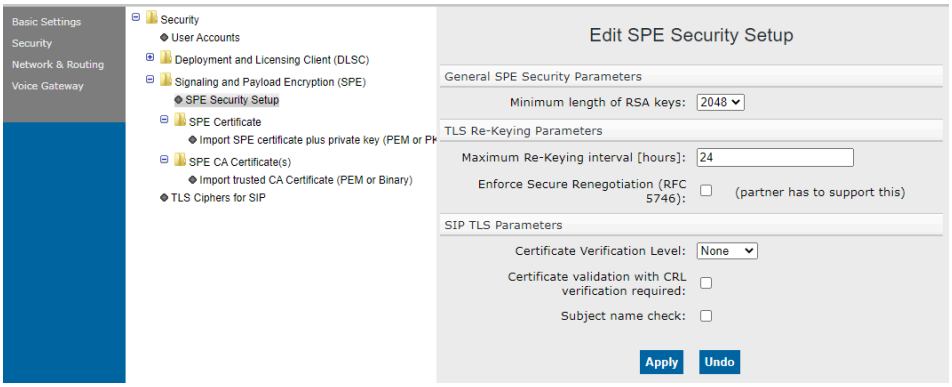
Führen Sie zum Beenden der WBM-Sitzung die folgenden Schritte durch:

Klicken Sie auf das Modul *Abmelden*. Die Verbindung zu den HG 3500/3575 Gateways wird beendet und die WBM-Sitzung wird geschlossen.

Erläuterungen zum Beenden der WBM-Sitzung finden Sie in Section 4.3.1.4, "Abmelden".

3.3 Anwendungsoberfläche des WBM

Das Hauptfenster des WBM besteht aus folgenden Bereichen:



Modulbereich:

Der Bereich unter dem Banner zeigt die Module an, die Ihnen zur Verfügung stehen. Sie wählen das gewünschte Modul, indem sie auf seinen Namen klicken. Siehe Section 4.3.1, "Module".

Menübereich:

Der Bereich am linken Rand wird für die Navigation innerhalb eines Moduls verwendet. Welche Menüs dort angezeigt werden, hängt vom gewählten Modul ab.

Schaltflächen- und Statusbereich:

Am unteren Rand finden Sie Symbole zur Steuerung des WBM sowie einige ständig angezeigte Statusinformationen. Zur Bedeutung der Symbole siehe Section 4.3.2, "Symbole im Steuerbereich des WBM-Fensters".

Auswahlbereich bei den Modulen *Wartung* und *Konfiguration*

In diesem Bereich wird eine Konfiguration-artige Baumstruktur angezeigt, die das Auswählen einzelner Funktionen erlaubt.

3.3.1 Module

Der Bereich unter dem Banner zeigt die Module an, die Ihnen zur Verfügung stehen. Sie wählen das gewünschte Modul, indem sie auf seinen Namen klicken.

Wenn ein Modul gewählt wird, wird sein Name *rot und kursiv* hervorgehoben, und im Menübereich werden modulspezifische Optionen angezeigt.

Angebotene Module:

1) *Konfiguration Wartung Hilfe Abmelden*

3.3.1.1 *Konfiguration*

Im Modul Konfiguration finden Sie alle Funktionen, die für die Konfiguration des Gateways erforderlich sind.

WBM-Pfad:

WBM **>** *Konfiguration*

Die Optionen des Moduls *Konfiguration* werden auf der linken Seite angezeigt.

Zur Detail-Beschreibung der Funktionen des Moduls 'Konfiguration' siehe Chapter 7, "Konfiguration".

3.3.1.2 Wartung

In diesem Modul finden Sie alle Funktionen, die für die Wartung und Administration des Gateways erforderlich sind.

WBM-Pfad:

WBM **>** *Wartung*

Links werden die Auswahlmöglichkeiten des Moduls *Wartung* angezeigt.

Zur Detail-Beschreibung der Funktionen des Moduls *Wartung* siehe Chapter 8, "Wartung".

3.3.1.3 Hilfe

WBM-Pfad:

WBM **>** *Hilfe* > *Produkt-Doku*

Es werden folgende Menüpunkte angezeigt:

- *Über das WBM*: Es werden der Titel des WBM, z. B. `Web-Based Management für HG 3575`, angezeigt.
- *Produkt-Doku*: Bei einem Klick auf *Produkt-Doku* werden Sie zur OpenScape 4000 Assistant V8-Anmeldeseite umgeleitet.

3.3.1.4 Abmelden

Nach Klicken auf *Abmelden* wird die Verbindung zum Gateway beendet und die WBM-Sitzung geschlossen. (siehe Section 4.3.2, "Symbole im Steuerbereich des WBM-Fensters").

WBM-Pfad:

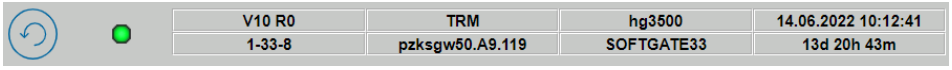
WBM **>** *Abmelden*

Automatisches Abmelden:

Wenn Sie den Browser einfach schließen und Sie zuvor Ihre Konfigurationsänderungen gesichert haben, werden Sie automatisch abgemeldet. Dann erscheint folgende Meldung: `Sie haben die WBM-Seite ohne Abmeldung verlassen. Sie werden automatisch aus der Telefonanlage ausgeloggt.`

3.3.2 Symbole im Steuerbereich des WBM-Fensters

Der Steuerbereich ist ein Applet, das ständig Steuer- und Statusinformationen bereitstellt. Die Abbildung unten zeigt ein Beispiel:



Es gibt folgende Steuersymbole:

Reset-Symbol (1)

Dieses Symbol löst einen Neustart des Gateways aus.

Blau Dateneingabe wird zurückgesetzt.

Aktivitäts-Symbol (2)

Das Symbol leuchtet grün, wenn eine Verbindung zum Webserver des Gateways besteht. Wenn keine Verbindung besteht, blinkt das Symbol rot.

Außerdem werden folgende Statusinformationen angezeigt:

- Systemversion der OpenScape 4000 und Aufstellungsort
- Zugangskategorie des Benutzers und Loadware-Version
- Boardname und Gateway-Standort
- Systemdatum und -uhrzeit sowie Zeit seit dem letzten Neustart

3.3.3 Symbole in den Baumdarstellungen des WBM

Die in den Modulen *Konfiguration* und *Wartung* verfügbaren Funktionen werden im Inhaltsbereich in einer Baumstruktur ähnlich der des Windows Explorers dargestellt. Diese Baumstruktur weist folgende Symbole auf:

- Verzeichnisse

	Jedes Verzeichnis, das ausgeblendete Funktionen enthält, ist durch ein Pluszeichen (+) gekennzeichnet. Durch einen Klick werden diese Funktionen eingeblendet. Die in diesem offenen Verzeichnis enthaltenen Funktionen sind dargestellt. Durch einen Klick werden diese Funktionen ausgeblendet.

- Listenpunkte

	Grau: Diese Funktion, kann aufgerufen werden, besitzt aber keine Statusanzeige. **Grün:** Diese Funktion ist aktiv und kann über eine Option im WBM abgeschaltet werden. **Rot:** Diese Funktion ist nicht aktiv und kann über eine Option im WBM eingeschaltet werden.

- Kontextmenüs
- Im WBM werden keine Kontextmenüs mehr angezeigt.

3.3.4 Dialoge und Dialogelemente

Eingaben und Änderungen im WBM werden im Browser-Fenster als grau hinterlegte Dialoge innerhalb des Browser-Fensters angezeigt. Ferner können separate Dialogfenster angezeigt werden, um z. B. einen Löschwunsch zu bestätigen.

In den Dialogen kommen folgende typische Dialogelemente vor:

Eingabefelder

	Eingaben von numerischen oder alphanumerischen Werten. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Bei Passwortfeldern werden zur Sicherheit nur einheitliche Symbole wie Sternchen für jedes eingegebene Zeichen angezeigt. Nicht auf der Tastatur verfügbare Zeichen können unter MS Windows z. B. über die Zeichentabelle 'Charmap' eingefügt werden.

Auswahlfelder

	Auf den Pfeil klicken, um die Liste zu öffnen oder zu schließen. Den gewünschten Eintrag mit der Maus anklicken.

Kontrollkästchen

	(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Option ein- oder auszuschalten.

Radio-Buttons

	(im nebenstehenden Bild links ausgeschaltet, rechts eingeschaltet): In einer zusammengehörigen Gruppe solcher Elemente ist stets eines eingeschaltet. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Funktion ein- oder auszuschalten.

Schaltflächen

	Bei Anklicken wird die Aktion ausgeführt, die als Text auf der Schaltfläche steht. Die Texte sind selbsterklärend wie z. B. *Rückgängig* oder *Übernehmen*.

Folgende Schaltflächen kommen vor:

- *Übernehmen*: Eingegebene Daten oder Änderungen werden im RAM zwischengespeichert und gegebenenfalls überprüft.
- *Rückgängig*: Im Dialog eingegebene Daten oder Änderungen werden verworfen. Der Anfangszustand des Dialogs wird wiederhergestellt.
- *Hinzufügen*: Einen neuen Eintrag in einer Tabelle hinzufügen.
- *OK*: Positive Quittung von separaten Dialogfenstern. Die gewünschte Aktion wird nach Anklicken (endgültig) ausgeführt.
- *Laden:* Es wird eine zuvor ausgewählte Datei, z. B. für Konfigurationsdaten, geladen.
- *Abbrechen* Negative Quittung von separaten Dialogfenstern. Die gewünschte Aktion wird nach Anklicken (doch) nicht ausgeführt.
- *Löschen*: Die konfigurierten Einstellungen werden gelöscht.
- *Zurück*: Zur vorherigen Bildschirmseite innerhalb eines mehrseitigen Dialogs wechseln. Kommt derzeit nur innerhalb eines Assistenten vor.

Sortierreihenfolge

In einer Tabelle kann durch Anklicken des Dreiecks neben der Überschrift in einem Tabellenkopf die Sortierreihenfolge in der darunterliegenden Spalte geändert werden, z. B. alphabetisch aufsteigend oder absteigend.

3.4 OpenScape 4000 Manager

Der OpenScape 4000 Manager ist ein Administrationswerkzeug zur Verwaltung der Datenbank einer OpenScape 4000 V10 und der OpenScape 4000 V10-Knoten. Dabei werden die relevanten Teile des OpenScape 4000 V10-Netzes wie ein virtuelles OpenScape 4000 V10-System dargestellt.

Bei jeder Sitzung werden die IP-Adresse des Management-Clients sowie der Beginn und das Ende der Sitzung protokolliert. Die Protokollierung der veränderten Daten geschieht weiterhin in den OpenScape 4000 V10-Knoten.

Der OpenScape 4000 V10 hat im OpenScape 4000 Manager-System Priorität gegenüber den laufenden Applikationen. Das heißt, die modifizierten Daten werden in der OpenScape 4000 V10-Datenbank gespeichert und die Applikation wird durch eine Meldung von der Änderung in Kenntnis gesetzt.

Eine Beschreibung des OpenScape 4000 Manager finden Sie in den entsprechenden Dokumentationen.

4 Frontansicht

Informationen zur Frontansicht, siehe Abschnitt Section 7.4.1.4, "Frontblende".

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Netzwerkschnittstellen* > *Frontansicht*

5 Assistent

IMPORTANT: Assistenten sind nur verfügbar, wenn Schreibzugriff möglich ist. Der Schreibzugriff wird über das Schloss-Symbol ein- und ausgeschaltet (siehe Abschnitt 4.3.2, 'Symbole im Steuerbereich des WBM-Fenster').

Ein Assistent besteht aus mehreren, nacheinander aufrufbaren Dialogen. Mit den Schaltflächen *Weiter* und *Rückgängig* kann in den Dialogen geblättert werden. Durch das Ausfüllen aller Dialoge eines Assistenten wird eine bestimmte, größere Aufgabe erledigt.

Derzeit ist im WBM ein Assistent für Ersteinstellungen verfügbar.

5.1 Ersteinstellungen

Es wird empfohlen, die Konfiguration des HG 3500/3575 zu organisieren, bevor Sie diesen Assistenten starten, damit Sie die Dialoge des Assistenten ohne Unterbrechung bearbeiten können.

Mit dem Assistenten für Ersteinstellungen können Sie konfigurieren:

- Name und Kontaktadresse des Gateways
- Zweite LAN-Schnittstelle
- Codec-Parameter
- Zusätzliche Leistungsmerkmale für das Gateway, für T.38-Fax und RFC2833

WBM-Pfad:

WBM (Schreibzugriff mit Schloss-Symbol im Steuerbereich aktiviert?) **>** Assistent **>** *Ersteinstellungen*

Der Dialog für Gateway-Eigenschaften wird angezeigt.

5.1.1 Gateway-Eigenschaften

Als Information werden die Steckplatznummer, die IP-Adresse des Gateways und die Subnetzmaske angezeigt. Sie können folgende Felder ansehen/bearbeiten:

Allgemein:

- *Board-Name*: Dieses Feld enthält den Namen des Systems. Geben Sie eine Zeichenkette in dieses Feld ein.
- *Physikalische Knotennummer (4K)*: Eindeutige Identifikationsnummer des Gateways. Format: 0-0-0
- *Gateway-Standort*: Dieses Feld enthält Angaben zum Aufstellungsort des HG 3500/3575. Diese Information hilft einem Servicetechniker, das Gateway zu finden, wenn physischer Zugang zum Gerät nötig ist. Geben Sie eine Zeichenkette in dieses Feld ein.
- *Kontakt-Adresse*: Dieses Feld enthält Angaben zu einer Kontaktperson, die bei Problemen mit dem Gateway angesprochen werden kann. Geben Sie eine Zeichenkette in dieses Feld ein.

- *System-Länderkennzeichen*: Als Information wird der bei der Installation festgelegte Ländercode sowie das zugehörige Land angezeigt. Dieser Eintrag ist hier nicht änderbar (nur für HG 3500).
- *Gateway-IP-Adresse*: Als Information wird die IP-Adresse des Gateways angegeben. Dieser Eintrag ist hier nicht änderbar.
- *Gateway-Netzmaske*: Als Information wird die Subnetzmaske des Gateways angegeben. Dieser Eintrag ist hier nicht änderbar.

Zusätzliche Leistungsmerkmale (nicht für HG 3575):

- *QoS - Fallback auf SCN*: Kreuzen Sie diese Option an, wenn Anrufe bei zu schlechter IP-Übertragungsqualität auf SCN umgeschaltet werden sollen.
- *Konferenz-Optimierung*: Bei einer Konferenz wird ein gezielter Fallback auf die G.711-Kodierung durchgeführt.
- *Unterstützung für Dispatch-Applikation* - nur für Native SIP Trunking-GW
- SIP-Register für Trunking erlauben - nur für Native SIP Trunking mit Profil
- *HFA via SIP aktivieren*: Wenn Sie dieses Kontrollkästchen aktivieren, werden SIP-Teilnehmer wie HFA-Teilnehmer behandelt. Dies bedeutet, dass das Call Processing der OpenScape 4000 für SIP-Teilnehmer die gleiche Art der Anrufsteuerung (call control) und das gleiche Protokoll (CorNet-TS) verwendet wie für HFA-Teilnehmer. SIP-Teilnehmer können ebenso wie HFA-Teilnehmer das Flex Routing nutzen, wenn diese Option aktiviert ist.

  NOTICE: Nur Basic Call wird zur Zeit unterstützt. Weitere Informationen finden Sie in der Dokumentation zu Remote Agent Server Solution.

- *Signalisierungsprotokoll für IP-Networking*: Unveränderbare Voreinstellung ist SIP.
- *SIP-Protokollvariante für IP-Networking*: Unveränderbare Voreinstellung ist SIP-Q.
- *Displayname Charactercode-Set*: Support von kyrillischen Displaynamen. Hierfür wird am Gateway die Zeichenkodierung über die Eingabe einer Zeichenkette (eines Strings) konfiguriert:

  – Default: Leerstring
  – Der String ist eine Zeichenfolge aus den Symbolen {'*', '1', '5', 'R', 'D'}: '*' = default, '1' = ISO8859-1, '5' = ISO-8859-5, 'R' = CorNet-TS (RUSSKYR), 'D' = H4000-DEUTSCH.

  An erster Stelle des Strings steht die Kodierung für Subscriber Downstream (DS)-Translation, an zweiter Stelle die Kodierung für Subscriber Upstream (US)-Translation, gefolgt von Trunking-DS/US und HFAviaSIP-DS/US.

  Für nicht vorhandene Stellen im String (Translation-Punkte) wird der Default (= '*') angewendet.

  Für Subscriber-DS/US und Trunking-DS/US ist der Default ISO-8859-1 Latin-1 (='1'), für HFAviaSIP ist das CorNet-TS (='R').

  Wird nur für einen der beiden Zwillingsparameter (-DS und -US) eine spezifische Translation eingestellt und der andere per Default, so wird auch

für den anderen die entsprechende Kodierung eingestellt, d.h. als Default angenommen.

Zum Übernehmen der Einstellung ist ein Neustart des Gateways erforderlich.

Klicken Sie auf *Übernehmen*, im Bestätigungsdialog auf *OK* und anschließend auf *Weiter*, um Ihre Eingaben zwischenzuspeichern und den Dialog für LAN2/Atlantik-LAN aufzurufen.

5.1.2 LAN2/Atlantik-LAN

Hintergrundinformationen:

siehe Abschnitt 9.1, 'Umgebungsanforderungen für VoIP' siehe Abschnitt 9.2, 'Bandbreitenbedarf in LAN/WAN-Umgebungen' siehe Abschnitt 9.3, 'Quality of Service (QoS)'

Die Anzeige des Dialogs und die möglichen Eingabefelder sind von der aktuellen Betriebsart der zweiten LAN-Schnittstelle abhängig.

- *Das zweite LAN verwenden als***:** Wählen Sie die gewünschte Betriebsart der zweiten LAN-Schnittstelle aus. Folgende Auswahlmöglichkeiten werden angeboten:
  - *PPTP*: Wird PPTP aktiviert, so wird gleich versucht, eine Verbindung zum PPTP-Server aufzubauen.
  - *Redundanz für LAN1*: Die zweite LAN-Schnittstelle soll verwendet werden, wenn die erste LAN-Schnittstelle ausfällt.
  - *Nicht konfiguriert oder deaktiviert*: Die zweite LAN-Schnittstelle soll nicht verwendet werden.

  Diese Auswahlmöglichkeit gibt es nur bei HG 3500, da die Funktion 'zweite LAN-Schnittstelle verwenden, wenn erste LAN-Schnittstelle ausfälltâ für HG 3575 standardmäßig aktiviert ist.

5.1.2.1 Dialog für Betriebsart: PPTP

Sie können folgende Einträge vornehmen:

IP-Parameter

- *Partner-IP-Adresse der PPP-Verbindung*: Geben Sie die IP-Adresse des Hostrechners ein, zu dem die Punkt-zu-Punkt-Verbindung aufgebaut wird. Bei einer getunnelten Verbindung ist dies die virtuelle IP-Adresse.
- *Lokale IP-Adresse der PPP-Verbindung*: Geben Sie die IP-Adresse des PCs ein, der die Punkt-zu-Punkt-Verbindung aufbaut. Bei einer getunnelten Verbindung ist dies die virtuelle IP-Adresse.
- *Max. Datenpaketlänge (Byte)*: Geben Sie die maximale Paketlänge in Bytes für das IP-Protokoll an. Der zulässige Wertebereich geht von 576 bis zu 1500 Byte.

- *IP-Adress-Aushandlung*: Wählen Sie aus, ob und wie die IP-Adresse zwischen dem Gateway und dem Hostrechner beim Verbindungsaufbau ausgehandelt werden soll. Es gibt die folgenden Optionen:
  - *konfigurierte IP-Adresse nutzen*: Das Gateway soll die im Eingabefeld *Partner-IP-Adresse der PPP-Verbindung* konfigurierte IP-Adresse des Hostrechners nutzen.
  - *jede IP-Adresse akzeptieren*: Das Gateway soll jede angebotene IP-Adresse akzeptieren.
  - *neue IP-Adresse anfordern*: Das Gateway soll vor jeder IP-Verbindung einen neue IP-Adresse vom Hostrechner anfordern.

PPTP-Parameter

- *Lokale IP-Adresse der Kontrollverbindung*: Geben Sie die IP-Adresse des Gateways ein, die für PPTP-Verbindungen verwendet wird. Der voreingestellte Wert lautet 192.0.2.4. Die Adressen 0.0.0.0 und 255.255.255.255 sind nicht erlaubt.
- *Partner-IP-Adresse der Kontrollverbindung*: Geben Sie die IP-Adresse des Hostrechners ein, zu dem die PPTP-Verbindung aufgebaut wird. Der voreingestellte Wert lautet 192.0.2.5. Die Adressen 0.0.0.0 und 255.255.255.255 sind nicht erlaubt.
- *Partner-Netzmaske für die Kontrollverbindung*: Geben Sie in dieses Feld die Netzmaske für die PPTP-Verbindung ein.

Authentifizierung

- *PPP-Authentifizierung*: Geben Sie an, ob eine Authentifizierung erfolgen soll. Bei angekreuzter Funktion wird die Parametermaske erweitert:
- *PPP-Benutzername*: Geben Sie einen frei wählbaren Benutzernamen an, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
- *PAP-Authentifizierungsmode*: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (PAP-Client, PAP-Host, nicht benutzt).
- *PAP-Kennwort*: Geben Sie das Kennwort ein, mit dem der Nutzer sich bei der Authentifizierung durch PAP identifiziert. Das Feld kann bei nicht genutzter PAP-Authentifizierung nicht beschrieben werden.
- *CHAP-Authentifizierungsmode*: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (CHAP-Client, CHAP-Host, CHAP-Client und -Host, nicht benutzt).
- *CHAP-Kennwort*: Geben Sie das Kennwort ein, mit dem der Nutzer sich bei der Authentifizierung durch CHAP identifiziert. Das Feld kann bei nicht genutzter CHAP-Authentifizierung nicht beschrieben werden.

Klicken Sie auf *Übernehmen*, im Bestätigungsdialog auf *OK* und anschließend auf *Weiter*, um Ihre Eingaben zwischenzuspeichern und den Dialog für Codec-Parameter aufzurufen.

5.1.2.2 Dialog für Betriebsart: Redundanz für LAN1

Mit dieser Einstellung legen Sie fest, dass bei Ausfall des LAN1 das LAN2 die Funktion inklusive MAC- und IP-Adresse des LAN1 übernimmt.

In dieser Betriebsart können Sie im Dialog keine weiteren Einträge vornehmen.

Klicken Sie auf *Übernehmen*, im Bestätigungsdialog auf *OK* und anschließend auf *Weiter*, um Ihre Eingaben zwischenzuspeichern und den Dialog für Codec-Parameter aufzurufen.

5.1.3 Codec-Parameter

Hintergrundinformationen:

siehe Abschnitt 9.2, 'Bandbreitenbedarf in LAN/WAN-Umgebungen'

Tabelle 'Codec'

In der Tabelle 'Codec' können Sie nachfolgende Parameter für die Protokolle 'G.711 A-law', 'G.711 Âµ-law', 'G.723' (nur für HG 3500), 'G.729', 'G.729A', 'G.729B' und 'G.729AB' bearbeiten:

- *Priorität:* In dieser Spalte kann die Priorität ausgewählt werden, mit welcher der Codec verwendet werden soll. Die Priorität kann von 1 (hoch) bis 5 (niedrig) eingestellt werden. Ordnen Sie den Codecs unterschiedliche Prioritäten zu. In der Voreinstellung haben die Codecs folgende Prioritäten:
  - G.711 A-law: Priorität 1 (HG 3500), 1 (HG 3575)
  - G.711 Âµ-law: Priorität 2 (HG 3500), nicht verwendet (HG 3575)
  - G.723: Priorität 4 (nur für HG 3500)
  - G.729: nicht verwendet
  - G.729A: Priorität 3 (HG 3500), 2 (HG 3575)
  - G.729B: nicht verwendet
  - G.729AB: Priorität 7 (HG 3500), 7 (HG 3575)
- *Sprechpausenerkennung (VAD)*:Dieses Feld legt fest, ob beim jeweiligen Codec die Sprechpausenerkennung (VAD) verwendet werden soll oder nicht.
- *Rahmengröße*:In diesem Feld können Sie die Sampling-Rate bestimmen. Die einstellbaren Werte sind von den Codecs abhängig.

T.38-Fax

- *T.38-Fax*:Dieses Feld legt fest, ob das T.38-Faxprotokoll zum Einsatz kommen soll oder nicht.
- *Max. UDP-Datagramm-Größe für T.38-Fax (Byte)*:Geben Sie die maximale Größe eines T.38-UDP-Datagramms in Bytes an.
- *Verwendete Fehlerkorrektur für T.38-Fax (UDP)*: Dieses Feld legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll. Zur Auswahl stehen *t38UDPRedundancy* und *t38UDPFEC*.
- Zeitspanne für direkte Umschaltung auf T.38-Fax (s): Voreinstellung ist '0'. Der Wert '0' bedeutet, dass die direkte Umschaltung ausgeschaltet ist.

IMPORTANT: Der Codec G729 ist identisch mit dem Codec G729A und der Codec G729B ist identisch mit dem Codec G729AB (kein Unterschied in 'payload'.) Deshalb sind die Codecs G729 und G729B in der Voreinstellung ausgeschaltet.

IMPORTANT: Aus H323-Signalisierungs-Sicht sind die Codecs G729 und G729A und die Codecs G729B und G729AB unterschiedlich.

IMPORTANT: Einige non-OpenScape H.323-Endpunkte (Cisco GK) verwenden die Codecnamen G729 oder G729B im 'H323 signalling'. In diesem Fall müssen die Codecs G729 und G729B verwendet werden.

IMPORTANT: In einem reinen OpenScape-Netz können die Codecs G729 und G729B ausgeschaltet bleiben.

Sonstiges

- *ClearMode (ClearChannelData)*:Dieses Feld legt fest, ob die ClearChannel-Funktionalität aktiviert sein soll oder nicht.
- *Rahmengröße*:In diesem Feld können Sie die Sampling-Rate bestimmen. Möglich sind 10, 20, 30, 40, 50 und 60 Millisekunden (ms). Die Voreinstellung beträgt 20 ms.

RFC2833

Ausführliche Beschreibung des Standards siehe http:///www.faqs.org/rfcs/rfc2833.html.

- *Übertragung von Fax/Modem Tönen nach RFC2833*: Unterstützte Events: 32 bis 36 und 49.
- *Übertragung von DTMF Tönen nach RFC2833*: Unterstützte Events: 0 bis 15.
- *Payload Type für ClearChannel*: (nicht für HG 3575) Unterstützte Payload Types 96 bis 126. Default: 96.
- *Payload Type für RFC2833*: (nicht für HG 3575) Unterstützte Payload Types 96 bis 126. Default: 98.
- *Payload Type für RFC2198*: (nicht für HG 3575) (= âPayload Type für RFC2833â + 1) Unterstützte Payload Types 96 bis 126. Default: 99.
- *Redundante Übertragung der RFC2833 Töne nach RFC2198*: Alle durch RFC2833 übertragene Töne sind nach RFC2198 versichert, wenn RFC2198 eingeschaltet ist. Ausführliche Beschreibung des Standards RFC 2198 siehe http:///www.faqs.org/rfcs/rfc2198.html.

Klicken Sie auf *Übernehmen* und anschließend auf *Weiter*, um Ihre Eingaben zwischenzuspeichern und den Assistenten für Ersteinstellungen zu beenden. Um alle Eingaben dauerhaft zu speichern, klicken Sie auf das Sichern-Symbol im Steuerbereich (siehe Abschnitt 4.3.2, 'Symbole im Steuerbereich des WBM-Fenstersâ).

6 Konfiguration

In diesem Modul finden Sie Funktionen, die für die Konfiguration der Gateways HG 3500/3575 erforderlich sind.

WBM-Pfad:

WBM **>** *Konfiguration*

Die Optionen des Moduls *Konfiguration* werden auf der linken Seite angezeigt.

Optionen im Modul *Konfiguration*:

1) *Grundeinstellungen Sicherheit Netzwerk und Routing Sprachgateway*

6.1 Grundeinstellungen

Zu den Grundeinstellungen der Gateways HG 3500/3575 gehören einsehbare Hardware-Daten und bearbeitbare Basisdaten der Gateway-Funktionalität.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen*

Die Baumstruktur für *Grundeinstellungen* wird angezeigt.

Einträge unter *Grundeinstellungen*:

1) *System Gateway Quality of Service Zeitzonen-Einstellungen*

6.1.1 System

Sie können sich über den aktuellen Zustand bzw. die aktuelle Konfiguration wichtiger Systemkomponenten informieren.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Gateway-Eigenschaften*

Klicken Sie auf das Pluszeichen (+) neben *System*, um die folgenden Einträge anzuzeigen:

1) *Hardware-Konfiguration*

Software-Build

CPU

Task-Monitor

Speicher

Flash

Net-Stack-Ressourcen

Der Dialog *Gateway-Eigenschaften* wird angezeigt. Feldbeschreibungen siehe Section 7.1.3, "Gateway".

6.1.1.1 Hardware-Konfiguration

Sie können Detailinformationen zur Hardware des HG 3500/3575 ansehen.

WBM-Pfad:

WBM > Konfiguration > Grundeinstellungen > System > *Hardware-Konfiguration*

Der Dialog *Hardware-Konfiguration* wird angezeigt. Er bietet folgende Informationen:

- *Hardware-ID:* Hardware-Identifikation der Baugruppe (ID der Baugruppe im System OpenScape 4000 V10, z. B. 0x007D)
- *Seriennummer:* Seriennummer des Systems (Nummer auf dem Aufkleber auf der Baugruppe, z. B. SPU34030530131)
- *Teileliste:* Teileliste (Ausgabeversion der Teileliste, z. B. -04)
- *Boot-ROM-Version:*
- *FPGA-CID-Version:* Versionsangaben zum FPGA (Field Programmable Gate Array). FPGA-CID-Version ist die Chip-Version, z. B. 2.
- *FPGA-FW-Version:* Versionsangaben zum FPGA (Field Programmable Gate Array). FPGA-FW-Version ist die Version für den FPGA-Code des EEPROMs, z. B. 1.5.

6.1.1.2 Software-Build

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Software-Build* **>** *Software-Build-Version*

Der Dialog *Software-Build-Version* wird angezeigt. Die folgenden Informationen werden angezeigt:

Aktuell aktives Gateway-Image:

- *Software-Build-Version* (genaue Version der aktiven Software)
- *Loadware-Version*
- *Loadware-Info*

Alternatives Gateway-Image (nur bei HG 3575):

- *Software-Build-Version* (genaue Version der aktiven Software)
- *Loadware-Version*
- *Loadware-Info*

Falls ein anderes Software-Image geladen aber noch nicht aktiviert wurde, werden Version und Dateigröße dieses zur Installation bereitstehenden Software-Image angezeigt.

OpenScape System:

- *OpenScape System-Version:* Version des OpenScape 4000 Systems

Third-Party- und Open-Source-Software

6.1.1.3 CPU

Sie können die Konfiguration des Hauptprozessors ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *CPU* **>** *CPU-Konfiguration*

Der Dialog *CPU-Konfiguration* wird angezeigt. Die Darstellung enthält Informationen über den verwendeten Prozessortyp und die Prozessorgeschwindigkeit.

6.1.1.4 Task-Monitor

NOTICE: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad:

WBM > Konfiguration > Grundeinstellungen > System > *Task-Monitor*

Die Tabelle *Task-Monitor* wird angezeigt. Diese Tabelle enthält Informationen zu den derzeit aktiven Tasks: *Task-ID*, *Task-Name*, *Priorität*, *Status*, *Stack-Größe*, *Aktuelle Stack-Nutzung*, *Bisher höchste Stack-Nutzung*, *Stack-Margin*, *Fehler-Nr.*, *Aktuelle Verzögerung*.

6.1.2 Speicher

Sie können Details zur Speicherauslastung ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Speicher*

Klicken Sie auf das Pluszeichen (+) neben *Speicher*, um die folgenden Einträge anzuzeigen:

1) *Speicher-Status anzeigen Speicherverbrauch anzeigen DMA-Speicherverbrauch anzeigen*

6.1.2.1 Speicher-Status anzeigen

Sie können überprüfen, ob die Überwachung des Net-Stacks aktiv ist und in welchem Zeitrhythmus sie arbeitet.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Speicher* **>** *Speicher-Status*

Der Dialog *Speicher-Status* wird angezeigt. Es wird angezeigt, ob die Speicherüberwachung aktiv ist. *Überwachungstimer (s)* zeigt das Zeitintervall in Sekunden an, innerhalb dessen die gemessene Auslastung mit dem Grenzwert verglichen wird. *Überwachungs-Protokollierungs-Timer (s)* zeigt in

Sekunden an, wie lange ein Ereignis mindestens anliegen muss, damit es in die Protokolldatei aufgenommen wird.

6.1.2.2 Speicherverbrauch anzeigen

Sie können den aktuell gemessenen Speicherverbrauch ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Speicher* **>** Speicherverbrauch anzeigen **>** *Speicherverbrauch*

Der Dialog *Speicherverbrauch* wird angezeigt. Folgende Daten werden dargestellt:

- *Absoluter Speicherverbrauch (frei/belegt)*: Anzahl der gesamten, freien und belegten Bytes, Anzahl der freien und belegten Blöcke, Größe des größten freien Blocks.
- *Relativer Speicherverbrauch (in %)*: Aktueller Speicherverbrauch in Prozent und maximaler Speicherverbrauch bis zur Anzeige der Information.

6.1.2.3 DMA-Speicherverbrauch anzeigen

Sie können den aktuell gemessenen DMA-Speicherverbrauch ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Speicher* **>** DMA-Speicherverbrauch anzeigen **>***DMA-Speicherverbrauch*

Der Dialog *DMA-Speicherverbrauch* wird angezeigt. Folgende Daten werden dargestellt:

- *Absoluter Speicherverbrauch (frei/belegt)*: Anzahl der gesamten, freien und belegten Bytes, Anzahl der freien und belegten Blöcke, Größe des größten freien Blocks.
- *Relativer Speicherverbrauch (in %)*: Aktueller Speicherverbrauch in Prozent und maximaler Speicherverbrauch bis zur Anzeige der Information.

6.1.2.4 Flash

Sie können Details zur Flash-Speicherauslastung ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Flash*

Klicken Sie auf das Pluszeichen (+) neben *Flash*, um die folgenden Einträge anzuzeigen:

1) *Flash-Status anzeigen Flash-Verbrauch anzeigen*

6.1.2.5 Flash-Status anzeigen

Sie können überprüfen, ob die Temperaturüberwachung aktiv ist und in welchem Zeitrhythmus sie arbeitet.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Flash* **>** Flash-Status anzeigen **>** *Flash-Status*

Der Dialog *Flash-Status* wird angezeigt. Es wird angezeigt, ob die Flash-Speicherüberwachung aktiv ist. *Überwachungstimer (s)* zeigt das Zeitintervall in Sekunden an, innerhalb dessen die gemessene Auslastung mit dem Grenzwert verglichen wird. *Überwachungs-Protokollierungs-Timer (s)* zeigt in Sekunden an, wie lange ein Ereignis mindestens anliegen muss, damit es in die Protokolldatei aufgenommen wird.

6.1.2.6 Flash-Verbrauch anzeigen

Sie können den aktuell gemessenen Speicherverbrauch ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Flash* **>** *Flash-Verbrauch anzeigen* **>** *Flash-Verbrauch*

Der Dialog *Flash-Verbrauch* wird angezeigt. Folgende Daten werden dargestellt:

- *Größe des Flash-Speichers*: Größe des gesamten Speichers sowie die Größe des belegten und des freien Bereichs in Byte.
- *Relativer Flash-Verbrauch (in %)*: Aktueller Speicherverbrauch in Prozent und maximaler Speicherverbrauch bis zur Anzeige der Information.

6.1.2.7 Net-Stack-Ressourcen

Sie können die verfügbaren Ressourcen sowie den Status des Net-Stack-Speichers ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Net-Stack-Ressourcen*

Klicken Sie auf das Pluszeichen (+) neben *Net-Stack-Ressourcen*, um die folgenden Einträge anzuzeigen:

1) *Net-Pool-Status anzeigen System-Pools anzeigen Daten-Pools anzeigen*

6.1.2.8 Net-Pool-Status anzeigen

Sie können überprüfen, ob die Überwachung des Net-Stacks aktiv ist und in welchem Zeitrhythmus sie arbeitet.

WBM-Pfad:

WBM > *Konfiguration* > *Grundeinstellungen* > *System* > *Net-Stack-Ressourcen* > *Net-Pool-Status anzeigen* > *Net- Stack-Pool-Status*

Der Dialog *Net-Stack-Pool-Status* wird angezeigt. Es wird angezeigt, ob die Überwachung des Net-Stacks aktiv ist. *Überwachungstimer (s)* zeigt das Zeitintervall in Sekunden an, innerhalb dessen die gemessene Auslastung mit dem Grenzwert verglichen wird. *Überwachungs-Protokollierungs-Timer (s)* zeigt in Sekunden an, wie lange ein Ereignis mindestens anliegen muss, damit es in die Protokolldatei aufgenommen wird.

6.1.2.9 System-Pools anzeigen

Sie können die Net-Stack-Ressourcen für System-Pools ansehen.

WBM-Pfad:

WBM > *Konfiguration* > *Grundeinstellungen* > *System* > *Net-Stack-Ressourcen* > *System-Pools anzeigen* > *Net-Stack-Ressourcen für System-Pools*

Der Dialog *Net-Stack-Ressourcen für System-Pools* wird angezeigt. Angezeigt werden die belegten und freien Blöcke im System-Pool des Net-Stack-Speichers. Die Darstellung ist in Blockgrößen von 64 Byte, 128 Byte, 256 Byte und 512 Byte unterteilt. Sie erhalten Informationen über belegte und freie Elemente, den aktuellen und den bisherigen maximalen Verbrauch

6.1.2.10 Daten-Pools anzeigen

Sie können die Net-Stack-Ressourcen für Daten-Pools ansehen.

WBM-Pfad:

WBM > *Konfiguration* > *Grundeinstellungen* > *System* > *Net-Stack-Ressourcen* > *Daten-Pools anzeigen* > *Net-Stack-Ressourcen für Daten-Pools*

Der Dialog *Net-Stack-Ressourcen für Daten-Pools* wird angezeigt. Angezeigt werden die belegten und freien Blöcke im Daten-Pool des Net-Stack-Speichers. Die Darstellung ist in Blockgrößen von 64 Byte, 128 Byte, 256 Byte und 512 Byte, 1024 Byte und 2048 Byte) unterteilt. Sie erhalten Informationen über belegte und freie Elemente, den aktuellen und den bisherigen Maximalverbrauch.

6.1.3 Gateway

Dieser Eintrag zeigt die Gateway-Eigenschaften und -Einstellungen an.

WBM-Pfad:

WBM > *Konfiguration* > *Grundeinstellungen* > *Gateway* > *Gateway-Eigenschaften*

Sie können Eigenschaften und Einstellungen des Gateways ansehen und ändern.

Der Dialog *Gateway-Eigenschaften* wird angezeigt. Folgende Daten werden angezeigt bzw. können bearbeitet werden:

Allgemein:

- *Baugruppenname*: In diesem Feld steht die Bezeichnung der Anlage. Geben Sie eine Zeichenkette in dieses Feld ein.
- *Physikalische Knotennummer (4K)*: Eindeutige Identifikationsnummer des Gateways. Format: 0-0-0
- *Gateway-Standort*: Dieses Feld enthält Informationen zum Aufstellungsort des SoftGate. Diese Informationen helfen den Servicetechnikern, das Gateway zu finden, wenn sie auf das Gerät zugreifen müssen. Der Wert dieses Feldes stammt von AMO USCU und kann im WBM nicht geändert werden.
- *Kontaktadresse*: Dieses Feld enthält Angaben zu einer Kontaktperson, die bei Problemen mit dem Gateway angesprochen werden kann. Geben Sie eine Zeichenkette in dieses Feld ein.
- *System-Länderkennzeichen*: Als Information wird der bei der Installation festgelegte Ländercode sowie das zugehörige Land angezeigt. Dieser Eintrag ist hier nicht änderbar (nur für HG 3500).
- *Gateway-IP-Adresse*: Als Information wird die IP-Adresse des Gateways angegeben. Dieser Eintrag ist hier nicht änderbar.
- *Gateway-Subnetz-Maske*: Als Information wird die Subnetzmaske des Gateways angegeben. Dieser Eintrag ist hier nicht änderbar.

Zusätzliche Leistungsmerkmale: (nicht für HG 3575)

- *QoS – Fallback auf SCN:* Kreuzen Sie diese Option an, wenn Anrufe, die ihr IP-Ziel verfehlen, automatisch von IP- auf SCN-Basis umgeschaltet werden sollen (siehe Section 7.5.8, "Fallback auf SCN-Parameter").
- *Konferenz-Optimierung:* Bei einer Konferenz wird ein gezielter Fallback auf die G.711-Kodierung durchgeführt.
- *Unterstützung für Dispatch-Applikation* – nur für Native SIP Trunking-GW
- *SIP-Register für Trunking erlauben* – Nur für Native SIP Trunking mit Profil.
- *Instant-DMC verwenden* – Nur für Native SIP Trunking und SIP-Endpunkte.
- *Early Media bei SIP-Trennung verwenden* – Nur für Native SIP Trunking-GW.
- **NOTICE:** Nur Basic Call wird zur Zeit unterstützt. Weitere Informationen finden sie in der Dokumentation zur Remote Agent Server-Lösung.
- *Signalisierungsprotokoll für IP-Networking:* SIP. Die Einstellung ist nicht änderbar und wird daher nur angezeigt.
- *Displayname Charactercode-Set*: Unterstützung für kyrillische Anzeige-namen. Hierfür wird am Gateway die Zeichenkodierung über die Eingabe einer Zeichenkette (eines Strings) konfiguriert:
- – Standard: Leere Zeichenfolge

– Die Zeichenfolge ist eine Folge der Symbole {'*', '1', '5', 'R', 'D'}:
'*' = Standard, '1' = ISO8859-1, '5' = ISO-8859-5, 'R' = CorNet-TS (RUSSKYR), 'D' = H4000-GERMAN.

An erster Stelle des Strings steht die Kodierung für Subscriber Downstream (DS)-Translation, an zweiter Stelle die Kodierung für Subscriber Upstream (US)-Translation, gefolgt von Trunking-DS/US und HFAviaSIP-DS/US.

Für nicht vorhandene Stellen im String (Translation-Punkte) wird der Default (= '*') angewendet.

Für Subscriber-DS/US und Trunking-DS/US ist der Default ISO-8859-1 Latin-1 (='1'), für HFAviaSIP ist das CorNet-TS (='R').

Wird nur für einen der beiden Zwillingsparameter (-DS und -US) eine spezifische Translation eingestellt und der andere per Default, so wird auch für den anderen die entsprechende Kodierung eingestellt, d.h. als Default angenommen.

Zum Übernehmen der Einstellung ist ein Neustart des Gateways erforderlich.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen. Starten Sie das Gateway neu.

6.1.4 Quality of Service

'Quality of Service' (Dienstgüte) wird im HG 3500/3575 durch die Priorisierung von IP-Paketen unterstützt. Die Priorisierung erfolgt anhand der Informationen im IP-Header. Dabei sollten die jeweiligen Übertragungspartner das gleiche 'Quality of Service'-Verfahren verwenden. Das Verfahren ist einsehbar und änderbar.

Beim IP-Datenverkehr werden Pakete, die das HG 3500/3575 selbst produziert, in verschiedene Gruppen aufgeteilt.

Hintergrundinformationen:

Siehe Section 9.3, "Quality of Service (QoS)"

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *Quality of Service*

Das Fenster *Quality of Service* wird angezeigt. Sie können die aktuellen Gateway-Einstellungen zur Quality of Service bearbeiten.

Folgende Daten können Sie bearbeiten:

- *Prioritätsklasse für Signalisierungsdaten*:Prioritätsklasse für den Verbindungsaufbau. Nicht veränderbar.
- *Prioritätsklasse für Fax/Modem-Payload (nur bei IP-Netzwerken)*:Wählen Sie die entsprechende Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung aus.
- Es werden zur Auswahl angeboten:
  – *AF:* Assured Forwarding (Garantierte Weiterleitung unter festgelegten Bedingungen). Dem Datenverkehr werden Klassen und Abwurf-Prioritäten zugeordnet. Damit kann die Weiterleitung von Daten garantiert

werden, solange ein bestimmtes Datenaufkommen nicht überschritten wird. Wird das festgelegte Datenaufkommen überschritten, werden Datenpakete entsprechend ihrer Abwurf-Priorität verworfen.

  - – *AF11, AF12, AF13:* Datenverkehr der Klasse 1 mit den Abwurf-Prioritäten niedrig (AF11), mittel (AF12) und hoch (AF13).
  - *AF21, AF22, AF23:* Datenverkehr der Klasse 2 mit den Abwurf-Prioritäten niedrig (AF21), mittel (AF22) und hoch (AF23).
  - *AF31, AF32, AF33:* Datenverkehr der Klasse 3 mit den Abwurf-Prioritäten niedrig (AF31), mittel (AF32) und hoch (AF33).
  - *AF41, AF42, AF43:* Datenverkehr der Klasse 4 mit den Abwurf-Prioritäten niedrig (AF41), mittel (AF42) und hoch (AF43).
  - *EF:* Expedited Forwarding (schnelle Weiterleitung). Ist vorgesehen für Datenverkehr, der einen geringen Verlust und eine geringe Latenzzeit haben darf.
  - *Best effort / DF:* Diese Priorisierung ist für ein typisches Routerverhalten vorgesehen.
  - *CS1, CS2, CS3, CS4, CS5, CS6, CS7:* Klassenselektor. Diese Priorisierung wird für Network Control Packets (z. B. SNMP) verwendet.
  - *DSCP1, DSCP2, DSCP3, DSCP4, DSCP5, DSCP6, DSCP7, DSCP9, DSCP11, DSCP13, DSCP15, DSCP17, DSCP19, DSCP21, DSCP23, DSCP25, DSCP27, DSCP29, DSCP31, DSCP33, DSCP35, DSCP37, DSCP39, DSCP41, DSCP42, DSCP43, DSCP44, DSCP45, DSCP47, DSCP49, DSCP50, DSCP51, DSCP52, DSCP53, DSCP54, DSCP55, DSCP57, DSCP58, DSCP59, DSCP60, DSCP61, DSCP62, DSCP63:* Differentiated Services Code Point; wird zur Priorisierung von IP-Paketen verwendet.

- *Prioritätsklasse für Netzwerksteuerung*: Prioritätsklasse für die Daten der Netzwerksteuerung (z. B. Übermittlung von SNMP-Traps). Nicht veränderbar.
- *Prioritätsklasse für Sprach-Payload*:Prioritätsklasse für Sprachdaten auf der IP-Verbindung.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen.

IMPORTANT: Die voreingestellten Werte müssen in der Regel nicht geändert werden.

6.1.5 Zeitzonen-Einstellungen

WBM-Pfad:

WBM > Konfiguration > Grundeinstellungen > *Zeitzonen-Einstellungen*

Das Fenster *Zeitzonen-Einstellungen* mit der Zeitverschiebung in Minuten zur UTC (Universal Time Coordinated) wird angezeigt.

NOTICE: Die Zeitzonen-Einstellung werden über das OpenScape-System gesendet und können nicht über das WBM geändert werden.

6.2 Statistiken

Leistung und Status des Gateways können durch Statistiken überwacht werden.

Sind Statistiken über Sprach-, TSC-, DMC- und Daten-Anrufe.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *Statistiken*

Leistung und Status des Gateways können durch Statistiken überwacht werden.

Klicken Sie auf das Pluszeichen (+) neben *Statistiken*, um die folgenden Einträge anzuzeigen:

Einträge in der Baumstruktur *Statistiken*:

1) *Device-Statistiken MSC-Statistiken Ruf-Statistiken*

6.2.1 Device-Statistiken

Device-Statistiken sind Statistiken zur LAN-Nutzung und zu SCN.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *Device-Statistiken*

Klicken Sie auf das Pluszeichen (+) neben *Device-Statistiken*, um die folgenden Einträge anzuzeigen:

1) *LAN-Statistik SCN-Statistik*

6.2.1.1 LAN-Statistik

Die LAN-Statistik informiert über konfigurierte und verwendete Kanäle einzelner LAN-Devices.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Statistiken* **>** *Device-Statistiken* **>** *LAN-Statistik* **>** *Ressourcen-Statistik über LAN-seitige Devices*

Sie können die aktuelle LAN-Statistik ansehen.

Der Dialog *Ressourcen-Statistik über LAN-seitige Devices* wird angezeigt. Er enthält eine Tabelle, in der für jeden Device-Typ die aktuell belegten Ressourcen angezeigt werden. Beachten Sie auch den Hinweis unterhalb der Tabelle, dass die Frontansicht (siehe Section 7.4.1.4, "Frontblende") ebenfalls Aufschluss über die Ressourcenbelegung durch Devices gibt.

6.2.1.2 SCN-Statistik

Die SCN-Statistik informiert über konfigurierte und verwendete Kanäle einzelner SCN-Devices.

WBM-Pfad:

WBM > *Konfiguration* > *Statistiken* > *Device-Statistiken* > *SCN-Statistik* > *Ressourcen-Statistik über SCN-seitige Devices*

Sie können die aktuelle LAN-Statistik ansehen.

Der Dialog *Ressourcen-Statistik über SCN-seitige Devices* wird angezeigt. Er enthält eine Tabelle, in der für jeden Device-Typ die Anzahl aktuell belegter Ressourcen sowie der prozentuale Anteil an lizenzierten Kanälen angezeigt werden. Ferner wird angezeigt, wie viele Kanäle lizenziert sind. Beachten Sie auch den Hinweis unterhalb der Tabelle, dass die Frontansicht (siehe Section 7.4.1.4, "Frontblende") ebenfalls Aufschluss über die Ressourcenbelegung durch Devices gibt.

6.2.2 MSC-Statistiken

MSC-Statistiken sind Statistiken zur Überwachung der Medienstromkontrolle (Media Stream Control – MSC).

WBM-Pfad:

WBM > *Konfiguration* > *Statistiken* > *MSC-Statistiken* > *MSC-Statistiken*

Klicken Sie auf das Pluszeichen (+) neben *MSC-Statistiken*, um die folgenden Einträge anzuzeigen:

1) *Gesamt-Statistik Einzelruf-Statistik*

6.2.2.1 Gesamt-Statistik

Die MSC-Gesamt-Statistik bieten einen Überblick über die statistischen Daten für alle registrierten Gespräche.

WBM-Pfad:

WBM > *Konfiguration* > *Statistiken* > *MSC-Statistiken* > Gesamt-Statistik >*MSC-Gesamtstatistik*

Sie können die aktuelle MSC-Gesamt-Statistik aufrufen.

Der Dialog *MSC-Gesamtstatistik* wird angezeigt. Er gibt Aufschluss über gesendete und nicht gesendete RTP/RTCP-Pakete, über empfangene und nicht empfangene Pakete, und über die Anzahl gesendeter und empfangener Bytes.

6.2.2.2 Einzelruf-Statistik

Die MSC-Einzelruf-Statistik listet tabellarisch für jeden registrierten Anruf die Verbindungsdaten auf.

WBM-Pfad:

WBM > *Konfiguration* > *Statistiken* > *MSC-Statistiken* > Einzelruf-Statistik > *MSC-Einzelruf-Statistik*

Sie können die aktuelle MSC-Statistik mit Verbindungsdaten zu einzelnen Anrufen aufrufen.

Der Dialog *MSC-Einzelanruf-Statistik* wird angezeigt. Die angezeigte Tabelle listet zu jedem Anruf beteiligte IP-Adressen, den Zeitpunkt des Verbindungsaufbaus, Codecs-Informationen, Anzahl gesendeter und empfangener Bytes und Pakete, sowie Informationen zur Verbindungsqualität und zum aufgetretenen Jitter auf.

6.2.3 Ruf-Statistiken

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Statistiken* **>** *Ruf-Statistiken*

Klicken Sie auf das Pluszeichen (+) neben *Ruf-Statistiken*, um die folgenden Einträge anzuzeigen:

1) *Statistiken löschen*

Ruf-Statistik (1h) Ruf-Statistik (24h) Ruf-Statistik (gesamt) Ruf-Statistik (maximal parallel) LAN-Ruf-Statistik PBX-Ruf-Statistik Aktuelle Verbindungen MCP IPDA Verbindungs-Statistik (nicht bei vHG 3500) DMC IPDA Verbindungs-Statistik (nicht bei vHG 3500)

6.2.3.1 Statistiken löschen

Löscht alle Statistiken (außer den Zählern seit letztem Reboot).

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>***Ruf-Statistiken* **>** *Statistiken löschen*

Der Dialog *Statistiken löschen* wird angezeigt. Klicken Sie auf die Schaltfläche *Löschen*, um die Zähler zurückzusetzen oder auf die Schaltfläche *Abbrechen*, um den Dialog ohne Aktion zu verlassen.

6.2.3.2 Ruf-Statistik (1h)

Diese Statistik listet die Summen von Sprach- TSC-, DMC- und Daten-Anrufen der letzten Stunde auf.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Statistiken* **>** *Ruf-Statistiken* **>** *Ruf-Statistik (letzte Stunde)*

Sie können die Summen von Sprach- TSC-, DMC- und Daten-Anrufen der letzten Stunde ansehen.

Der Dialog *Ruf-Statistik (letzte Stunde)* wird angezeigt. Die angezeigten Summen unterteilen sich in vier Bereiche:

- Sprach-Anrufe
- TSC-Anrufe (**T**emporary **S**ignaling **C**all)
- DMC-Anrufe (**D**irect **M**edia **C**onnection)
- Daten-Anrufe

jeweils über über LAN oder PBX. Für alle vier Bereiche werden die Anzahl der

- erfolgreichen Verbindungen (... *Verbunden*) und
- die Anzahl der erfolgreich angenommenen Anrufe (... *Empfangen*) angezeigt.

Außerdem wird jeweils die Summe der Dauer aller Verbindungen in Sekunden angezeigt.

6.2.3.3 Ruf-Statistik (24h)

Diese Statistik listet die Summen von Sprach- TSC-, DMC- und Daten-Anrufen der letzten 24 Stunden auf.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *Ruf-Statistik (letzte 24 Stunden)*

Sie können die Summen von Sprach- TSC-, DMC- und Daten-Anrufen für LAN und PBX der letzten 24 Stunden ansehen.

Der Dialog *Ruf-Statistik (letzte 24 Stunden)* wird angezeigt. Kurzbeschreibung der Daten siehe Section 7.2.3.2, "Ruf-Statistik (1h)".

6.2.3.4 Ruf-Statistik (gesamt)

Diese Statistik listet die Summen von Sprach- TSC-, DMC- und Daten-Anrufen für LAN und PBX seit dem letzten Reboot auf.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *Ruf-Statistik (gesamt)* **>** *Ruf-Statistik (gesamt seit letztem Reboot)*

Sie können die Summen von Sprach- TSC-, DMC- und Daten-Anrufen für LAN und PBX seit dem letzten Reboot ansehen.

Der Dialog *Ruf-Statistik (gesamt)* wird angezeigt. Kurzbeschreibung der Daten siehe Section 7.2.3.2, "Ruf-Statistik (1h)".

6.2.3.5 Ruf-Statistik (maximal parallel)

Sie können die Summen von Sprach-, TSC-, DMC- und Daten-Anrufen für LAN und PBX ansehen, die das Gateway zum Spitzenlastzeitpunkt gleichzeitig bearbeitet hat.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *Ruf-Statistik (maximal parallel)* **>** *Ruf-Statistik (Maximum der gleichzeitigen Anforderungen seit letztem Reboot)*

Sie können die Summen von Sprach-, TSC-, DMC- und Daten-Anrufen für LAN und PBX ansehen, die das Gateway zum Spitzenlastzeitpunkt gleichzeitig bearbeitet hat.

Der Dialog *Ruf-Statistik (Maximum der gleichzeitigen Anforderungen)* wird angezeigt. Kurzbeschreibung der Daten siehe Section 7.2.3.2, "Ruf-Statistik (1h)".

6.2.3.6 LAN-Ruf-Statistik

Bei LAN-Rufen handelt es sich um Verbindungen mit anderen Knoten der OpenScape 4000 V10 (IP-Trunking) und vCAPI.

Diese Statistik listet die Summen der über LAN empfangenen Sprach-, TSC-, DMC-, und Daten-Anrufe der letzten Stunde, der letzten 24 Stunden, seit dem letzten Reboot und die, die das Gateway zum Spitzenlastzeitpunkt gleichzeitig bearbeitet hatte, auf.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *LAN-Ruf-Statistik* **>** *LAN-Ruf-Statistik gestartet*

Der Dialog *LAN-Ruf-Statistik gestartet* wird angezeigt.

Die angezeigten Summen unterteilen sich in vier Bereiche: einen für die zurückliegende Stunde, und einen für die zurückliegenden 24 Stunden, einen für seit dem letzten Reboot und für die mit der Eigenschaft 'maximal parallel'. Die Anzahl der erfolgreichen Verbindungen (*... Verbunden*) und die Anzahl der erfolgreich angenommenen Anrufe (*... Empfangen*) werden für alle Kategorien angezeigt. Außerdem wird jeweils die Summe der Dauer aller Verbindungen in Sekunden angezeigt. Alle Zahlen beziehen sich ausschließlich auf Verbindungen, die über LAN zustande kamen.

6.2.3.7 PBX-Ruf-Statistik

Bei PBX-Rufen handelt es sich um Anrufe mit System-Clients.

Diese Statistik listet die Summen der über PBX gelaufenen Sprach-, TSC-, DMC- und Daten-Anrufe der letzten Stunde, der letzten 24 Stunden, seit dem letzten Reboot und die, die das Gateway zum Spitzenlastzeitpunkt gleichzeitig bearbeitet hatte, auf.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *PBX-Ruf-Statistik* **>** *PBX-Ruf-Statistik gestartet*

Sie können die Summen der über PBX gelaufenen Sprach-, TSC-, DMC-, und Daten-Anrufe der letzten Stunde, der letzten 24 Stunden, seit dem letzten Reboot und die, die das Gateway zum Spitzenlastzeitpunkt gleichzeitig bearbeitet hatte, ansehen.

Der Dialog *PBX-Ruf-Statistik gestartet* wird angezeigt. Kurzbeschreibung der Daten siehe Section 7.2.3.6, "LAN-Ruf-Statistik". Alle Zahlen beziehen sich jedoch bei dieser Statistik ausschließlich auf Verbindungen, die über PBX zustande kamen.

6.2.3.8 Aktuelle Verbindungen

Anzahl derzeitiger Verbindungen und Verbindungsanforderungen ohne Unterschied zwischen Anruf-Art oder Herkunft.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *Aktuelle Verbindungen*

Sie können die Anzahl derzeitiger Verbindungen und Verbindungsanforderungen ansehen.

Der Dialog *Aktuelle Verbindungen* wird angezeigt. Die angezeigte Summe ergibt sich aus der Anzahl derzeitiger Verbindungen und Verbdindungsanforderungen ohne Unterschied zwischen Anruf-Art oder Herkunft.

6.2.3.9 MCP IPDA Verbindungs-Statistik (nicht bei vHG 3500)

Die Tabelle *MCP IPDA Verbindungs-Statistik* zeigt die MCP-Rufe (Multimedia Call Processing) in der IPDA (IP Distributed Architecture) von OpenScape 4000 V10.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>***MCP IPDA Verbindungs-Statistik (nicht bei vHG 3500)*

Sie können die MCP-Rufe seit der letzten Aktualisierung (60 Sekunden) ansehen.

Die Tabelle *MCP IPDA Verbindungs-Statistik* wird angezeigt. Sie umfasst die folgenden Spalten: *NPCI*, *Teilnehmer A*, *Teilnehmer B*, *Vermittlungsattribute*, *Codec*, *Quellport*, *Zielport*, *IP-Adresse* und *Index*.

6.2.3.10 DMC IPDA Verbindungs-Statistik (nicht bei vHG 3500)

Die Tabelle *MCP IPDA Verbindungs-Statistik* zeigt die DMC-Rufe (Direct Media Connection) in der IPDA von OpenScape 4000 V10.

WBM-Pfad:

WBM **>** *Konfiguration* **>** Statistiken **>** *Ruf-Statistiken* **>** *DMC IPDA Verbindungs-Statistik (nicht bei vHG 3500)*

Sie können die DMC-Rufe seit der letzten Aktualisierung (60 Sekunden) ansehen.

Die Tabelle *DMC IPDA Verbindungs-Statistik* wird angezeigt. Sie umfasst die folgenden Spalten: *NPCI*, *Korrelations-ID*, *Vorwärts-Codec*, *Rückwärts-Codec*, *Quellport*, *Zielport* und *IP-Adresse*.

6.3 Sicherheit

Zu den sicherheitsrelevanten Berechtigungen des HG 3500/3575 gehören Filter für zugreifende Geräte oder Anschlüsse und die Zugangsverwaltung der Gateway-Administration.

WBM-Pfad:

WBM > Konfiguration > *Sicherheit*

Die Baumstruktur für *Sicherheit* wird angezeigt.

Einträge in der Baumstruktur *Sicherheit*:

1) *MEK für IPDA (nur für HG 3575)*

MAC-Adress-Filter

IP-Adress-Filter

Benutzerkennungen

Deployment- und Licensing-Client (DLSC) Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))

TLS-Chiffren für HTTPS

TLS-Chiffren für SIP

TLS-Chiffren für HFA

6.3.1 MEK für IPDA (nur für HG 3575)

In diesem Dialog können MEKs (Master Encryption Keys) für IPDA (IP-Distributed Architecture) gesetzt und auch wieder gelöscht werden. Ein MEK ist ein spezieller symmetrischer Schlüssel, der zum Aufbau einer IP-Verbindung benötigt wird. Er besteht aus genau 16 alphanumerischen Zeichen.

WBM-Pfad:

WBM > Konfiguration > Sicherheit > *MEK für IPDA (nur für HG 3575)*

Klicken Sie auf das Pluszeichen (+) neben *MEK für IPDA*, um die folgenden Einträge anzuzeigen:

1) *Neuen MEK setzen Alle MEKs löschen*

6.3.1.1 Neuen MEK setzen

WBM-Pfad:

WBM > Konfiguration > Sicherheit > *MEK für IPDA (nur für HG 3575)* > *Neuen MEK setzen*

Der Dialog *Neuen MEK setzen* wird angezeigt. Es erscheinen die Eingabefelder *Neuer MEK* und *Bestätigung des neuen MEK*.

6.3.1.2 Alle MEKs löschen

WBM-Pfad:

WBM > Konfiguration > Sicherheit > *MEK für IPDA (nur für HG 3575)* > *Alle MEKs löschen*

Der Dialog *Alle MEKs löschen* wird angezeigt. Die Schaltfläche *Alle MEKs löschen* wird angezeigt.

6.3.2 MAC-Adress-Filter

MAC-Adressfilter schützen das HG 3500/3575 gegen nicht-autorisiertem Zugriff (z. B. über einen externen PC). Es sind nur PCs zugriffsberechtigt, deren IP-Adresse in Kombination mit der jeweils eindeutigen MAC-Adresse über diese Sicherheitsfunktion freigeben sind. Stimmt die IP- und MAC-Adresse nicht mit der hinterlegten Kombination überein, wird der Zugriff verweigert.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *MAC-Adress-Filter* **>** *MAC-Adress-Filter-Tabelleneditor*

Über den Dialog 'MAC-Adress-Filter-Tabelleneditorâ können Sie bequem alle vorhandenen und weitere MAC-Adress-Filterregeln auf einmal bearbeiten.

Wenn bereits MAC-Adress-Filterregeln hinzugefügt wurden, wird *MAC-Adress-Filter* als Liste dargestellt. In diesem Fall können Sie durch Klick auf *MAC-Adress-Filter* in der Baumstruktur die definierten MAC-Filterregeln sehen.

Jede Zeile der Tabelle stellt eine MAC-Adress-Filterregel dar.

- Schaltfläche *Hinzufügen*: Vor dem Klicken auf diese Schaltfläche müssen die unten genannten Einstellungen vorgenommen werden. Nach dem Klicken auf diese Schaltfläche werden diese Einstellungen automatisch überprüft und wenn sie richtig sind, wird die neue Regel hinzugefügt. Wenn die Einstellungen nicht richtig sind, erscheint eine Fehlermeldung.
- Schaltfläche *Löschen*: Wenn MAC-Adress-Filterregeln vorhanden sind, können Sie eine einzelne MAC-Adress-Filterregel löschen.
- Schaltfläche *Übernehmen*: Mit dieser Schaltfläche übernehmen Sie alle durchgeführten Änderungen.
- Schaltfläche Rückgängig: Mit dieser Schaltfläche machen Sie die Änderungen rückgängig.
- *Regelname*: Tragen Sie in dieses Feld einen eindeutigen Namen für die neue Filterregel ein.
- *Regel aktiviert*: Wenn Sie diese Option ankreuzen, wird die neu definierte Filterregel nach Klicken auf *Übernehmen* aktiviert.
- *IP-Adresse*: Tragen Sie in dieses Feld die IP-Adresse ein, von der IP-Pakete akzeptiert werden sollen. Beachten Sie, dass der Filter Pakete von dieser Adresse nur akzeptiert, wenn auch die MAC-Adresse übereinstimmt.
- *MAC-Adresse*: Geben Sie in dieses Feld die MAC-Adresse des Geräts ein, von dem Pakete akzeptiert werden sollen. Ist das Gerät über einen Router und nicht direkt mit der Baugruppe verbunden, müssen Sie die MAC-Adresse des Routers eintragen. In diesem Fall müssen Sie auch eine weitere MAC-Filterregel erstellen, die aus der IP-Adresse und der MAC-Adresse des Routers besteht. Dieses Vorgehen ist notwendig, da der Router

beim Transport der Pakete die MAC-Adressen austauscht (d. h. seine eigene MAC-Adresse einsetzt).
- *Für PPPoE Verbindung*: Wenn Sie diese Option ankreuzen, wird für die Verbindung nach dieser Regel das PPPoE-Protokoll aktiviert.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

IMPORTANT: Wenn der MAC-Filter aktiviert ist, können nicht mehr alle MAC-Filterregeln gelöscht werden. Ist nur noch eine Filterregel vorhanden, so kann diese nicht gelöscht werden. Damit soll sichergestellt werden, dass man, bei eingeschaltetem MAC-Filter, von mindestens einem PC noch das Gateway erreichen kann.

6.3.3 IP-Adress-Filter

IP-Adress-Filter schützen das HG 3500/3575 gegen nicht-autorisierten Zugriff (z. B. über ein externes Netz oder einen externen PC). Bei aktiviertem IP-Adress-Filter wird der Zugriff über ein ungesichertes Netz auf die freigegebenen IP-Adressen eingeschränkt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *IP-Adress-Filter* **>** *IP-Adress-Filter-Tabelleneditor*

Der Dialog *IP-Adress-Filterregel* wird angezeigt. In der Tabelle werden zu jeder definierten IP-Adress-Filterregel die Detail-Daten angezeigt (zur Bedeutung der Spaltenüberschriften siehe die entsprechenden Feldbeschreibungen).

Über den IP-Adress-Filter-Tabelleneditor können Sie bequem alle vorhandenen und weitere IP-Adress-Filterregeln auf einmal bearbeiten.

Jede Zeile der Tabelle stellt eine IP-Adress-Filterregel dar.

- Schaltfläche *Hinzufügen*: Vor dem Klicken auf diese Schaltfläche müssen die unten genannten Einstellungen vorgenommen werden. Nach dem Klicken auf diese Schaltfläche werden diese Einstellungen automatisch überprüft und wenn sie richtig sind, wird die neue Regel hinzugefügt. Wenn die Einstellungen nicht richtig sind, erscheint eine Fehlermeldung.
- Schaltfläche *Löschen*: Wenn MAC-Adress-Filterregeln vorhanden sind, können Sie eine einzelne MAC-Adress-Filterregel löschen.
- Schaltfläche *Übernehmen*: Mit dieser Schaltfläche übernehmen Sie alle durchgeführten Änderungen.
- Schaltfläche Rückgängig: Mit dieser Schaltfläche machen Sie die Änderungen rückgängig.
- *Regelname*: Regelname hier eingeben. Dieser Regelname wird nach dem Hinzufügen der Regel in der Baumstruktur angezeigt.
- *Regel aktiviert*: Wenn Sie diese Option ankreuzen, wird die neu definierte Filterregel nach Klicken auf *Übernehmen* aktiviert.
- *IP-Protokoll*: Geben Sie an, welches Protokoll zugelassen werden soll (*TCP*, *UDP*, *ICMP* oder *Alle*). Bei Auswahl von *ICMP* werden für ICMP die Kontrollkästchen *Alle Typen erlaubt* und *Alle Codes erlaubt* freigeschaltet.

- **Erläuterungen zu den Protokollen:**
  - TCP: Das Transmission Control Protocol (TCP) ist ein verbindungsorientiertes, paketvermittelndes Internetprotokoll zur Datenübertragung. Es können in beiden Richtungen Daten übertragen werden.
  - UDP: Das User Datagram Protocol (UDP) ist ein einfaches, verbindungsloses Internetprotokoll. Es dient dazu, über das Internet übertragene Daten der richtigen Anwendung zuzustellen. Es können nur in eine Richtung Daten übertragen werden.
  - ICMP: Das Internet Control Message Protocol (ICMP) dient zum Austauschen von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert ein ähnliches Protokoll mit dem Namen ICMPv6.
- *ICMP-Typ*: Das Eingabefeld wird freigeschaltet, wenn zuvor im Auswahlfeld *IP-Protokoll* der Eintrag *ICMP* ausgewählt und das Kontrollkästchen *Alle Typen erlaubt* deaktiviert wurde.
- In das Eingabefeld können Sie die zugelassenen ICMP-Pakettypen eingeben, wobei ein Wert zwischen 0 und 255 erlaubt ist. Die definierten Pakettypen sind wie folgt: 0, 3 bis 18, 30 bis 41, die übrigen Werte sind nur reserviert.

  Wenn Sie alle ICMP-Pakettypen erlauben möchten, aktivieren Sie das Kontrollkästchen *Alle Typen erlaubt*.
- *ICMP-Codenummer*: Das Eingabefeld wird freigeschaltet, wenn zuvor im Auswahlfeld *IP-Protokoll* der Eintrag *ICMP* ausgewählt und das Kontrollkästchen *Alle Codes erlaubt* deaktiviert wurde.
- In das Eingabefeld können Sie die zugelassenen ICMP-Codenummern eingeben, wobei ein Wert zwischen 0 und 255 erlaubt ist. Definierte Codenummern sind: 0 bis 5 und 13.

  Wenn Sie alle ICMP-Codenummern erlauben möchten, aktivieren Sie das Kontrollkästchen *Alle Codes erlaubt*.
- *Untergrenze des Quell-IP-Adressbereichs*: Die Filterregel lässt nur IP-Adressen passieren, deren Absenderadressen einem festgelegten Bereich entstammen. Geben Sie in dieses Feld die untere Grenze des zulässigen Adressbereichs ein, von dem Pakete durchgelassen werden sollen.
- *Obergrenze des Quell-IP-Adressbereichs*: Geben Sie in dieses Feld die obere Grenze des zulässigen Adressbereichs ein, von dem Pakete durchgelassen werden sollen.
- *IP-Portnummern ([v]=Alle)*: Eingabefeld und Kontrollkästchen
- *Untergrenze des Ziel-IP-Adressbereichs*: Die Filterregel lässt einen IP-Bereich zu, zu dem Pakete durchgelassen werden. Geben Sie in dieses Feld die untere Grenze des zulässigen Adressbereichs ein, zu dem Pakete durchgelassen werden sollen.
- *Obergrenze des Ziel-IP-Adressbereichs*: Geben Sie in dieses Feld die obere Grenze des zulässigen Adressbereichs ein, zu dem Pakete durchgelassen werden sollen.

IMPORTANT: Um Pakete zu beliebigen IP-Adressen durchzulassen, geben Sie für *Untergrenze des Ziel-IP-Adressbereichs* den Wert `0.0.0.0` ein, und für *Obergrenze des Ziel-IP-Adressbereichs* den Wert `255.255.255.255`. Die Bezeichnung Quell- und Ziel-Adresse bezieht sich darauf, wer die Verbindung aufbaut. Soll z. B. das HG 3500/3575 die Verbindung aufbauen können, so ist die Baugruppe die Quelle und die Gegenseite der Verbindung das Ziel. Wenn eine

Verbindung erfolgreich aufgebaut wurde, werden die zu dieser Verbindung gehörenden Pakete in beide Richtungen übertragen, auch wenn nur für eine Richtung eine Filterregel angegeben wurde.

- *Port* und *Alle Ports erlaubt*: Das Kontrollkästchen *Alle Ports erlaubt* wird freigeschaltet, wenn im Auswahlfeld *IP-Protokoll* das Protokoll *TCP* oder das Protokoll *UDP* ausgewählt wurde.
- Nach Deaktivieren von *Alle Ports erlaubt* kann ein Protokoll-Port für den angegebenen Adressbereich eingegeben werden. Damit können Sie den Filterbereich weiter einschränken. Falls alle Ports benutzt werden dürfen, aktivieren Sie das Kontrollkästchen *Alle Ports* erlaubt.

Regel aktivieren

Wenn IP-Adress-Filterregeln vorhanden sind, können Sie eine einzelne, bislang deaktivierte IP-Adress-Filterregel (rotes Symbol) aktivieren.

Eine Warnung wird angezeigt. Bestätigen Sie sie mit *OK*.

Regel deaktivieren

Wenn IP-Adress-Filterregeln vorhanden sind, können Sie eine einzelne, bislang aktivierte IP-Adress-Filterregel (grünes Symbol) deaktivieren.

Eine Warnung wird angezeigt. Bestätigen Sie sie mit *OK*.

6.3.4 Benutzerkennungen

Es werden alle mit dem AMO CGWB definierten Benutzerkennungen in einer Tabelle angezeigt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Benutzerkennungen*

Der Dialog *Benutzerkennungen* wird angezeigt. In der Tabelle werden zu jeder Benutzerkennung der *Name* und die *Autorisierung* angezeigt.

Benutzerkennungen werden als Liste dargestellt. Durch Klick auf *Benutzerkennungen* werden in der Baumstruktur die eingerichteten Benutzerkennungen angezeigt. *Name* und *Autorisierung* der jeweiligen Benutzerkennung werden aufgelistet.

Name

Name der Benutzerkennung

Autorisierung

Berechtigungsklasse der Benutzerkennung

6.3.5 Deployment- und Licensing-Client (DLSC)

Der Deployment- und Licensing-Client (DLSC) wird zur Verwaltung von PKI-Daten und der QDC-Konfiguration (PKI) verwendet: **P**ublic **K**ey **I**nfrastructure,

QDC: **Q**uality of Service **D**ata **C**ollection, DLS: **D**ep**l**oyment **S**ervice oder **D**eployment and **L**icensing **S**erver).

WBM-Pfad:

WBM > Konfiguration > Sicherheit > *Deployment- und Licensing-Client (DLSC)*

Klicken Sie auf das Pluszeichen (+) neben *Deployment- und Licensing-Client (DLSC)*, um die folgenden Einträge anzuzeigen:

1) *DLSC Grundeinstellung anzeigen*

DLSC Grundeinstellung ändern

PIN Eingabe

Bootstrapping zurücksetzen

DLSC kontaktieren

DLSC Client-Zertifikat DLSC CA-Zertifikate

Zertifikatsgenerierung und -verteilung für die Kommunikation zwischen DLS-Client und DLS-Server:

Alle Zertifikate und privaten Schlüssel für die verschlüsselte Kommunikation zwischen DLS-Client und DLS-Server werden durch eine selbst-signierende Zertifizierungsstelle (CA) des DLS-Servers erzeugt und durch den DLS-Server während des Bootstrapping Mode zum DLS-Client gesendet.

Die vom DLS-Server zum DLS-Client gesendete PKCS#12-Datei enthält das DLSC Client-Zertifikat, den darin enthaltenen privaten Schlüssel und das Zertifikat der Zertifizierungsstelle des DLS-Servers (DLSC CA-Zertifikat). Der DLS-Server kann alle von ihm gelieferten Zertifikate zurücklesen, jedoch nicht den privaten Schlüssel.

Generation und Distribution von Zertifikaten für die sichere Verbindung zwischen dem WBM und dem DLS-Server:

Der Administrator sendet das WBM-Zertifikat mit dem von der PKI-Zertifizierungsstelle des Kunden generierten privaten Schlüssel manuell an OpenScape 4000 Assistant. Anschließend sendet OpenScape 4000 Assistant das WBM-Zertifikat automatisch an alle Gateways. Mit diesem Zertifikat weist sich der DLS-Client gegenüber dem DLS-Server aus.

6.3.5.1 DLSC Grundeinstellung anzeigen

Im Dialog *DLS Client Grundeinstellung* sehen Sie die Parameter für den Aufbau der Kommunikation des Deployment- und Licensing-Client (im Folgenden: DLS-Client) mit dem Deployment- und Licensing Server (im Folgenden: DLS-Server).

Zum Beginn der Kommunikation mit dem DLS-Server befindet sich der DLS-Client im Bootstrapping Mode. Der Bootstrapping Mode dient dem Registrieren des DLS-Client am DLS-Server. Nachdem das Registrieren abgeschlossen ist, wechselt der DLS-Client automatisch in den Secure Mode.

Der Secure Mode ist die normale Betriebsart des DLS-Client. Im Secure Mode werden der Port für die sichere Verbindung und die individuellen Zertifikate, die während des Bootstrapping Mode konfiguriert wurden, verwendet.

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC Grundeinstellung anzeigen* > *DLS Client Grundeinstellung anzeigen*

Daten im Dialog *DLS Client Grundeinstellung*:

Aktuelle DLS Client Grundeinstellung:

- *Zeitintervall für ContactMe-Antwort:*
- Der DLS-Client wartet eine bestimmte Zeit auf eine ContactMe Message des DLS-Servers, die dieser nach einem Scan des Netzwerkes zu den gefundenen Geräten sendet. Unter 'Aktuelle DLS Client Grundeinstellung' sehen Sie dafür den Parameter *Zeitintervall für ContactMe-Antwort*. Die ContactMe-Message enthält die IP-Adresse und den Port des DLS-Servers für den Bootstrapping Mode. Der DLS-Client entnimmt diese Daten und sendet daraufhin periodisch Startup Request Messages an die ermittelte IP-Adresse und den Port des DLS-Servers, bis die Requests vom DLS-Server akzeptiert werden.

  Die Wartezeit des DLS-Client für den Empfang von ContactMe Messages vom DLS-Server beträgt z.B. '0'. Die Wartezeit muss begrenzt sein, damit ContactMe Messages von böswilligen DLS-Servern nicht empfangen werden können.
- *PIN für DLS-Bootstrapping erforderlich:*

Während des Bootstrapping Mode benutzt der DLS-Client Zertifikate. Wenn der Parameter *PIN für DLS-Bootstrapping erforderlich* auf 'Nein' gesetzt ist, werden die Default-Zertifikate verwendet. Um Angriffe von böswilligen DLS-Servern zu verhindern, sollten keine Default-Zertifikate, sondern Zertifikate mit individuellen Passphrases verwendet werden (Passphrase: ein aus mehreren Wörtern bestehendes Passwort).

- *Sichere Kommunikation mit DLS Client:*
- Wenn sich der DLS-Client im Secure Mode befindet, ist der Parameter 'Sichere Kommunikation mit DLS Client' im Dialog *DLS Client Grundeinstellung anzeigen* aktiviert.

  Aktuelle DLS Client Server Einstellung:

  Für jede Betriebsart wird ein eigener Port am DLS-Server benötigt. Unter 'Aktuelle DLS Client Server Einstellung' sehen Sie dafür die folgenden Daten:
- *IP-Adresse des DLS-Servers:* Wird für den Bootstrapping Mode verwendet.
- *Port des DLS-Servers:* Wird z. B. für den Bootstrapping Mode verwendet: 18443
- *Sicherer Port des DLS-Servers:* Wird z. B. für den Bootstrapping Mode verwendet: 18444

6.3.5.2 DLSC Grundeinstellung ändern

Außer dem automatischen Registrieren des DLS-Client am DLS-Server mittels der ContactMe-Antwort kann der DLS-Client auch manuell registriert werden. Dafür müssen Ihnen vom DLS-Server die IP-Adresse und der Port für den Bootstrapping Mode bekannt sein.

Die IP-Adresse und der Port des DLS-Servers können mittels AMO konfiguriert werden. Diese Änderung wird erst nach einem Reboot des Gateways wirksam.

Nach Setzen von IP-Adresse und Port des DLS-Servers erfolgt beim Reboot (und jedem weiteren Reboot) ein einmaliger Versuch durch Senden einer Startup Request Message das Bootstrapping einzuleiten.

Mit dem WBM Menüpunkt "DLS kontaktieren" können manuell weitere Verbindungsversuche eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC Grundeinstellung ändern* > *DLS Client Grundeinstellung ändern*

Der Dialog *DLS Client Grundeinstellung ändern* erscheint. In diesem Dialog können Sie Folgendes ändern:

1) *Zeitintervall für ContactMe-Antwort*: z. B. '0'. Wartezeit des DLS-Client für den Empfang von ContactMe Messages vom DLS-Server. Die Wartezeit muss begrenzt sein, damit ContactMe Messages von böswilligen DLS-Servern nicht empfangen werden können.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Die geänderten Daten werden in die Konfiguration übernommen.

6.3.5.3 PIN Eingabe

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *PIN Eingabe* > *Eingabe der Bootstrap PIN*

Der Dialog Eingabe der Bootstrap PIN wird geöffnet. Sie können die Bootstrap PIN eingeben.

Klicken Sie auf Übernehmen, um die Änderungen zu speichern.

6.3.5.4 Bootstrapping zurücksetzen

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *Bootstrapping zurücksetzen* > DLS Client Bootstrapping zurücksetzen

Der Dialog *Bootstrapping zurücksetzen* wird angezeigt. Sie können DLS Client Bootstrapping zurücksetzen.

Klicken Sie auf *Bootstrapping zurücksetzen*.

6.3.5.5 DLSC kontaktieren

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC kontaktieren*

Der Dialog *DLSC kontaktieren* wird angezeigt. Klicken Sie auf *Kontakt*, um zu überprüfen, ob der DLS-Client immer noch verfügbar ist.

6.3.5.6 DLSC Client-Zertifikat

Dieser Ordner enthält das DLSC Client-Zertifikat mit dem privaten Schlüssel. Mit diesem Zertifikat weist sich der DLS-Client gegenüber dem DLS-Server aus. Per Default ist dieser Ordner leer. Während des Bootstrapping Mode bekommt der DLS-Client das Zertifikat vom DLS-Server.

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC Client-Zertifikat*

Zertifikat anzeigen

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC Client-Zertifikat* > *DLSC Client-Zertifikat*

Der Dialog *Zertifikatsinformationen* wird angezeigt. Sie erhalten folgende Informationen:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Alternativer Antragstellername*
- *Verschlüsselungsdaten mit öffentlichem Schlüssel*: *Länge des öffentlichen Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

6.3.5.7 DLSC CA-Zertifikate

Dieser Ordner enthält die vom DLS-Server während des Bootstrapping Mode gelieferten DLSC CA-Zertifikate.

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC CA-Zertifikate*

Zertifikat anzeigen

WBM-Pfad:

WBM > Konfiguration > Sicherheit > Deployment- und Licensing-Client (DLSC) > *DLSC CA-Zertifikate* > *DLSC CA-Zertifikat*

Der Dialog *Zertifikatsinformationen* wird angezeigt. Sie erhalten folgende Informationen:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*,

Beginn der Zertifikatsgültigkeit (GMT), *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*

- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name*: *(CN)*
- *Alternativer Antragstellername*
- *Verschlüsselungsdaten mit öffentlichem Schlüssel*: *Länge des öffentlichen Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

6.3.6 Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))

Die Funktion 'Signaling and Payload Encryption' (SPE, Signalisierungs- und Sprachverschlüsselung) verschlüsselt ankommende und abgehende VoIP Benutzer- und Signalisierungsdatenströme am Gateway. Dieses Leistungsmerkmal erfordert eine PKI (Public Key Infrastructure).

Die benötigten Zertifikate werden entweder von einer PKI-Zertifizierungsstelle (RA/CA) des Kunden oder von der internen Zertifizierungsstelle des DLS-Servers (CA) generiert. Anschließend sendet der DLS-Server die Dateien mit diesen Zertifikaten an den DLS-Client des Gateways.

Je nach den Anforderungen des Kunden können Sicherheitseinstellungen für die Zertifikatsevaluierung sowie für die Signalisierungs- und Sprachverschlüsselung konfiguriert, aktiviert oder deaktiviert werden. Dadurch steigt oder sinkt die Sicherheit.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signaling and Payload Encryption (SPE)*

Bei HG 3500 Klicken Sie auf das Pluszeichen (+) neben *Signaling and Payload Encryption (SPE)*, um die folgenden Einträge anzuzeigen:

1) *SPE Sicherheitseinstellung (nicht bei HG 3575)*

SPE Zertifikat (nicht bei HG 3575) SPE CA-Zertifikate(nicht bei HG 3575)

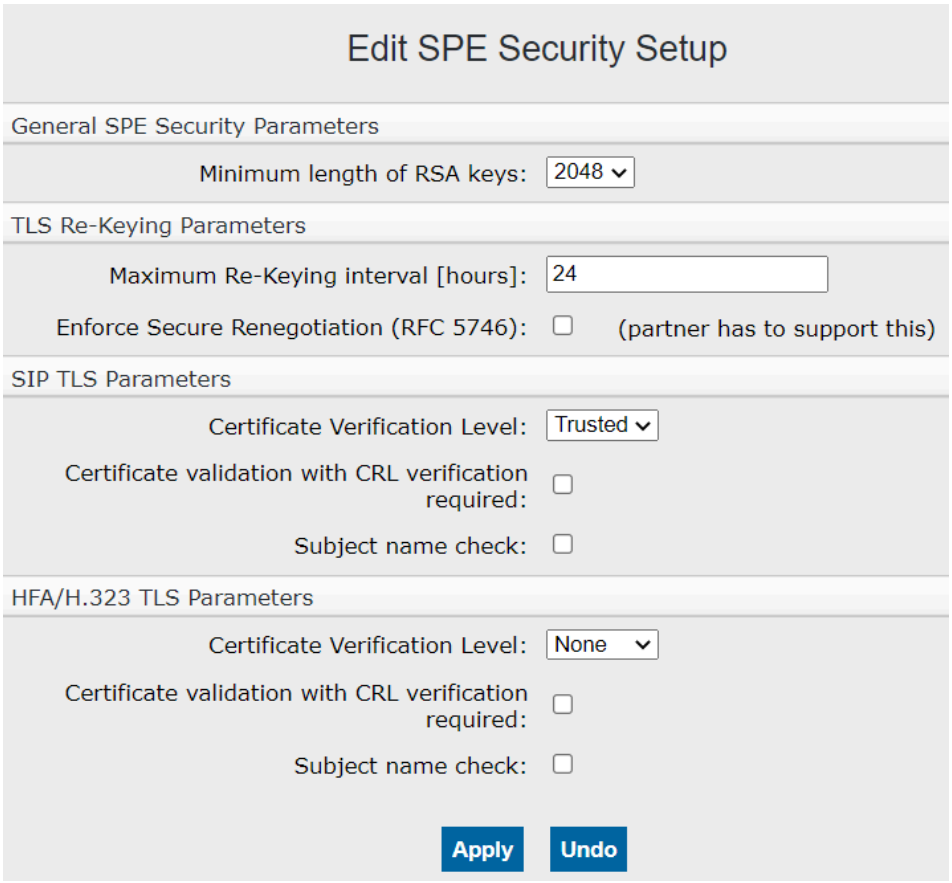
6.3.6.1 SPE Sicherheitseinstellung (nicht bei HG 3575)

Im Dialog *SPE Sicherheitseinstellung* werden Signaling and Payload Encryption (SPE)-Einstellungen für die Verschlüsselung der Signalisierung und der Sprachdaten zwischen den Gateways und den VoIP-Clients sowie zwischen zwei Gateways angezeigt.

Vorgehensweise:

Führen Sie zum Anzeigen der SPE-Sicherheitseinstellungen die folgenden Schritte durch:

1) Auswählen: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung* Das Dialogfeld *SPE Sicherheitseinstellung ändern* mit den folgenden Daten wird angezeigt:



6.3.6.2 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.

IMPORTANT: 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 aber kein Zertifikat haben, wählen Sie auf dem Gateway (auf dem TLS-Server dieser Schnittstelle) unter Certificate Verification Level (Zertifikatsprüfungsstufe) die Einstellung None. Der Client darf die Prüfungsstufe nicht auswählen. SPE kann nur aktiviert oder deaktiviert werden (das Serverzertifikat ist entweder ausgewählt oder nicht ausgewählt).

IMPORTANT: Für SIP-Q-Trunks ist die Certificate Verification Level-Einstellung None nicht zulässig, weil Mutual TLS obligatorisch ist.

IMPORTANT: Wenn bei nativen SIP-Trunks das Gateway über ein Zertifikat verfügt, sollte die Zertifikatsprüfungsstufe nicht auf None eingestellt werden, damit das empfangene Zertifikat geprüft wird.

IMPORTANT: 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:

WBM-Pfad:

Konfiguration **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung (nicht bei HG 3575)* **>** *SPE Sicherheitseinstellung ändern***>** SIP TLS Parameter

- 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 Erweiterungen geprüft. Wenn eine Erweiterung als kritisch gekennzeichnet ist und nicht erkannt wird, muss das Zertifikat zurückgewiesen werden. Und die korrekte Verwendung bekannter Erweiterungen wird geprüft (z. B. Grundlegende Einschränkungen, Verwendung des Schlüssels, Verwendung des erweiterten Schlüssels).
- Subject name check: Die Identität der Remote-Entity wird anhand ihres alternativen oder ihres allgemeinen Namens überprüft. Dieses Verhalten kann per Kontrollkästchen geändert werden.
- Es gibt optionale Prüfungen:

  Stufen Trusted und Full:
- Zertifikatsprüfung mit CRL-Prüfung erforderlich:
- Die Zertifikatssperrliste (CRL) gibt an, ob und warum ein Zertifikat gesperrt/widerrufen werden sollte. Wenn eine Zertifikats- oder Zertifizierungsstelle (CA) ein Zertifikat für ungültig erklärt, wird dessen Seriennummer in diese Liste eingetragen. Die Liste kann zur Prüfung von Zertifikaten von der Website der Zertifizierungsstelle heruntergeladen werden.

  Die Zertifikatskette darf keine widerrufenen Zertifikate enthalten. Dieses Verhalten kann per Kontrollkästchen geändert werden:

  WBM-Pfad:

  Konfiguration **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung*

(nicht bei HG 3575) **>** *SPE Sicherheitseinstellung ändern* **>** HFA/H.323 TLS Parameter **>** Zertifikatsprüfung mit CRL-Prüfung erforderlich

Stufe Full:

- Subject name check: Die Identität der Remote-Entity wird anhand ihres alternativen oder ihres allgemeinen Namens überprüft. Dieses Verhalten kann per Kontrollkästchen geändert werden:

WBM-Pfad:

Konfiguration **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung (nicht bei HG 3575)* **>** *SPE Sicherheitseinstellungen ändern* **>** HFA/H.323 TLS Parameter **>** Namensprüfung Antragsteller

6.3.6.3 Minimale Länge der RSA-Schlüssel

Legen Sie die minimale Länge des RSA-Schlüssels in dem vom der Remote Entity übertragenen Zertifikat fest. Je größer der Wert ist, desto sicherer ist der Schlüssel.

Die minimale Länge der im WBM festgelegten RSA-Schlüssel:

- 512 Bit

Die maximale Länge:

- 2048 Bit

WBM-Pfad:

Konfiguration > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE Sicherheitseinstellung (nicht bei HG 3575)* **>** *SPE Sicherheitseinstellungen ändern* **>** Minimale Länge der RSA-Schlüssel

6.3.6.4 Maximales Intervall für Schlüssel-Neuverhandlung

Die TLS-/SSL-Verbindungen bleiben permanent aktiv und werden in regelmäßigen Zeitabständen erneuert. Das Zeitintervall für die Schlüssel-Neuverhandlung stellen Sie im WBM ein:

- Maximal 72 Stunden
- Minimal 6 Stunden
- Deaktiviert 0 (NICHT EMPFOHLEN)

WBM-Pfad:

Konfiguration **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung (nicht bei HG 3575)* **>** *SPE Sicherheitseinstellungen ändern***>** *TLS Schlüssel-Neuverhandlung > TLS Intervall für die Schlüssel-Neuverhandlung [Stunden] > Maximales Intervall für die Schlüssel-Neuverhandlung*

6.3.6.5 Sichere Neuverhandlung erzwingen (RFC 5746)

TLS ist anfällig für Situationen, in denen ein böswilliger Server eine Verbindung zu einem Zielserver herstellt, diesen mit seinen eigenen manipulierten Daten füttert und dann die neue TLS-Verbindung von einem Client zuschaltet. Der Zielserver behandelt den anfänglichen TLS-Handshake des Clients als Neuverhandlung einer bestehenden Verbindung, die der böswillige Server zuvor hergestellt hat, und geht deshalb davon aus, dass die anfänglich vom Angreifer übertragenen Daten von derselben Entity stammen wie die nachfolgenden Client-Daten. Dieses Problem lässt sich durch eine sichere Neuverhandlung gemäß RFC 5746 vermeiden.

Aktivieren Sie diese Funktion nur, wenn alle über TLS verbundenen Remote-Entities die sichere Neuverhandlung (RFC 5746) unterstützen. Wenn eine Remote-Entity RFC nicht unterstützt, schlägt die Neuverhandlung fehl. In manchen Szenarien kann sogar der Aufbau der TLS-Verbindung fehlschlagen.

Dieses Verhalten kann per Kontrollkästchen geändert werden:

WBM-Pfad:

Konfiguration **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE Sicherheitseinstellung (nicht bei HG 3575)* **>** *SPE Sicherheitseinstellung ändern* **>** *TLS Schlüssel-Neuverhandlung* **>** *Sichere Neuverhandlung erzwingen (RFC 5746)*

6.3.6.6 SPE-Zertifikat (nicht für HG 3575)

Dieser Ordner enthält das SPE-Client-Zertifikat mit dem privaten Schlüssel und ist standardmäßig leer. Das Zertifikat muss zunächst importiert werden. Sie können dieses importierte Zertifikat einsehen und bei Bedarf ersetzen. Die Datei mit dem SPE-Zertifikat muss im Format PEM oder PKCS#12 vorliegen. Diese Datei stammt entweder von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder von der internen Zertifizierungsstelle (CA) des DLS-Servers.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* **>** *SPE-Zertifikat*

Ordner *SPE Zertifikat*:

SPE Zertifikat und privaten Schlüssel importieren (PEM oder PKCS#12)

NOTICE:

Der unterstützte Public Key Algorithmus für SPE-Zertifikate ist RSA mit einer Mindestschlüssellänge von 2048 Bit für HFA und SIP.

ECDSA wird für STMI- oder NCUI-Baugruppen nicht unterstützt.

SPE Zertifikat und privaten Schlüssel importieren (PEM oder PKCS#12)

In einer Datei, die im PEM oder im PKCS#12-Format vorliegen muss, sind die Daten eines Zertifikats und der zugehörige private Schlüssel gespeichert. Sie

können die entsprechende PEM- oder PKCS#12-Datei importieren, um dieses Zertifikat zu verwenden.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* **>** *SPE-Zertifikat (nicht für HG 3575)* **>** *SPE-Zertifikat plus privaten Schlüssel importieren (PEM oder PKCS#12)* **>** *SPE-Schlüsselzertifikat über HTTP laden*

Vorgehensweise:

Führen Sie zum Importieren des SPE-Zertifikats die folgenden Schritte durch:

1) Wählen Sie: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* **>** *SPE-Zertifikat (nicht für HG 3575)* **>** *SPE-Zertifikat und privaten Schlüssel importieren (PEM oder PKCS#12).* Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12)*: Geben Sie den Pfad und Namen der Datei an, die die zu importierenden Zertifikatsdaten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen.

NOTICE: Wenn Sie zum ersten Mal ein Zertifikat installieren, wenn SPE aktiviert ist, wird anschließend ein automatischer Reset durchgeführt.

---

2) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

Überprüfen Sie den Fingerabdruck (= Hexadezimalzahl). Der Fingerabdruck ändert sich immer, wenn ein Zertifikat geändert wurde. Ein unveränderter Fingerabdruck ist die einzige Garantie dafür, dass das Zertifikat authentisch ist. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall müssen Sie den Schlüssel vernichten und geeignete Maßnahmen ergreifen.

Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

1) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

SPE-Zertifikat anzeigen

Sie können z. B. ein SPE-Zertifikat anzeigen, wenn Sie es überprüfen möchten.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* **>** *SPE-Zertifikat (nicht für HG 3575)* **>** *SPE-Zertifikat (nicht für HG 3575) > SPE-Zertifikat (nicht für HG 3575)* **>** *(Linksklick) SPE-Zertifikat*

Vorgehensweise:

1) Wählen Sie: *WBM* > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* > *SPE-Zertifikat (nicht für HG 3575)* > *SPE-Zertifikat (nicht für HG 3575)* > *(Linksklick) SPE-Zertifikat*. Die Maske *Zertifikatsinformationen* wird angezeigt. Hier werden allgemeine Zertifikatsdaten (wie Name, Typ und Seriennummer), Informationen über den Aussteller und den Namen des Betreffs sowie Verschlüsselungsdaten angezeigt. Der verwendete öffentliche Schlüssel und der Fingerabdruck werden im hexadezimalen Format angezeigt.
2) Klicken Sie auf *OK*. Die Maske wird geschlossen.

SPE-Zertifikat löschen

Sie können z. B. ein SPE-Zertifikat entfernen, wenn Sie ein neues benötigen.

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* > *SPE-Zertifikat (nicht für HG 3575)* > *SPE-Zertifikat löschen*

Vorgehensweise:

1) Wählen Sie: *WBM* > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Nutzdatenverschlüsselung (SPE)* > *SPE-Zertifikat (nicht für HG 3575)* > *SPE-Zertifikat löschen*.
2) Eine Warnung wird angezeigt. Zu Prüfzwecken wird außerdem der Name des Zertifikats angegeben.
3) Klicken Sie in der Bestätigungsmaske auf *Löschen* und anschließend auf *OK*.

6.3.6.7 SPE CA-Zertifikate(nicht bei HG 3575)

Dieser Ordner enthält vertrauenswürdige SPE CA-Zertifikate. Sie können neue vertrauenswürdige SPE CA-Zertifikate importieren, bereits vorhandene ansehen und auch wieder löschen.

Das HG 3500 SIP und die vHG 3500 SIP unterstützen mehrstufige CA-Zertifikatshierarchien. Sie können also auch mehrstufige CA-Zertifikatshierarchien importieren. Beim Empfang einer Zertifikatskette von einem TLS Partner wird nun die gesamte empfangene Zertifikatskette verifiziert.

Bei Nutzung von mehrstufigen Zertifikatshierarchien müssen Sie

1) in den Ordner "SPE CA Zertifikate" die CA-Zertifikate aller Zwischenzertifizierungsstellen der Hierarchie des eigenen SPE Zertifikats importieren. Der Import des Zertifikats der Stammzertifizierungsstelle (RootCA) für das eigene Zertifikat ist optional. Beim TLS-Verbindungsaufbau wird dann das eigene Zertifikat zusammen mit der Kette der CA-Zertifikate gesendet.

Zusätzlich müssen Sie in den Ordner "SPE CA Zertifikate" die CA-Zertifikate aller derjenigen Stammzertifizierungsstellen importiert werden, die als vertrauenswürdig betrachtet werden sollen. Bei der Verifikation einer empfangenen Zertifikatskette werden die Root-CA-Zertifikate im Ordner "SPE CA Zertifikate" verwendet.

Die Reihenfolge des Imports der Zertifikate ist beliebig.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate*

Klicken Sie auf das Pluszeichen (+) neben *SPE CA-Zertifikate*, um die folgenden Einträge anzuzeigen:

1) Vertrauenswürdiges CA-Zertifikat importieren (PEM oder Binär-Format)

Vertrauenswürdiges CA-Zertifikat importieren (PEM oder Binär-Format)

Die vom DLS-Server gesendete PEM- oder Binär-Datei, die von einer Kunden PKI-Zertifizierungsstelle (RA/CA) oder der internen Zertifizierungsstelle (CA) des DLS-Servers stammt, kann außer dem SPE Zertifikat mit dem privaten Schlüssel bis zu 16 vertrauenswürdige CA-Zertifikate enthalten.

WBM-Pfad:

WBM **&gt** *Konfiguration* **&gt** *Sicherheit Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) SPE CA-Zertifikate(nicht bei HG 3575) Vertrauenswürdiges CA-Zertifikat importieren (PEM oder binär)*

Vorgehensweise:

Führen Sie zum Importieren eines vertrauenswürdigen CA-Zertifikats die folgenden Schritte durch:

1) Auswählen: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate(nicht bei HG 3575)* **>** *Vertrauenswürdiges CA-Zertifikat importieren (PEM oder binär)* Der Dialog *Laden eines SPE CA-Zertifikats über HTTP* wird angezeigt. Folgende Felder können bearbeitet werden:

2)
- *Datei mit Zertifikat (PEM oder Binär-Format)*: Geben Sie den Pfad und den Dateinamen der zu importierenden PEM- oder Binär-Datei ein. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen.
- *CRL-Verteilungspunktprotokoll (CDP):* Aktivieren Sie entweder das *LDAP*- oder das *HTTP*-Protokoll für den CDP. Ein CDP ist eine optionale Zertifikatserweiterung. Ein empfangenes Zertifikat wird nur gegen die CRLs geprüft, für die der CDP konfiguriert wurde.
- *CDP (ohne z. B. ldap://):* Geben Sie den CDP ein.

3) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

Prüfen Sie den Fingerabdruck (hexadezimale Zahl). Wenn ein Zertifikat verändert wurde, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden, darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.

Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

1) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

Klicken Sie auf das SPE CA-Zertifikat, um es anzuzeigen.

SPE CA-Zertifikat anzeigen

Sie können sich ein SPE CA-Zertifikat ansehen, z.B. um es zu überprüfen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate(nicht bei HG 3575)* **>** SPE CA-Zertifikate **>** *(Linksklick) SPE CA-Zertifikat*

Vorgehensweise:

1) Auswählen: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate(nicht bei HG 3575)* **>** SPE CA-Zertifikate **>** *SPE CA-Zertifikat*. Der Dialog *Zertifikatsinformationen* wird angezeigt. Sie erhalten Informationen über allgemeine Daten aus der Zertifikatsdatei wie Name, Typ und Seriennummer, Angaben über den Aussteller und den Antragsteller sowie Daten zur Verschlüsselung. Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.
2) Klicken Sie auf *OK*. Der Dialog wird geschlossen.

CDP und CRL anzeigen

Sie können sich mit dieser Funktion den CRL Distribution Point (CDP) einer Certificate Revocation List (CRL) anzeigen lassen.

In einer CRL kann man bereits herausgegebene Zertifikate für ungültig erklären, weil diese z.B. unsicher geworden sind.

Der CDP ist eine URI bzw. URL über die eine CRL zu einem Zertifikat zu finden ist (z.B. ldap://ldapserver.de/cdps/â¦).

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate(nicht bei HG 3575)* **>** SPE CA-Zertifikat **>** *Zertifikatsinformationen*

Vorgehensweise:

1) Auswählen: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))***>***SPE CA-Zertifikate(nicht bei HG 3575)* **>** SPE CA-Zertifikat **>** *Zertifikatsinformationen*. Der Dialog *Zertifikatsinformationen* wird angezeigt. Sie erhalten Informationen über allgemeine Daten aus der Zertifikatsdatei wie Name, Typ und Seriennummer, Angaben über den Aussteller und den Antragsteller sowie Daten zur Verschlüsselung. Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.
2) Klicken Sie auf *OK*. Der Dialog wird geschlossen.

Zertifikat für SPE löschen

Sie können ein zuvor importiertes SPE CA-Zertifikat löschen, z.B. wenn Sie ein neues Zertifikat benötigen.

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE CA-Zertifikate(nicht bei HG 3575)* > SPE CA-Zertifikate > *Zertifikat für SPE löschen*

Vorgehensweise:

1) *WBM* > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE CA-Zertifikate(nicht bei HG 3575)* > SPE CA-Zertifikate > *SPE CA-Zertifikat löschen*. Eine Warnung wird angezeigt. Zur Kontrolle wird außerdem der Name des Zertifikats angegeben.
2) Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

6.3.7 TLS-Chiffren für HTTPS

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > TLS-Chiffren für HTTPS

Das Protokoll TLSv1.3 mit Fallback auf TLSv1.2 wird ab V10 unterstützt, SSLv2 und SSLv3 sind aufgrund von Sicherheitsproblemen nicht zulässig.

TLSv1.0 wird nicht mehr unterstützt.

Die TLS-Version kann im WBM-Menü konfiguriert werden. Sie wird vom Webserver von HG 3500 / 3575 angeboten und unterstützt.

Standardmäßig ist TLS 1.3 mit Fallback auf 1.2 voreingestellt.

Die TLS-Version und für TLSv1.3 auch die Schlüsselverhandlungsmethode, der Verschlüsselungsalgorithmus und der AES-Betriebsmodus können konfiguriert werden. (Weitere Informationen zu TLSv1.3 finden Sie unter https://www.ietf.org/rfc/rfc5246.txt).

IMPORTANT: Nach dem Ändern und Speichern der TLS-Einstellungen muss das Gateway neu gestartet werden, damit die Änderungen in Kraft treten.

6.3.8 TLS-Chiffren für SIP

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > TLS-Chiffren für SIP

6.3.9 TLS-Chiffren für HFA

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > *TLS-Chiffren für HFA*

6.4 Netzwerk und Routing

Das Gateway verfügt über zwei LAN-Schnittstellen. Beide Schnittstellen können unabhängig voneinander konfiguriert werden.

Bei HG 3500 ist die zweite LAN-Schnittstelle in der Voreinstellung deaktiviert. Falls Sie die zweite LAN-Schnittstelle nutzen wollen, müssen Sie die Funktion aktivieren und festlegen, in welcher Betriebsart die Schnittstelle arbeiten soll.

Bei HG 3575 wird die zweite LAN-Schnittstelle ausschließlich als Redundanz für LAN1 zur Signalling-Survivability verwendet.

WBM-Pfad:

WBM > Konfiguration > *Netzwerk und Routing*

Die Baumstruktur für *Netzwerk und Routing* wird angezeigt:

1) *Netzwerkschnittstellen*

Routing

6.4.1 Netzwerkschnittstellen

WBM-Pfad:

WBM > Konfiguration > *Netzwerk und Routing* > *Netzwerkschnittstellen*

Einträge in der Baumstruktur *Netzwerkschnittstellen*:

1) *LAN1 (LAN1) LAN2 (Redundantes LAN1) [nur für HG 3500] LAN2 (Redundanz für LAN1, (LAN1-Spiegel)) [nur für HG 3575]*

Frontblende

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Netzwerkschnittstellen*

6.4.1.1 LAN1 (LAN1)

Sie können Details der LAN-Schnittstelle 1 konfigurieren. Die Funktion der ersten LAN-Schnittstelle ist vordefiniert: Die LAN1-Schnittstelle wird für den Anschluss HG 3500/3575 an das LAN verwendet.

Hintergrundinformationen:

Siehe Section 9.1, "Umgebungsanforderungen für VoIP" Siehe Section 9.2, "Bandbreitenbedarf in LAN/WAN-Umgebungen" Siehe Section 9.3, "Quality of Service (QoS)"

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Netzwerkschnittstellen* **>** *LAN1 (LAN1)* **>** *LAN1/Kunden-LAN*

Klicken Sie auf *LAN1 (LAN1)*, um die LAN1-Schnittstelle anzuzeigen

Sie können Detaildaten zur Verwendung der LAN1-Schnittstelle ansehen.

Der Dialog *LAN1/Kunden-LAN* wird angezeigt.

Sie können die Einstellungen zur Verwendung der LAN1-Schnittstelle bearbeiten.

Folgende Felder können bearbeitet werden:

- *Schnittstelle aktiviert*: Kreuzen Sie diese Option an, wenn diese Schnittstelle aktiviert werden soll.
- *IP-Adresse*: In diesem Feld wird die IP-Adresse der Schnittstelle angezeigt. Änderungen sind nicht möglich.
- *Subnetzmaske*: In diesem Feld wird die Subnetzmaske angezeigt. Änderungen sind nicht möglich.
- MAC Address (MAC-Adresse): Zur Information wird die MAC-Adresse der LAN1-Schnittstelle angezeigt.
- *Ethernet-Link-Modus*: In diesem Feld wird der Ethernet-Link-Modus angezeigt. Folgende Anzeigen sind möglich:
- – *Auto*: Automatisches Umschalten zwischen 10 und 100 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb
  – *10HDX*: 10 Mbit/s, Halbduplex
  – *10FDX*: 10 Mbit/s, Vollduplex
  – *100HDX*: 100 Mbit/s, Halbduplex
  – *100FDX*: 100 Mbit/s, Vollduplex

  IMPORTANT: Um die Funktionsfähigkeit des LAN sicherzustellen, müssen die Schnittstellenpartner identisch konfiguriert sein.

- *Max. Datenpaketlänge (Byte)*: In diesem Feld wird die maximale Paketlänge mit 1500 Byte angegeben. Sie kann über WBM geändert werden.
- *IEEE802.1p/q-Tagging*: Mit IEEE802.1p/q wird ermöglicht, dass sich mehrere virtuelle LANs ein gemeinsames physisches Netzwerk teilen. Das virtuelle LAN ist paketbasiert, im Gegensatz zu älteren portbasierten LANs. Im Datenbereich des Ethernet-Pakets befindet sich ein Tag, das definiert, zu welchem VLAN das Ethernet-Paket gehört und welche Priorität das Datenpaket hat.
- *IEEE802.1p/q-VLAN-ID*: Jedem VLAN wird eine eindeutige Nummer zugeordnet, die VLAN-ID. Alle Geräte, welche dieselbe VLAN-ID haben, können miteinander kommunizieren.

- Geben Sie als VLAN-ID einen vom Standardwert '0â abweichenden Wert ein, wenn der verwendete Switch Probleme mit dem Standardwert '0â hat.

  Dieses Feld ist nur sichtbar, wenn *IEEE802.1p/q-Tagging* angekreuzt ist.

  Layer 2-QoS-Klasse:

  – *Signalisierungsdaten*: Geben Sie einen Wert für die Priorität der Layer 2 QoS Klasse '*Signalisierungsdaten*â ein. Es sind Werte von 0 bis 7 erlaubt. Default = 3.
  – *Fax/Modem-Payload***:** Geben Sie einen Wert für die Priorität der Layer 2 QoS Klasse '*Fax/Modem-Payload'* ein. Es sind Werte von 0 bis 7 erlaubt. Default = 5.
  – *Netzwerksteuerung*: Geben Sie einen Wert für die Priorität der Layer 2 QoS Klasse 'Netzwerksteuerung' ein. Es sind Werte von 0 bis 7 erlaubt. Default = 0.
  – Sprach-Payload: Geben Sie einen Wert für die Priorität der Layer 2 QoS Klasse '*Sprach-Payload*' ein. Es sind Werte von 0 bis 7 erlaubt. Default = 5.

  Zugangspunkt Signalisierungskommunikation:
- *IP-Adresse des Zugangspunkts für die Signalkommunikation*: In diesem Feld wird die IP-Adresse des Access Points angezeigt. Änderungen sind nicht möglich.
- *Subnetzmaske des Zugangspunkts für die Signalkommunikation*: In diesem Feld wird die Subnetzmaske angezeigt. Änderungen sind nicht möglich.
- *Router des Zugangspunkts für Signalkommunikation*: In diesem Feld wird die IP-Adresse des Routers angezeigt. Änderungen sind nicht möglich.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

6.4.1.2 *LAN2 (Redundantes LAN1) [nur für HG 3500]*

Sie können Detaildaten zur Verwendung der LAN2-Schnittstelle eingeben.

Der Dialog *LAN2/Atlantic-LAN* wird angezeigt. Die Anzeige und die angebotenen Felder sind von der aktuellen Einstellung im ersten Feld *Das zweite LAN verwenden als* abhängig. Wählen Sie daher in diesem Feld zunächst die gewünschte Verwendung der LAN2-Schnittstelle aus. Folgende Einträge werden angeboten:

- *Nicht konfiguriert oder deaktiviert*: Verwenden Sie nicht die LAN2-Schnittstelle.
- *PPTP*: LAN2-Schnittstelle mit PPTP-Verbindung verwenden. (siehe Unterabschnitt *Ausgewählte Verwendungsart: PPTP*)
- *Redundanz für LAN1*: Wenn LAN1 ausfällt, dann übernimmt LAN2 dessen Funktion inklusive MAC- und IP-Adresse.
- *Management LAN*: Wird automatisch ausgewählt, wenn die Management-IP über AMO CGWB konfiguriert wurde.

Ausgewählte Verwendungsart: PPTP

Wenn Sie im Feld *Das zweite LAN verwenden als* den Eintrag *PPTP* ausgewählt haben, können Sie folgende Felder bearbeiten:

IP-Parameter

- *Partner-IP-Adresse der PPP-Verbindung*: Geben Sie in dieses Feld die IP-Adresse der Gegenseite der PPP-Verbindung ein. Wird diese PPP-Verbindung für den Internet-Zugang verwendet, muss der Eintrag nur erfolgen, wenn der Internet Service Provider eine statische IP-Adresse verwendet. Andernfalls lassen Sie den voreingestellten Wert 0.0.0.0 unverändert.
- *Lokale IP-Adresse der PPP-Verbindung*: Geben Sie in dieses Feld die IP-Adresse der lokalen HG 35xx-Baugruppe ein. Wird der voreingestellte Wert `0.0.0.0` nicht geändert, wird die IP-Adresse aus dem IP-Stack entnommen (IP-Adresse der LAN1-Schnittstelle). Wird diese PPP-Verbindung für den Internet-Zugang verwendet, muss der Eintrag nur erfolgen, wenn Ihnen der Internet Service Provider eine statische IP-Adresse zugeordnet hat. Andernfalls lassen Sie den voreingestellten Wert `0.0.0.0` unverändert.
- *Max. Datenpaketlänge (Byte)*: Geben Sie die maximale Paketlänge in Byte für das IP-Protokoll an. Der zulässige Wertebereich geht von 576 bis zu 1500 Byte.
- *IP-Adress-Aushandlung*: Wählen Sie aus, wie die IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau ausgehandelt werden soll.
- – Konfigurierte IP-Adresse nutzen: Nur die angegebene IP-Adresse wird verwendet.
  – Jede IP-Adresse akzeptieren: Jede angebotene IP-Adresse wird verwendet, auch wenn diese von der angegebenen abweicht.
  – Neue IP-Adresse anfordern: Vom Verbindungspartner wird eine neue IP-Adresse angefordert.

PPTP-Parameter

- Lokale IP-Adresse der Kontrollverbindung: Geben Sie die IP-Adresse des für PPTP-Verbindungen verwendeten HG 3500/3575 ein. Der Standardwert ist 192.0.2.4. Die Adressen 0.0.0.0 und 255.255.255.255 sind nicht erlaubt.
- Partner-IP-Adresse der Kontrollverbindung: Geben Sie die IP-Adresse des Hostrechners ein, zu dem die PPTP-Verbindung aufgebaut wird. Der Standardwert ist 192.0.2.4. Die Adressen 0.0.0.0 und 255.255.255.255 sind nicht erlaubt.
- Partner-Netzmaske der Kontrollverbindung: Geben Sie in diesem Feld die Netzmaske für die PPTP-Verbindung ein.

Authentifizierung

- PPP-Authentifizierung: Geben Sie an, ob eine Authentifizierung erfolgen soll. Bei angekreuzter Funktion wird die Parametermaske erweitert:
- – PPP-Benutzername: Geben Sie einen frei wählbaren Benutzernamen an, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
  – PAP-Authentifizierungsmodus: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (PAP-Client, PAP-Host, nicht benutzt).
  – PAP-Kennwort: Geben Sie das Kennwort ein, mit dem der Nutzer sich bei der Authentifizierung durch PAP identifiziert. Das Feld kann bei nicht genutzter PAP-Authentifizierung nicht beschrieben werden.
  – CHAP-Authentifizierungsmodus: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (CHAP-Client, CHAP-Host, CHAP-Client und -Host, nicht benutzt).
  – CHAP-Kennwort: Geben Sie das Kennwort ein, mit dem der Nutzer sich bei der Authentifizierung durch CHAP identifiziert. Das Feld kann bei nicht genutzter CHAP-Authentifizierung nicht beschrieben werden.

6.4.1.3 LAN2 (Redundanz für LAN1, (LAN1-Spiegel)) [nur für HG 3575]

WBM > *Konfiguration* > *Netzwerk und Routing* > *Netzwerkschnittstellen* > LAN2 (Redundanz für LAN1, (LAN1-Spiegel)) [nur für HG 3575] >

Bei HG 3575 wird die zweite LAN-Schnittstelle ausschließlich als Redundanz für LAN1 zur Signalling-Survivability verwendet.

Es werden für die LAN2-Schnittstelle folgende Einstellungen angezeigt:

- *IP-Adresse*: IP-Adresse
- *IP-Netzmaske*: Subnetzmaske
- *MAC-Adresse*: MAC-Adresse
- *Management LAN*: Wird automatisch ausgewählt, wenn die Management-IP über AMO CGWB konfiguriert wurde.
- *IEEE802.1p/q-Tagging*: Mit IEEE802.1p/q wird ermöglicht, dass sich mehrere virtuelle LANs ein gemeinsames physikalisches Netz teilen. Das virtuelle LAN ist paketbasiert, im Gegensatz zu älteren portbasierten LANs. Im Datenbereich des Ethernet-Pakets befindet sich ein Tag, das definiert, zu welchem VLAN das Ethernet-Paket gehört und welche Priorität das Datenpaket hat.
- *IEEE802.1p/q-VLAN-ID*: Jedem VLAN wird eine eindeutige Nummer zugeordnet, die VLAN-ID. Alle Geräte, welche dieselbe VLAN-ID haben, können miteinander kommunizieren.

6.4.1.4 Frontblende

Die Anzeige des Anschlussfeldes enthält Symbole, die direkten Zugang zum aktuellen Status wichtiger Hardware-Elemente und logischer Einheiten bieten.

WBM-Pfad:

WBM > *Konfiguration* > *Netzwerk und Routing* > *Netzwerkschnittstellen* > *Frontansicht*

Die einzelnen Elemente des Anschlussfeldes werden im folgenden beschrieben.

LAN (10/100 Base-TX)

Das Symbol zeigt den Betriebszustand der beiden LAN-Schnittstellen 1 und 2 an (oberes Feld: LAN1-Schnittstelle, unteres Feld: LAN2 Schnittstelle).

Table 2: Status der LAN-Schnittstellen

Symbol	Status
Grün	LAN ist aktiv
Rot	LAN ist nicht aktiv

Table 3: Kommunikationsstatus der LAN-Schnittstellen

	Status
Linkstatus	Das Verbindungskabel ist gesteckt Das Verbindungskabel ist nicht gesteckt.
Linkmodus	Voll/Halb-Duplex-Betrieb
Linkgeschwindigkeit	100/10 Mbit/s Übertragungsrate

6.4.2 Routing

In kleinen Netzen kann eine Routing-Tabelle auf jedem Router vom Netzwerkadministrator manuell gepflegt werden. In größeren Netzen wird diese Aufgabe mithilfe eines Protokolls automatisiert, das Routing-Informationen im Netz verteilt.

Ein IP-Paket kann viele Router überqueren, bevor es sein Ziel erreicht. Sein Weg wird nicht von einer zentralen Instanz bestimmt, sondern von den Routing-Tabellen in den einzelnen Routern auf dem Weg. Jeder Router legt nur den nächsten Schritt auf dem Weg fest und verlässt sich darauf, dass die nachfolgenden Router das Paket richtig weiterleiten.

Konfigurierbar sind im HG 3500/3575 das IP-Routing, IP-Mapping, NAT, PSTN-Routing und SCN-Routing.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing*

Die Baumstruktur für *Routing* wird angezeigt.

Einträge in der Baumstruktur *Routing*:

1) *IP-Routing PSTN (nur für HG 3500)*

Wahlparameter

6.4.3 IP-Routing

Im HG 3500/3575 sind statische Routen sowie ein Default Router konfigurierbar. Ferner werden Diagnose- und Überwachungs-Tools für das Routing angeboten.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing*

In der Baumstruktur werden folgende Untereinträge angezeigt:

1) *Statische Routen Default Router DNS-Server (nicht für HG 3575) Address Resolution Protocol Routen-Tabelle ICMP-Anforderung*

6.4.3.1 Statische Routen

Das HG 3500/3575 unterstützt ausschließlich statische Routen. Statische Routen verbinden zwei Geräte miteinander. Sie werden manuell angelegt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing* **>** *Statische Routen* **>** *Statische Routentabelle*

Klicken Sie auf das Pluszeichen (+) neben *Statische Routen*, um die folgenden Einträge anzuzeigen:

1) *Statische Route hinzufügen*

Statische Routen:

Wenn bereits statische Routen hinzugefügt wurden (siehe Section 7.4.3.4, "Statische Route hinzufügen"), wird *Statische Routen* in der statischen Routentabelle dargestellt. In diesem Fall können Sie durch einen Klick auf *Statische Routen* in der Baumstruktur eingerichtete statische Routen sehen.

6.4.3.2 Automatische statische Routen

Statische Routen werden automatisch erstellt, wenn das Management LAN bereits konfiguriert ist und MGNTIP oder BUSIP anschließend über den AMO AENDERN-CGWB Typ=MGNTDATA eingerichtet wurden.

Wenn MGNTIP=0.0.0.0 oder BUSIP=0.0.0.0, werden die statischen Routen automatisch gelöscht.

Den erstellten statischen Routen wird ein fester Index von 1001 oder 1002 zugewiesen. Der mit dem festen Index 1001 verbundene Routenname ist Assistant_IP. Der Routenname für den festen Index 1002 lautet Backup_Server_IP.

NOTICE: Änderungen der automatischen statischen Routen im WBM werden über den AMO AENDERN-CGWB TYP=MGNTDATA überschrieben

---

Die automatischen statischen Routen werden im WBM angezeigt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Routing* **>** *IP-Routing* **>** *Statische Routen* **>** *Statische Routentabelle*

6.4.3.3 Statische Routentabelle

Sie können eine Tabelle mit allen angelegten statischen Routen ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Routing* **>** *IP-Routing* **>** *Statische Routen* **>** *Statische Routentabelle*

Der Dialog *Statische Routentabelle* wird angezeigt. Feldbeschreibungen siehe Section 7.4.3.4, "Statische Route hinzufügen".

6.4.3.4 Statische Route hinzufügen

Sie können eine neue statische Route zwischen zwei IP-Geräten anlegen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Routing* **>** *IP-Routing* **>** *Statische Routen* **>** *Statische Route hinzufügen*

Der Dialog *Statische Route hinzufügen* wird angezeigt. Die Anzeige *Route-Index* kennzeichnet die laufende Nummer der Route. Folgende Felder können bearbeitet werden:

- *Route-Name*: Der Name der statischen Route. Geben Sie eine Zeichenkette ein.
- *Ziel-Netzwerk/Host*: Die IP-Adresse des Ziel-Netzwerks.
- *Subnetzmaske*: Die Subnetzmaske des Ziel-Netzwerks.
- *Route-Gateway*: Die IP-Adresse des nächsten Routers auf dieser Route oder die IP-Adresse der lokalen oder entfernten Schnittstelle eines PSTN-Partners.

Der Route-Index wird automatisch vergeben und nur zu Ihrer Information angezeigt. Änderungen sind nicht möglich.

Klicken Sie abschließend auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Die Änderungen werden automatisch gespeichert.

Sie können vorhandene statische Routen löschen. Zur Kontrolle werden die Daten der zu löschenden statischen Route angezeigt.

6.4.3.5 Default Router

Um sicherzustellen, dass das Gateway auch Ziele erreicht, die nicht explizit in einer Routingtabelle aufgeführt sind, muss ein Gateway für die Weiterleitung solcher Pakete (Default Router) angegeben sein.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing* **>** *Default Router*

Sie können die aktuellen Einstellungen des Default Routers ansehen.

Der Dialog *Default Router* wird angezeigt. Es werden die aktuellen Einstellungen des Default Routers angezeigt:

- *Default-Routing über:* Es wird angezeigt, über welches Netzwerk, z. B. LAN, der Default Router erreichbar ist.
- *IP-Adresse des Default Routers* Es wird die IP-Adresse des Default Routers angezeigt.

6.4.3.6 DNS-Server (nicht für HG 3575)

Sie können die IP-Adressen des bevorzugten und des alternativen DNS-Servers ansehen (DNS: Domain Name System). DNS-Server werden zur Namensauflösung verwendet, d. h. zur Umsetzung von alphanumerischen IP-Adressen in numerische IPv4 oder IPv6-Adressen, die von einem Computer verarbeitet werden können.

WBM-Pfad:

WBM > Konfiguration > *Netzwerk und Routing* **>** Routing > IP-Routing > DNS-Server (nicht für HG 3575) > *DNS-Einstellungen*

Das Fenster *DNS-Einstellungen* erscheint. Es werden die aktuellen Einstellungen für den DNS-Server angezeigt:

- *IP-Adresse des bevorzugten DNS-Servers:* Zeigt die IP-Adresse des bevorzugten DNS-Servers.
- *IP-Adresse des sekundären DNS-Servers:* Zeigt die IP-Adresse des alternativen DNS-Servers.

6.4.3.7 Address Resolution Protocol

Zur Kontrolle können Sie Daten des Address Resolution Protocol (ARP) ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing* **>** *Address Resolution Protocol* **>** *ARP-Protokoll*

Sie können die Daten des Address Resolution Protocol (ARP) als Tabelle ansehen.

Der Dialog *ARP-Protocol* erscheint. Es wird eine Tabelle mit den Spalten 'IP-Adresse', 'MAC-Adresse', 'Typâ und 'Schnittstelleâ angezeigt.

6.4.3.8 Routen-Tabelle

Diese Funktion zeigt die Routen-Tabelle des Betriebssystems an.

WBM-Pfad:

WBM > Konfiguration >*Netzwerk und Routing* > Routing > IP-Routing > Routen-Tabelle > *Routen-Tabelle anzeigen*

Das Fenster *Routen-Tabelle anzeigen* wird angezeigt. Nach Klicken auf die Schaltfläche *Senden* bzw. *Senden (in eigenem Fenster)* wird die Routen-Tabelle des Betriebssystems angezeigt.

6.4.3.9 ICMP-Anforderung

Zur Kontrolle können Sie ping- und traceroute-Befehle absetzen, um das Routing zu testen.

WBM-Pfad:

WBM > Konfiguration > *Netzwerk und Routing* > Routing > IP-Routing > *ICMP-Anforderung*

Klicken Sie auf das Pluszeichen (+) neben *ICMP-Anforderung*, um die folgenden Einträge anzuzeigen:

1) *Ping Traceroute*

6.4.3.10 Ping

Zur Kontrolle können Sie einen ping-Befehl absetzen, um das Routing zwischen dem HG 3500/3575 und einer frei wählbaren Zieladresse zu testen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing* **>** *ICMP-Anforderung* **>** *Ping*

Es wird die Netzwerkverbindung zwischen HG 3500/3575 und Zieladresse des zu überprüfenden Hosts überprüft. Dabei wird ein ICMP-'Echo-Request'-Paket an die Zieladresse gesendet. Der Empfänger muss, sofern er das Protokoll unterstützt, ein ICMP-'Echo-Reply'-Paket zurücksenden. Diese Antwortpakete werden zusammen mit den Umlaufzeiten angezeigt.

Der Dialog *Ping* wird angezeigt. Folgende Felder können Sie bearbeiten:

- *Zieladresse*: Adresse, an die mit einem Ping eine Anfrage gestellt werden soll.
- *Anzahl zu sendender Echoanforderungen*: Geben Sie an, wie viele Paketanforderungen ausgetauscht werden sollen. Übliche Werte sind 3 oder 4.

Klicken Sie auf *Senden* oder *Senden (in eigenem Fenster)*.

Das Ergebnis der Ping-Anforderung wird ausgegeben.

Die folgenden Schaltflächen sind im Ausgabebereich vorhanden: *Kleiner* reduziert die Schriftgröße in der Ausgabe. *Größer* erhöht die Schriftgröße in der Ausgabe. *Neu laden* startet die Ping-Anforderung erneut.

6.4.3.11 Traceroute

Zur Kontrolle können Sie einen traceroute-Befehle absetzen, um das Routing zu testen. Das Traceroute überprüft die Netzwerkverbindung zwischen HG 3500/3575 und der Zieladresse mittels ICMP-Echoanforderungs-Paketen. Die ICMP-Echoanforderungs-Pakete werden mit unterschiedlichen, ansteigenden TTL-Werten (Time-To-Live) gesendet. Die Antwortquittungen werden zusammen mit den Umlaufzeiten angezeigt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *IP-Routing* **>** *ICMP-Anforderung* **>** *Traceroute*

Sie können das Traceroute-Kommando zum Testen des Routings starten.

Der Dialog *Traceroute* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Zieladresse*: Geben Sie die IP-Adresse des Ziels ein. Zwischen dem HG 3500/3575 und dieser Zieladresse wird die Traceroute ermittelt.
- *TOS-Byte*: Geben Sie ein, ob TOS-Bytes gesendet werden sollen (TOS = Type-of-Service). TOS-Bytes geben Aufschluss über die Qualität eines Dienstes.

Klicken Sie auf *Senden* oder *Senden (in eigenem Fenster)*.

Das Ergebnis der Traceroute-Anforderung wird ausgegeben.

Die folgenden Schaltflächen sind im Ausgabebereich vorhanden: *Kleiner* reduziert die Schriftgröße in der Ausgabe. *Größer* erhöht die Schriftgröße in der Ausgabe. *Neu laden* startet die Traceroute-Anforderung erneut.

6.4.4 PSTN (nur für HG 3500)

PSTN steht für **P**ublic **S**witched **T**elephone **N**etwork, also für das öffentliche Fernsprechnetz.

Partner, die über analoge oder ISDN-Verbindungen erreicht werden sollen, müssen als PSTN-Partner konfiguriert werden. Die Einwahl ins Firmennetz geschieht üblicherweise über die Router-Rufnummer. Anhand der übermittelten Rufnummer wird der Partner identifiziert. Für jeden Partner, der keine Rufnummer übermittelt, muss eine eindeutige MSN konfiguriert werden, welche anstelle der Router-Rufnummer gewählt wird.

Zum Transport von IP-Paketen über analoge oder ISDN-Verbindungen verwendet das HG 3500/3575 das Point-to-Point Protokoll (PPP).

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)*

Klicken Sie auf das Pluszeichen (+) neben PSTN, um die folgenden Einträge anzuzeigen:

1) *Globale PSTN-Daten ändern*

PPP-Protokoll (Laden über HTTP)

PPP-Protokoll löschen PSTN-Partner

6.4.4.1 Globale PSTN-Daten ändern

Sie können die Basis-PSTN-Konfigurationsdaten des HG 3500/3575 zu Rufnummer, Wahlwiederholung und Scripting ansehen.

Sie können die Basis-PSTN-Konfigurationsdaten des HG 3500/3575 zu Rufnummer, Wahlwiederholung und Scripting bearbeiten.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** Globale PSTN-Daten ändern **>** *Globale PSTN-Daten*

Der Dialog *Globale PSTN-Daten* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Router-Rufnummer*: Wählen Sie im Auswahlmenü die Durchwahl des Systems OpenScape 4000 V10 aus. Alle Anwendungen, die die Routerfunktion nutzen, sind unter dieser Durchwahl von außen erreichbar. Externe Routingpartner, die keine Rufnummer übermitteln, müssen jeweils andere Rufnummern benutzen. Diese Rufnummern werden als MSN konfiguriert.
- *Anzahl Wahlwiederholungen*: Geben Sie an, wie viele Wiederholungsversuche das HG 3500/3575 zum Aufbau einer Verbindung unternehmen soll.
- *Wahlwiederholungspause (s)*: Geben Sie die Pausendauer zwischen den Wahlwiederholungsversuchen in Sekunden ein.

6.4.4.2 PPP-Protokoll (Laden über HTTP)

Sie können das PPP-Logfile des Gateways über HTTP laden und es auf dem Gateway löschen. Das Logfile enthält Daten über Authentifizierungsfehler bei PAP oder CHAP. Wenn das Logfile gelöscht wurde, wird es automatisch neu angelegt und beschrieben.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** PPP-Protokoll (Laden über HTTP)

Sie können das PPP-Logfile des Gateways über HTTP laden.

Ein Hinweis wird angezeigt, den Sie mit *OK* bestätigen müssen. Je nach Einstellung des Browsers wird nun ein weiterer Dialog angezeigt, in dem Sie entscheiden können, ob Sie das heruntergeladene Logfile speichern oder gleich im Default-Editor öffnen möchten.

6.4.4.3 PPP-Protokoll löschen

Sie können das PPP-Logfile auf dem Gateway löschen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PPP-Protokoll löschen*

Ein wichtiger Warnhinweis wird angezeigt.

Klicken Sie auf *Protokoll löschen* und im Bestätigungsdialog auf *OK*.

6.4.4.4 PSTN-Partner

Es können bis zu 70 Partner konfiguriert werden. Jede Einstellung beschreibt eine PSTN-Gegenstelle, die sich über OpenScape 4000 V10 in das Firmennetz einwählt oder vom Firmennetz erreicht werden soll. Die Einwahl in das Firmennetz geschieht normalerweise über die Router-Rufnummer, wobei die übertragene Rufnummer überprüft wird. Wird keine Rufnummer übermittelt, kann als Einwahl eine MSN für einen PSTN-Partner konfiguriert werden.

Ab Werk ist bereits ein Default-PSTN-Partner konfiguriert, dessen Einträge bei jeder Neukonfiguration eines weiteren Partners in die Eingabemaske übernommen werden. Durch Änderung der Werksangaben des Default PSTN-

Partners können Sie einen eigenen, benutzerspezifischen Vorgabedatensatz erstellen.

Die Symbole für den Default-PSTN-Partner und dessen Rufnummer sind blau dargestellt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PSTN-Partner*

Klicken Sie auf das Pluszeichen (+) neben PSTN-Partner, um die folgenden Einträge anzuzeigen:

1) *PSTN-Partner hinzufügen*

Sie können einzelne PSTN-Partner und den Default-PSTN-Partner bearbeiten. Jeder Eintrag unterhalb von *PSTN-Partner* steht für einen eingerichteten PSTN-Partner.

Wenn für einen selbst hinzugefügten PSTN-Partner (siehe auch Section 7.4.4.6, "Rufnummer hinzufügen") bereits eine Rufnummer hinzugefügt wurde, wird der Eintrag des PSTN-Partners als Ordner dargestellt. Per Klick auf den PSTN-Partner-Namen können Sie den Ordnerinhalt anzeigen. Jeder Eintrag unterhalb des geöffneten Ordners steht für eine dem PSTN-Partner zugewiesene Rufnummer.

6.4.4.5 PSTN-Partner hinzufügen

Sie können einen neuen PSTN-Partner anlegen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** PSTN-Partner **>** *PSTN-Partner hinzufügen*

Der Dialog *PSTN-Partner hinzufügen* wird angezeigt. Folgende Felder können bearbeitet werden:

- *Name des Partners*: Geben Sie einen frei wählbaren Namen für den PSTN-Partner an. Das Feld akzeptiert bis zu 14 Zeichen.
- *Art der PSTN-Verbindung*: Wählen Sie aus, ob die PSTN-Verbindung eingerichtet werden soll (Auswahl *Aktiv*). Wenn Sie *Nicht konfiguriert* wählen, können Sie den PSTN-Partner vorkonfigurieren. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung jedoch verhindert.

IMPORTANT: Die Optionen *Default Router*, *Internet-Zugang mit DNS-Abfrage* und *NAT* (Beschreibungen siehe weiter unten) können nur für **einen** aktiven PSTN-Partner aktiviert werden.

IP-Parameter:

- *IP-Adresse des PSTN-Partners*: Geben Sie in dieses Feld die IP-Adresse des PSTN-Partners ein. Wird diese PPP-Verbindung für den Internet-Zugang verwendet, muss der Eintrag nur erfolgen, wenn der Internet Service Provider eine statische IP-Adresse verwendet.
- *IP-Adresse der lokalen PSTN-Schnittstelle*: Geben Sie in dieses Feld die IP-Adresse der lokalen PSTN-Schnittstelle ein. Wird diese PPP-Verbindung für

den Internet-Zugang verwendet, muss der Eintrag nur erfolgen, wenn Ihnen der Internet Service Provider eine statische IP-Adresse zugeordnet hat.

- *Max. Datenpaketlänge (Byte)*: Geben Sie die maximale Paketlänge in Byte für das IP-Protokoll an. Der Wertebereich geht von 576 bis zu 1500 Byte.
- *IP-Adress-Aushandlung*: Wählen Sie aus, wie die IP-Adresse zwischen HG 3500/3575 und dem PSTN-Partner beim Verbindungsaufbau ausgehandelt werden soll. Es stehen die folgenden Optionen zur Verfügung:
- – *konfigurierte IP-Adresse nutzen*
  – *jede IP-Adresse akzeptieren*
  – *neue IP-Adresse anfordern*

Allgemeine PPP-Parameter:

- *MSN-/Durchwahl*: In diesem Feld können Sie eine MSN-Nummer konfigurieren.

IMPORTANT: Übermittelt der Partner seine Rufnummer, so muss diese konfiguriert sein, sonst wird der Ruf abgewiesen. Sind hingegen Rufnummern des Partners konfiguriert, aber der Partner übermittelt keine, so kommt die Verbindung trotzdem zustande.

- *B-Kanäle*: Geben Sie die Anzahl der verwendeten B-Kanäle an.
- *Rückruf*: Geben Sie an, ob ein Anruf abgelehnt und der Partner danach sofort zurückgerufen werden soll. Dies verhindert das Einwählen von nicht autorisierten Gegenstellen. Die anrufende Stelle muss im D-Kanal der ISDN-Verbindung die Rufnummer übertragen und die Einwahl durch das HG 3500/3575 erlauben. Beim PSTN-Partner muss diese Rufnummer mit gehender Richtung konfiguriert sein.

IMPORTANT: Ist Rückruf aktiviert, werden nur gehende Verbindungen von diesem Partner akzeptiert. Ist die Gegenstelle ebenfalls ein Gateway, und ist für diese Verbindung ebenfalls Rückruf aktiviert, kann keine Verbindung aufgebaut werden, weil keiner der Partner einen einkommenden Verbindungsaufbau akzeptiert. Ist bei einer solchen Fehlkonfiguration nur Rückruf ohne Wahlwiederholung aktiviert, so kann sie erkannt werden, und ein ständiger Verbindungsaufbau wird unterdrückt. Ist jedoch Wahlwiederholung aktiviert, wird das Problem nicht erkannt.

- *LCP-Echo-Anforderung senden*: Geben Sie an, ob eine LCP Echo-Anforderung gesendet werden soll. Diese Funktion dient der Prüfung, ob die Verbindung noch aktiv ist.

Short-Hold:

- *Short-Hold-Modus*: Geben Sie an, ob für die PPP-Verbindung die Betriebsart 'Short Hold' ein- oder ausgeschaltet sein soll. Die nachfolgenden Eingaben sind nur bei eingeschaltetem Short-Hold Modus möglich:
- – *Short-Hold-Zeit (s)*: Geben Sie die Zeit ohne Datenübertragungen an, nach der die PPP-Verbindung getrennt werden soll. Der zulässige Wertebereich liegt zwischen 10 und 9999 Sekunden. Der Shorthold-Timer wird nur von ausgehenden Paketen getriggert (HG 3500/3575 an den PSTN-Partner). Um hängende Verbindungen zu vermeiden, sollte der SHORT

HOLD-Modus eingeschaltet und auf einen Wert von 120 Sek. gesetzt werden.

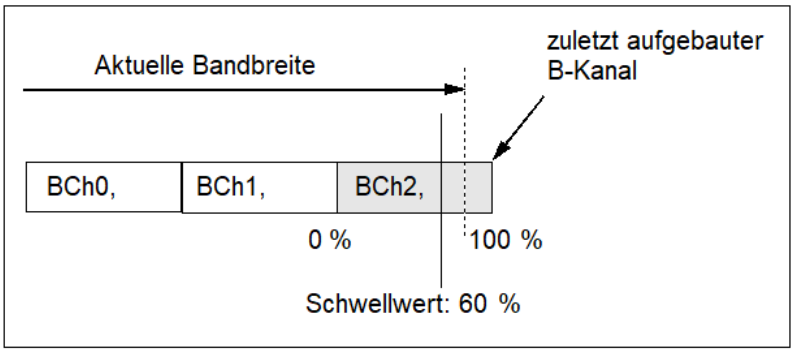
Authentifizierung:

- *PPP-Authentifizierung*: Geben Sie an, ob eine Authentifizierung erfolgen soll. Bei angekreuzter Funktion wird die Parametermaske erweitert:
- – *PPP-Benutzername*: Geben Sie einen frei wählbaren Benutzernamen an, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
  – *PAP-Authentifizierungsmodus*: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (*PAP-Client*, *PAP-Host*, *nicht benutzt*).
  – *CHAP-Authentifizierungsmodus*: Geben Sie an, welche Authentifizierung für die PPP-Verbindung genutzt werden soll (*CHAP-Client*, *CHAP-Host*, *CHAP*-Client und -Host, *Nicht benutzt*).

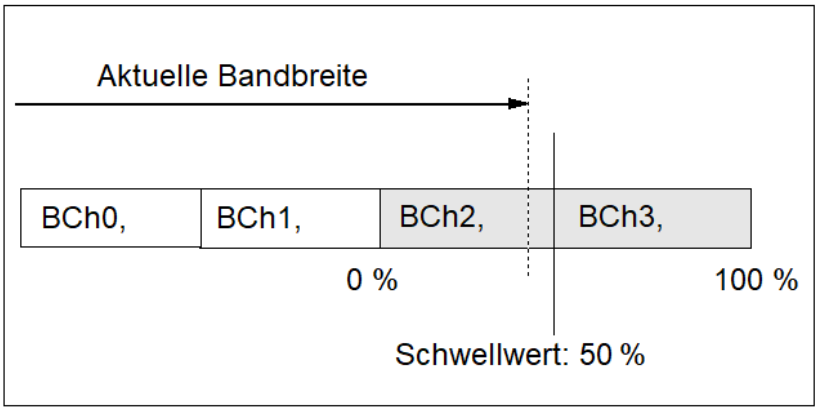
Multi-Link:

- *Multi-Link*: Geben Sie an, ob Kanalbündelung auf dieser PPP-Verbindung möglich sein soll. Die folgenden Eingaben sind nur bei eingeschaltetem Multi-Link möglich:
- – *Kanal-Zuweisung*: Geben Sie an, ob für diese PPP-Verbindung die Kanalanforderung statisch oder dynamisch erfolgen soll. Bei der statischen Kanal-Zuweisung wird die gewünschte Anzahl der Kanäle zu Beginn der Verbindung aufgebaut (siehe allg. PPP-Parameter: B-Kanäle). Steht die gewünschte Anzahl der B-Kanäle Richtung System nicht zur Verfügung (z. B. wegen Belegung durch Anrufe), wird nur die maximal verfügbare Anzahl der B-Kanäle aufgebaut. B-Kanäle, die zu einem späteren Zeitpunkt frei werden, können zu dieser Multilink-Verbindung nicht mehr hinzugefügt werden. Dazu ist ein komplett neuer Verbindungsaufbau notwendig. Bei der dynamischen Kanal-Zuweisung werden in Abhängigkeit der genutzten Bandbreite zusätzliche B-Kanäle aufgebaut oder bereits belegte B-Kanäle abgebaut. Die maximal gewünschte Anzahl der B-Kanäle für diese Multilink-Verbindung wird im Feld 'B Kanäle' unter den allgemeinen PPP-Parametern festgelegt. Auch hier können, wie beim statischen Multilink, weniger B-Kanäle zur Verfügung stehen, als gewünscht. Im Gegensatz zum statischen Multilink können jedoch frei gewordene B-Kanäle für die Multilink-Verbindung genutzt werden, wenn gleichzeitig der Bandbreitenbedarf hoch genug ist. Der Auf- und Abbau von B-Kanälen wird mithilfe der Einstellungen zum oberen und unteren Multi-Link-Schwellenwert sowie zur oberen und unteren Multi-Link-Zeitbegrenzung kontrolliert. Die Anzahl der aktuell belegten B-Kanäle kann über die Device-Statistiken abgefragt werden.
  – *Segmentierung*: Wenn Sie diese Option aktivieren, werden IP-Pakete in mehrere Fragmente aufgeteilt. Die Fragmente werden über verschiedene B-Kanäle einer Multilink-Verbindung übertragen und auf der Empfangsseite wieder in die ursprünglichen IP Pakete zusammen gesetzt. Die Aktivierung der Segmentierung führt zu kürzeren Übertragungszeiten von IP-Paketen und einer gleichmäßigeren Auslastung der B-Kanäle. Die Segmentierung sollte bei Spachdatenübertragung in Multilink-Verbindungen unbedingt aktiviert werden, um den Jitter zu verringern und damit die Sprachqualität zu verbessern.
  – *Oberer Multi-Link-Schwellwert (%)*: Dieser Wert legt die Schwelle fest, ab der ein weiterer B-Kanal zugeschaltet wird. Die Schwelle bezieht sich

dabei auf die rechnerische Auslastung des zuletzt aufgebauten B-Kanals. Der einstellbare Wertebereich liegt zwischen 51 und 100 %.



- *Obere Multi-Link-Zeitbegrenzung (s)*: Geben Sie an, wie lange die obere Schwelle der Übertragungsrate überschritten sein muss, bis ein weiterer B-Kanal zugeschaltet wird (Kanalbündelung). Der zulässige Wertebereich liegt zwischen 10 und 60 Sekunden.
- *Unterer Multi-Link-Schwellwert (%)*: Dieser Wert legt die Schwelle fest, ab der ein B-Kanal abgebaut wird. Die Schwelle bezieht sich dabei auf die rechnerische Auslastung der beiden zuletzt aufgebauten B-Kanäle. Der einstellbare Wertebereich liegt zwischen 20% und 80%.



- *Untere Multi-Link-Zeitbegrenzung (s)*: Geben Sie an, wie lange die untere Schwelle der Übertragungsrate unterschritten sein muss, bis ein zusätzlich geschalteter B-Kanal wieder abgeschaltet wird. Der zulässige Wertebereich liegt zwischen 10 und 60 Sekunden.

6.4.4.6 Rufnummer hinzufügen

Zu jedem PSTN-Partner können bis zu fünf Rufnummern konfiguriert werden. Bei Übermittlung der Rufnummer wird diese überprüft und es werden nur Anrufe entgegengenommen, wenn für die eingehende Rufnummer ein PSTN-Partner mit der entsprechenden Rufberechtigung definiert ist.

Sind allgemeine Wahlparameter (siehe Section 7.4.5, "Wahlparameter") konfiguriert, so werden diese bei der Konfiguration und der Rufnummernüberprüfung mit ausgewertet. Alle Rufnummern werden in das niedrigste implizite Format umgewandelt.

Beispiel:

Es werden folgende allgemeine Wahlparameter verwendet:

Internationales Präfix= 000	Länderkennung = 49
Nationaler Präfix = 00	Vorwahl = 89
Präfix für Amtsholung = 0	Anschlussnummer = 722

Unabhängig vom Format der übermittelten Rufnummer ('0722 123' oder '0089722123' oder '000 49 89 722 123') werden alle auf '123' als das niedrigste implizite Format umgewandelt.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PSTN-Partner* **>** gewünschter PSTN-Partner **>** *Rufnummer hinzufügen*

Der Dialog *PSTN-Rufnummer hinzufügen* wird angezeigt. Sie können folgende Einträge ändern:

- *Rufnummer*: Geben Sie die Rufnummer an, unter der ein PSTN-Partner erreichbar ist. Sie muss innerhalb der Gesamtkonfiguration eindeutig sein und kann aus bis zu 22 Dezimalziffern (0 bis 9) bestehen. Es können Bindestriche verwendet werden.
- *Rufrichtung*: Geben Sie an, wie die Verbindung unter dieser Rufnummer zustande kommen darf.
- – *Gesperrt*: Die Nummer ist nicht verwendbar.
  – *Kommend*: Der Partner darf anrufen, aber nicht angerufen werden.
  – *Gehend*: Der Partner darf angerufen werden, aber nicht anrufen.
  – *Kommend und gehend*: Der Partner darf anrufen und angerufen werden.

  Klicken Sie auf *Übernehmen*. Ein Hinweis wird angezeigt, den Sie mit *OK* bestätigen müssen. Ebenso müssen Sie im Bestätigungsdialog auf *OK* klicken.

6.4.4.7 Rufnummer anzeigen

Sie können eine Rufnummer zu einem PSTN-Partner und deren Rufrichtung ansehen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PSTN-Partner* **>** gewünschter PSTN-Partner **>** gewünschte Rufnummer **>** *PSTN-Rufnummer*

Der Dialog *PSTN-Rufnummer* wird angezeigt. Feldbeschreibungen siehe Section 7.4.4.6, "Rufnummer hinzufügen".

Sie können eine Rufnummer eines PSTN-Partners und deren Rufrichtung bearbeiten.

Sie können die Zuweisung einer Rufnummer an einen PSTN-Partner löschen.

Klicken Sie auf *Übernehmen*. Ein Hinweis wird angezeigt, den Sie mit *OK* bestätigen müssen. Ebenso müssen Sie im Bestätigungsdialog auf *OK* klicken.

Sie können die Zuweisung einer Rufnummer an einen PSTN-Partner löschen.

Der Dialog *PSTN-Rufnummer löschen* wird angezeigt. Zur Kontrolle wird die Rufnummer angezeigt.

Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

6.4.4.8 Auf Lieferzustand zurücksetzen

Sie können die Einstellungen zum Default-PSTN-Partner auf den ursprünglichen Zustand zurücksetzen. Dies betrifft jedoch nicht die zugewiesene Rufnummer. Diese können Sie separat auf ihren Lieferzustand zurücksetzen – siehe Section 7.4.4.10, "Auf Lieferzustand zurücksetzen".

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PSTN-Partner* **>** *PSTN-Partner hinzufügen* **>** *Auf Lieferzustand zurücksetzen*

Eine Warnung wird angezeigt, die Sie zur Kenntnis nehmen sollten. Klicken Sie anschließend auf *Auf Lieferzustand zurücksetzen* und im Bestätigungsdialog auf *OK*.

6.4.4.9 Default-Rufnummer

Sie können die Default-Rufnummer des Default-PSTN-Partners verwalten.

Sie können die Default-Rufnummer und die zugewiesene Rufrichtung des Default-PSTN-Partners bearbeiten.

Der Dialog *Default-PSTN-Rufnummer* wird angezeigt. Feldbeschreibungen siehe Section 7.4.4.6, "Rufnummer hinzufügen".

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *PSTN (nur für HG 3500)* **>** *PSTN-Partner* **>** *PSTN-Partner hinzufügen* **>** *Default-Rufnummer*

6.4.4.10 Auf Lieferzustand zurücksetzen

Sie können die Einstellungen zur Default-Rufnummer des Default-PSTN-Partners auf den ursprünglichen Zustand zurücksetzen. Dies betrifft jedoch nur die zugewiesene Rufnummer. Die Grundeinstellungen zum Default-PSTN-Partner können Sie separat auf ihren Lieferzustand zurücksetzen – siehe Section 7.4.4.8, "Auf Lieferzustand zurücksetzen".

Eine Warnung wird angezeigt, die Sie zur Kenntnis nehmen sollten. Klicken Sie anschließend auf *Auf Lieferzustand zurücksetzen* und im Bestätigungsdialog auf *OK*.

6.4.5 Wahlparameter

Die Durchwahlnummern, die in OpenScape 4000 V10 mithilfe von OpenScape 4000 Manager als S0-Teilnehmer konfiguriert wurden, können im HG 3500/3575 einem VCAPI-Client, der MSN/DUWA-Nummer eines PSTN-Partners oder der Routerrufnummer zugewiesen werden. Über das WBM sind

die Wahlparameter selbst konfigurierbar. Eingerichtete Teilnehmer und IP-Adressen sind einsehbar.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *Wahlparameter*

Klicken Sie auf das Pluszeichen (+) neben *Wahlparameter*, um die folgenden Einträge anzuzeigen:

1) *Allgemeine Wahlparameter ändern*

Eingerichtete Teilnehmer Verwendete IP-Adressen

6.4.5.1 Allgemeine Wahlparameter ändern

Sie können die Grundeinstellungen anzeigen und bearbeiten. Die Konfiguration ist optional.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *Wahlparameter* **>** *Allgemeine Wahlparameter ändern*

Der Dialog *Allgemeine Wahlparameter* wird angezeigt. Folgende Felder können bearbeitet werden:

- *CLIR bestätigen*:Dies ist eine Sicherheitsfunktion. Um die Weiterleitung einer als geheim gekennzeichneten Anrufernummer ins LAN zu unterdrücken, kreuzen Sie diese Option an. Hintergrund dieser Option ist, dass die CLIR-Funktionalität im Zusammenhang mit IP-Routing in LANs nicht eindeutig definiert ist, weil es die Endteilnehmerschnittstelle zum öffentlichen Netz nicht in der Form gibt wie in der klassischen Telefonie.

E.164,

- *Internationales Präfix*: Das Präfix für internationale Nummern (inklusive Amtsholungsziffer).
- *Nationales Präfix*: Das Präfix für nationale Ferngespräche (inklusive Amtsholungsziffer).
- *Teilnehmer-Präfix*: Die Amtsholungsziffer bzw. das Präfix für Gespräche ins öffentliche Telefonnetz.
- *Ländercode*: Die Länderkennung für den Standort des HG 3500/3575.
- *Ortskennzahl*: Die Ortskennzahl für den Standort des HG 3500/3575.
- *Standortcode*: Der Standortcode für das HG 3500/3575 (falls vorhanden).

Beispiel:

Als Amtsholungsziffer ist in der OpenScape 4000 V10 die Null (0) konfiguriert. Die Anlage steht in München und hat die Anschlussnummer 722:

Internationales Präfix= 000	Länderkennung = 49
Nationaler Präfix = 00	Ortskennzahl = 89
Teilnehmer-Präfix = 0	Standortcode = 722

Die Rufnummernbewertung durch HG 3500/3575 wird ausschließlich durch die hier konfigurierbaren Wahlparameter und unabhängig von entsprechenden

weiteren Parametern der OpenScape 4000 V10 festgelegt. Daher ist explizit darauf zu achten, dass das verwendete Rufnummernschema des HG 3500/3575 schlüssig zur entsprechenden Konfiguration der OpenScape 4000 V10 eingerichtet wird. Bezogen auf dieses Beispiel bedeutet das: Wenn die OpenScape 4000 V10 im impliziten Rufnummernformat mit Amtskennzahl 0 an das HG 3500/3575 signalisiert, so muss der Präfix für Amtsholung in den Wahlparametern ebenfalls auf 0 eingestellt werden. In dem Beispiel wird das nationale Präfix auf 00 und das internationale Präfix auf 000 gesetzt. In beiden Fällen steht die erste 0 für den Leitungszugangscode.

Privater Nummernplan

- *Level 0-Präfix*: Teilnehmer-Vorwahl
- *Level 1-Präfix*: Nationales Präfix
- *Level 2-Präfix*: Internationales Präfix
- *Level 0-Code*: Standortcode
- *Level 1-Code*: Vorwahl
- *Level 2-Code*: Ländercode

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

6.4.5.2 Eingerichtete Teilnehmer

Dies sind eingerichtete S0-Teilnehmer.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *Wahlparameter* **>** *Eingerichtete Teilnehmer*

Sie können sich eingerichtete Teilnehmer auflisten lassen.

Der Dialog *Eingerichtete Teilnehmer* wird angezeigt. In einer Tabelle werden die Nebenstellenrufnummern und die Teilnehmertypen aufgelistet. Teilnehmertypen sind z. B. HFA-System-Client oder PSTN-Partner.

6.4.5.3 Verwendete IP-Adressen

Dies sind die verwendeten IP-Adressen, z. B. der LAN-Schnittstellen, der Teilnehmer und der PSTN-Partner.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Netzwerk und Routing* **>** *Routing* **>** *Wahlparameter* **>** *Verwendete IP-Adressen*

Sie können sich die betroffenen IP-Adressen auflisten lassen.

Der Dialog *Verwendete IP-Adressen* wird angezeigt. In einer Tabelle werden die IP-Adressen und die Teilnehmertypen aufgelistet. Teilnehmertypen sind z. B. LAN-Schnittstellen oder PSTN-Partner.

Die Einträge sind sortierbar. Ein Dreieck hinter einem Spaltennamen kennzeichnet die Spalte, nach der sortiert wurde. Wenn Sie die Tabelle nach einer anderen Spalte sortieren möchten, klicken Sie auf den jeweiligen Spaltennamen.

6.5 Sprachgateway

Das OpenScape 4000 V10 bietet Ihnen mit Voice over IP (VoIP) die Möglichkeit, die Leistungsmerkmale von HG 3500/3575 über IP-Netze zu nutzen. Dazu sind allgemeine Einstellungen der H.323-Parameter und die Konfiguration von PBX-Knoten und PBX-Routen erforderlich. Außerdem ermöglicht diese Funktion die Anmeldung von System-Clients.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway*

Die Baumstruktur für *Sprachgateway* wird angezeigt.

Einträge in der Baumstruktur *Sprachgateway*:

1) H.323-Parameter SIP-Parameter (nicht für HG 3575) Codec-Parameter IP-Networking-Modus (nicht für HG 3575) SIP-Trunk-Profilparameter (nicht für HG 3575)

SIP-Trunk-Profile

Ziel-Codec-Parameter Fallback auf SCN-Parameter

KZPs für MLPP (nicht für HG 3575) Clients ISDN Classmarks (nicht für HG 3575)

6.5.1 H.323-Parameter

Sie können Einstellungen für das H.323-Protokoll zur Übertragung von Sprache über das IP-Netz ansehen und einstellen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *H.323-Stack-Parameter*

Der Dialog *H.323-Stack-Parameter* wird angezeigt.

Folgende Felder können bearbeitet werden:

- *Benutzereingabezeichenfolge für Außerband-Signalisierung*: Dieses Feld schaltet die Funktion für die 'Außerband-Signalisierung (postdialing)' mit H.245-Nutzer-Eingangssignalisierung für 'Zeichenfolge für Außerband' ein oder aus.
- *Benutzereingabe für MFV-Außerband-Signalisierung*: Dieses Feld schaltet die Funktion für die 'Außerband-Signalisierung (postdialing)' mit H.245-Nutzer-Eingangssignalisierung für 'MFV-Außerband' ein oder aus.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

6.5.2 SIP-Parameter (nicht für HG 3575)

Sie können SIP-Einstellungen für das IP-Netz ansehen und teilweise einstellen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *SIP-Parameter*

Das Fenster *SIP-Parameter* wird angezeigt. Sie können folgende Felder ansehen:

SIP User-Agent

- *SIP-Registrar verwenden*: Ein SIP-Registrar ist ein Server in einem SIP-Netz (**S**ession **I**nitiation **P**rotocol), der SIP REGISTER-Anfragen akzeptiert und verarbeitet. Um erreichbar zu sein, muss sich jeder SIP-Teilnehmer an einem SIP-Registrar anmelden. Mögliche Anzeigen: Ja/Nein
- *SIP-Registrar IP-Adresse*: IP-Adresse des SIP-Registrars.
- *SIP-Registrar TLS-Port-Nummer*: Nummer des TLS-Ports auf dem SIP-Registrar. TLS (**T**ransport **L**ayer **S**ecurity) ist ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet.
- *SIP-Registrar TCP/UDP-Portnummer*: Nummer des TCP/UDP-Ports auf dem SIP-Registrar. TCP (**T**ransmission **C**ontrol **P**rotocol) und UDP (**U**ser **D**atagram **P**rotocol) sind Protokolle für die IP-Kommunikation.
- *Alternativer SIP-Registrar IP-Adresse*: IP-Adresse des zweiten SIP-Registrars, der benutzt werden soll, wenn der erste SIP-Registrar nicht verfügbar ist.
- *Alternative SIP-Registrar TLS-Portnummer*: Nummer des TLS-Ports am zweiten SIP-Registrar.
- *Alternativer SIP-Registrar TCP/UDP-Port-Nummer*: Nummer des TCP/UDP-Ports auf dem zweiten SIP-Registrar.
- *Dauer der Registrierung (s)*: Nach Ablauf dieser Registrierungsdauer muss sich ein SIP-Teilnehmer neu registrieren.

SIP-Server (Registrar / Redirect)

- *SIP-Server IP-Adresse*: IP-Adresse des SIP-Servers.
- *SIP-Server TCP/UDP-Port-Nummer:* Nummer des TCP/UDP-Ports auf dem SIP-Server.
- *SIP-Server TLS-Portnummer*: Portnummer des SIP-Servers für TLS.
- *Standardregistrierungsdauer (s):* 600 (wird verwendet, wenn kein 'Verfällt'-Wert erhalten wird)
- *Range used for Randomized Registration (%) (Bereich für randomisierte Registrierung)*: 25 (0 bedeutet: keine Randomisierung verwenden).

RFC 3261 Timer-Werte

Transaction Timeout (ms): In RFC 3261 ist der SIP-Timer definiert.

SIP Transport-Protokoll

- *SIP über TCP*: (Abkürzung für **T**ransmission **C**ontrol **P**rotocol).
  TCP ist neben IP das zentrale Protokoll im Internet. Es stellt einen verbindungsorientierten, zuverlässigen, vollduplex Dienst in Form eines Datenstroms zur Verfügung.
- *SIP über UDP*: (Abkürzung für **U**ser **D**atagram **P**rotocol). UDP kann alternativ zu TCP verwendet werden, wenn keine Anforderungen an die Zuverlässigkeit gestellt werden. UDP garantiert weder die Zustellung der Pakete, noch ist eine bestimmte Reihenfolge des Eintreffens von Paketen gewährleistet.
- *SIP über TLS*: (Abkürzung für Transport Layer Security). TLS ist ein hybrides Verschlüsselungsprotokoll im Internet und Nachfolger von SSL (SSL: Secure Sockets Layer).

SIP-Session-Timer

- *RFC 4028 verwenden*: In RFC 4028 sind Session Timer als Erweiterung des SIP definiert. Dadurch werden periodische Aktualisierungen von SIP-Sitzungen ermöglicht.
- *Session-Expires (s)*: Zeit, nach der eine Sitzung abläuft.
- *Minimal-SE (s)*: Minimale Zeitdauer, nach der eine Session abläuft.

DNS-SRV Einträge

- *Sperrzeit für nicht erreichbares Ziele (s)*: Zeit, für die nicht erreichbare Ziele gesperrt sind. DNS: **D**omain **N**ame **S**ystem, SRV: **Serv**ice

Trunking-Parameter

- *Intervall für SIP OPTIONS ping senden (s)*: Abstand in Sekunden, in dem die 'SIP OPTIONS ping'-Nachricht zur Abfrage der Betriebsbereitschaft des Empfängergerätes gesendet wird. Der Wert '0â bedeutet, dass die Nachricht nicht gesendet wird. Wertebereich 2 bis 720 Sekunden

Anrufüberwachung

- *MakeCallReq Timeout (s)*: Timeout-Zeit, in der auf eine MakeCallReq-Message gewartet wird.
- SIP Connect Timeout (s): 300

Schaltflächen

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen.

6.5.3 Codec-Parameter

Sie können die Einstellungen für die Codecs G.711-A-law, G.711-Âµ-law, G.723 (nur für HG 3500), G.729, G.729A, G.729B, G.729AB sowie für das Faxprotokoll T.38 ansehen und einstellen.

Hintergrundinformationen:

Siehe Section 9.2, "Bandbreitenbedarf in LAN/WAN-Umgebungen"

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Codec-Parameter*

Feldbeschreibungen siehe unten.

Der Dialog *Codec-Parameter* wird angezeigt. In der Tabelle 'Codec' können Sie nachfolgende Parameter für die Protokolle G.711-A-law, G.711-Âµ-law, G.723, , G.729, G.729A, G.729B, G.729AB, und bearbeiten:

- *Priorität:*Dieses Feld enthält die Priorität, mit der der Codec verwendet werden soll. Die Priorität kann von 1 (hoch) bis 7 (niedrig) eingestellt werden. Ordnen Sie den Codecs unterschiedliche Prioritäten zu. In der Voreinstellung hat G.711-A-law die Priorität 1, G.711-Âµ-law Priorität 2, G.723 Priorität 5, , G.729A Priorität 4 und G.729AB Priorität 3. G.729, G.729B haben den Status 'nicht verwendet'.

- *Sprechpausenerkennung (VAD)*:Dieses Feld legt fest, ob beim jeweiligen Codec die Sprechpausenerkennung (VAD) verwendet werden soll oder nicht.
- *Rahmengröße*:In diesem Feld können Sie die Sampling-Rate bestimmen. Die einstellbaren Werte sind von den Codecs abhängig.

T.38-Fax

- *T.38-Fax*: Legt fest, ob das T.38-Faxprotokoll zum Einsatz kommen soll oder nicht.
- *Max. UDP-Datagramm-Größe für T.38-Fax*: Maximale Größe eines T.38-UDP-Datagramms in Byte.
- *Verwendete Fehlerkorrektur für T.38-Fax (UDP)*: Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll (t38UDPRedundancy oder t38UDPFEC).

IMPORTANT: Der Codec G.729 ist identisch mit dem Codec G.729A und der Codec G729B ist identisch mit dem Codec G.729AB (kein Unterschied in 'payload'.) Deshalb sind die Codecs G.729 und G.729B in der Voreinstellung ausgeschaltet.

IMPORTANT: Aus H.323-Signalisierungs-Sicht sind die Codecs G.729 und G.729A und die Codecs G.729B und G.729AB unterschiedlich.

IMPORTANT: Einige non-OpenScape H.323-Endpunkte (Cisco GK) verwenden die Codecnamen G.729 oder G.729B im 'H.323 signalling'. In diesem Fall müssen die Codecs G.729 und G.729B in HG 3500/3575 auch verwendet werden.

IMPORTANT: In einem reinen OpenScape-Netz können die Codecs G.729 und G.729B ausgeschaltet bleiben.

Sonstiges

- *ClearMode (ClearChannelData)*: Legt fest, ob die ClearChannel-Funktionalität aktiviert sein soll oder nicht.
- *Rahmengröße*:In diesem Feld können Sie die Sampling-Rate bestimmen. Möglich sind 10, 20, 30, 40, 50 und 60 Millisekunden (ms). Die Voreinstellung beträgt 20 ms.

RFC2833:

- *Übertragung von Fax/Modem-Tönen nach RFC2833*: Unterstützte Events: 32 bis 36 und 49. Für eine detaillierte Beschreibung des Standards siehe http:///www.faqs.org/rfcs/rfc2833.html.
- *Übertragung von DTMF-Tönen nach RFC2833*: Unterstützte Events: 0–15. Für eine detaillierte Beschreibung des Standards siehe http:///www.faqs.org/rfcs/rfc2833.html
- *Payload Type für ClearChannel*: Standard: 96, Payload Type für den ClearChannel-Codec.
- *Payload Type für RFC2833*: Standard: 98

- *Payload Type für RFC2198*: Standard: 99, entspricht dem 'Payload Type für RFC2833' +1
- Redundante Übertragung der RFC2833 Töne nach RFC2198: Alle durch RFC2833 übertragene Töne sind nach RFC2198 versichert, wenn RFC2198 eingeschaltet ist. Ausführliche Beschreibung des Standards siehe http:/// www.faqs.org/rfcs/rfc2833.html und http:///www.faqs.org/rfcs/rfc2198.html

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

6.5.4 IP-Networking-Modus (nicht für HG 3575)

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *IP-Networking-Modus (nicht für HG 3575)*

Das Fenster *IP-Networking-Modus* wird angezeigt. Es enthält das verwendete *Signalisierungsprotokoll für IP-Networking (SIP)* und die *SIP-Protokollvariante für IP-Networking (SIP-Q)* sowie eine Tabelle der *IP-Networking-Sätze* mit den Angaben *Satznummer (Circuit)*, *Anzahl der konfigurierten B-Kanäle* und *Gesperrt*.

Das Fenster *IP-Networking-Modus* wird angezeigt. Es enthält die folgenden Angaben:

- *Signalisierungsprotokoll für IP-Networking*: z. B. SIP, Nicht konfiguriert
- *SIP-Protokollvariante für IP-Networking*: SIP-Q
- *Max. Anzahl der B-Kanäle für SIP-Q*: Hier steht der Wert aus dem AMO CGWB, z. B. 0.
- *SIP DNS-SRV Survivability-Modus*: Ja/Nein (DNS: **D**omain **N**ame **S**ystem, SRV: **S**er**v**ice)
- *Anzahl der für IP-Networking konfigurierten Circuits*: z. B. 0, 2

Das Fenster enthält im Bereich *IP-Networking-Sätze* eine Tabelle mit den folgenden Angaben:

- *Portnummer (circuit)*
- *Gesperrt*: Ja/Nein

6.5.5 SIP-Trunk-Profilparameter (nicht für HG 3575)

Um das Funktionieren von SIP-Trunking zu ermöglichen, muss die Einstellung für SIP-Trunking an die Anforderungen des jeweiligen SIP-Providers angepasst werden. Dazu sind Profile für Trunks über SIP-Q und Profile für Trunks über native SIP aktivier- oder deaktivierbar.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *SIP-Trunk-Profilparameter*

Der Dialog *SIP-Trunk-Profilparameter* wird angezeigt. Feldbeschreibungen siehe unten.

Sie können die Einstellungen für *SIP-Trunk-Profilparameter* bearbeiten.

Der Dialog *SIP-Trunk-Profilparameter* wird angezeigt. Er enthält:

- *SIP-Protokollvariante für IP-Networking: SIP-Q* (kann nicht geändert werden)

- *Profile für Trunks via SIP-Q verwenden*: Aktivierbar/Deaktivierbar. Ist per Default deaktiviert. Diese Einstellung muss aktiviert werden, wenn SIP-Load-Balancing verwendet werden soll (nicht bei HG 3575).
- *Trunk-Profile via Native SIP verwenden*: Aktivierbar/Deaktivierbar. Ist per Default aktiviert.
- *SIP-Peer-Filtering aktivieren* Aktivierbar/Deaktivierbar. Ist per Default deaktiviert. Bei aktiviertem Feature/Checkbox wird nur auf Anfragen von "bekannten" Peers geantwortet. Alle Anfragen von "unbekannten" Peers werden ignoriert.
- *An SIP-Load Balancing teilnehmen:* Aktivierbar/Deaktivierbar. Ist per Default deaktiviert.

6.5.6 SIP-Trunk-Profile

NOTICE: Der Ordner *SIP-Trunk-Profile* wird nur angezeigt, wenn unter *SIP-Trunk-Profilparameter (nicht für HG 3575)* die Option *Profile für Trunks via SIP-Q verwenden* aktiviert wurde.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *SIP-Trunk-Profile*

In der Baumstruktur von *SIP-Trunk-Profile* werden Unterordner mit den Namen von SIP-Providern angezeigt. Jeder Unterordner enthält die Einstellungen für den SIP-Provider. Die Einstellungen können angezeigt, geändert und aktiviert werden.

Das SIP-Trunk-Profil des ausgewählten SIP-Providers wird angezeigt. Es können folgende Änderungen vorgenommen werden:

- *Profilname*: nicht änderbar
- Trunk-Profil aktivieren: Aktivierbar/deaktivierbar
- *Account/Authentifizierung nötig*: Aktivierbar/Deaktivierbar.
- *Remote Domain-Name*: Den Namen für eine Remotedomäne eingeben.
- *SIP Transport-Protokoll*: *UDP* oder *TCP* kann im Optionsfeld ausgewählt werden. Diese beiden Protokolle gehören zur Transportschicht des TCP/IP-Referenzmodells (UDP: User Datagram Protocol, TCP: Transmission Control Protocol).

Sicherheit:

- Freigegebene Sicherheitsstufe: Nicht änderbar.
- TLS verwendet: Nicht konfigurierbar
- RTP-Sicherheitsmodus:
- Verwendung von Payload Encryption: Nicht konfigurierbar

Registrar:

- *Registrar verwenden*: Aktivierbar/Deaktivierbar. Festlegen, ob ein Domain-Name-Registrar verwendet werden soll.
- *IP Adresse/Host-Name*: IP-Adresse oder Hostname des Domain-Name-Registrars eingeben.
- *Port festlegen*: Aktivierbar/Deaktivierbar. Port für den Domain-Name-Registrar festlegen.
- *Reregistrations-Intervall (s)*: Festlegen, in welchen Zeitabständen eine Neuregistrierung erforderlich ist.

Proxy:

- *IP Adresse/Host-Name*: IP-Adresse oder Hostname des Proxy-Servers eingeben. Das ist der SIP-Server des Providers.
- *Port festlegen*: Aktivierbar/Deaktivierbar. Port für den Proxy-Server festlegen.

Outbound-Proxy:

- *Outbound-Proxy verwenden*: Aktivierbar/Deaktivierbar. Ist der Proxy-Server, über den der SIP-Server des Providers erreicht wird. Für ausgehenden Datenverkehr beim SIP-Provider.
- *IP Adresse/Host-Name*: IP-Adresse oder Hostname des Outbound-Proxy-Servers eingeben.
- *Port festlegen*: Aktivierbar/Deaktivierbar. Port für den Outbound-Proxy-Server festlegen.

Inbound-Proxy:

- *Inbound-Proxy verwenden*: Aktivierbar/Deaktivierbar. Ist der Proxy-Server, über den der SIP-Server des Providers erreicht wird. Für eingehenden Datenverkehr beim SIP-Provider.
- *IP Adresse/Host-Name*: IP-Adresse oder Hostname des Inbound-Proxy-Servers eingeben.
- *Port festlegen*: Aktivierbar/Deaktivierbar. Port für den Inbound-Proxy-Server festlegen.

Schaltflächen

Klicken Sie auf die Schaltfläche *Übernehmen*, um die Daten zu aktualisieren; auf *Rückgängig*, um die vorherigen Werte wiederherzustellen; auf Löschen, um die Änderungen zu verwerfen.

6.5.7 Ziel-Codec-Parameter

Sie können Codecs G.711-A-law, G.711-Âµ-law, G.723, G.729A, G.729B für eine bestimmte IP-Adresse hinzufügen, ändern oder löschen.

Hintergrundinformationen:

Siehe Section 9.2, "Bandbreitenbedarf in LAN/WAN-Umgebungen"

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Ziel-Codec-Parameter*

6.5.7.1 Ziel-Codec-Parameter hinzufügen

Sie können Ziel-Codec-Parameter für eine bestimmte IP-Adresse hinzufügen.

Haben Sie Ziel-Codec-Parameter für eine bestimmte IP-Adresse hinzugefügt, so können Sie sie ändern.

Sie können Ziel-Codec-Parameter für eine bestimmte IP-Adresse löschen.

WBM-Pfad:

WBM > *Konfiguration* **>** *Sprachgateway* **>** *Ziel-Codec-Parameter* **>** *Ziel-Codec-Parameter hinzufügen* **>** *Ziel-Codec-Parameter*

Der Dialog *Ziel-Codec-Parameter* wird angezeigt. In der Tabelle 'Codec' können Sie nachfolgende Parameter für die Protokolle 'G.711 A-law', 'G.711 Âµ-law', 'G.723' (nur für HG 3500), 'G.729', 'G.729A', 'G.729B' und 'G.729AB'eintragen:

- *Priorität:*Dieses Feld enthält die Priorität, mit der der Codec verwendet werden soll. Die Priorität kann von 1 (hoch) bis 7 (niedrig) eingestellt werden. Ordnen Sie den Codecs unterschiedliche Prioritäten zu. In der Voreinstellung hat G.711-A-law die Priorität 1 (bei HG 3500, 3 bei HG 3575), G.711 Âµ law Priorität 2 (bei HG 3500, 4 bei HG 3575), G.723 Priorität 5 (bei HG 3500), G.729A Priorität 4 (bei HG 3500, 3 bei HG 3575) und G.729AB Priorität 3 (bei HG 3500, 1 bei HG 3575). G.729 und G.729B haben den Status 'nicht verwendet'.
- *Sprechpausenerkennung (VAD)*:Dieses Feld legt fest, ob beim jeweiligen Codec die Sprechpausenerkennung (VAD) verwendet werden soll oder nicht.
- *Rahmengröße*:In diesem Feld können Sie die Sampling-Rate bestimmen. Die einstellbaren Werte sind von den Codecs abhängig.

Ziel

- *Ziel-Adress-Typ*: Wählen Sie den *Host*, das *Subnetz* oder den *Bereich*aus.
- *IP-Adresse*: Geben Sie die zugehörige IP-Adresse für den Eintrag an.

Schaltflächen

Klicken Sie auf Übernehmen, um die Änderungen zu übernehmen. Klicken Sie auf *Rückgängig*, um die vorherigen Werte wiederherzustellen. Klicken Sie auf *Löschen*, um zu bestätigen, dass Sie den Eintrag löschen möchten.

6.5.8 Fallback auf SCN-Parameter

Sie können sich Fallback auf SCN-Parameter anzeigen lassen und bearbeiten. Weiterhin können Sie Fallback auf SCN aktivieren bzw. deaktivieren oder sich blockierte IP-Adressen anzeigen lassen.

Klicken Sie auf das Pluszeichen (+) neben Fallback auf SCN-Parameter, um die folgenden Einträge anzuzeigen:

Blockierte IP-Adressen anzeigen

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Fallback auf SCN-Parameter* **>** *QoS – Fallback auf SCN*

Sie können sich die Parameterliste für Fallback auf SCN-Parameter anpassen.

Der Dialog *QoS – Fallback auf SCN* wird angezeigt. Folgende Felder können Sie bearbeiten

- *Fallback auf SCN aktiviert*: Kreuzen Sie diese Option an, wenn ein Fallback auf SCN dann stattfinden soll, wenn eine der unterhalb festlegbaren Bedingungen erfüllt ist.
- *Aktivieren (Packetverlust)*: Kreuzen Sie diese Option an, wenn Paketverluste zu einem Fallback führen können.

- *Aktivieren – Round Trip Delay*: Kreuzen Sie diese Option an, wenn zu lange Zeiten zwischen dem Absenden von Anforderungen und dem Erhalt der Antworten im Netzwerk zu einem Fallback führen können.
- *Aktivieren (Jitter)*:Kreuzen Sie diese Option an, wenn instabile Taktsignale zu einem Fallback führen können.
- *Schwellwert (Packetverlust)*: Wenn 'Aktivieren (Packetverlust)' angekreuzt ist, geben Sie in diesem Feld an, bei welchem Prozentwert eines Paketverlusts ein Fallback ausgelöst werden soll.
- *Schwellwert (Umlaufzeit)*: Wenn 'Aktivieren (Umlaufzeit)' angekreuzt ist, geben Sie in diesem Feld an, ab wie vielen Millisekunden Antwortzeit ein Fallback ausgelöst werden soll.
- *Schwellwert (Jitter)*:Wenn 'Aktivieren (Jitter)' angekreuzt ist, geben Sie in diesem Feld an, ab wie vielen Millisekunden Abweichung bei Taktsignalen ein Fallback ausgelöst werden soll.
- *Zeitdauer des Routensperrtimers (Min.)*:Geben Sie in diesem Feld an, wie viele Minuten ein Fallback andauern kann, bevor ein erneutes IP-Routing versucht wird.
- *Reaktion des Auswertungs-Algorithmus*: Wählen Sie aus, wie schnell der Auswert-Algorithmus reagieren soll. Zur Auswahl stehen 'Langsam' und 'Schnell'.

Schaltflächen

Klicken Sie auf die Schaltfläche *Übernehmen*, um die Daten zu aktualisieren, oder auf *Rückgängig*, um die vorherigen Werte wiederherzustellen.

6.5.8.1 Blockierte IP-Adressen anzeigen

Sie können sich die Liste der blockierten IP Adessen anzeigen lassen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Fallback auf SCN-Parameter* **>** *Blockierte IP-Adressen anzeigen* **>** *Liste der blockierten IP Adressen*

Die Tabelle *Liste der blockierten IP Adressen* wird angezeigt.

6.5.8.2 KZPs für MLPP (nicht für HG 3575)

Sie können die Kennzahlpunkte für MLPP anzeigen und bearbeiten.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *KZPs für MLPP (nicht für HG 3575)* > *KZPs für MLPP*

Die Tabelle *KZPs für MLPP (nicht für HG 3575)* wird angezeigt. Sie enthält Kennzahlpunkte für Anrufe.

Die Kennzahlpunkte können geändert werden. Es sind maximal 16 Zeichen erlaubt. Diese sind: 0–9, *, #.

Es können die folgenden Kennzahlpunkte geändert werden:

- Routine Call (DSNR)
- Priority Call (PRTY)

- Immediate Call (IMMED)
- Flash Call (FLASH)
- Flash_Override (FLASHOV)

Klicken Sie auf *Übernehmen*, um die Daten zu aktualisieren. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen.

6.5.9 Clients

Sie können die Client-Einstellungen anzeigen. Die Client-Einstellungen werden über den OpenScape 4000 Manager vorgenommen. Im WBM gibt es nur eine Anzeigefunktion.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Clients*

Clients (Ordner):

Klicken Sie auf das Pluszeichen (+) neben *Clients* in der Baumstruktur, um die folgenden Einträge anzuzeigen:

1) *HFA UFIP SIP*

Klassische SIP-Clients

6.5.9.1 HFA

Sie können die eingerichteten HFA-Clients im OpenScape 4000-Netz ansehen.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Clients* > *HFA* > *HFA-Clients*

HFA Clients

Port Number	Station Number	Authentication required	Port Status	IP Address	TLS used	Cipher	RMX blocked	AC-Win IP
1	13000	No		0.0.0.0	No	No	No	No
2	13001	No		0.0.0.0	No	No	No	No
3	13002	No		0.0.0.0	No	No	No	No
4	13003	No		0.0.0.0	No	No	No	No

Sie können die Einstellungen eines einzelnen HFA-Clients ansehen.

Der Dialog HFA-System-Client wird angezeigt. Sie können die folgenden Felder anzeigen:

- *Port number (Anschlussnummer) Zeigt die interne OpenScape 4000-Geräte-kennung des SIP-Clients an.*
- *Rufnummer:*Zeigt die interne Durchwahl des SIP-Clients an.
- *Authentifizierung erforderlich*: Zeigt an, dass der Teilnehmer für das Anmelden zum SIP-Client eine Authentifizierung (Benutzerkennung und Passwort) benötigt.
- *Port-Status:* angemeldet

- *IP-Adresse*: IP-Adresse des HFA-Clients
- *TLS verwendet*: Transport Layer Security ja/nein
- *Cipher (Ziffer):* Konfigurationsparameter in OpenScape 4000 (AMO SDAT-Parameter CLASSEC) des SIP-Client.
- *Gesperrt:*
- *AC-Win IP*: Angabe, ob der HFA-Client eine AC-Win IP-Applikation ist

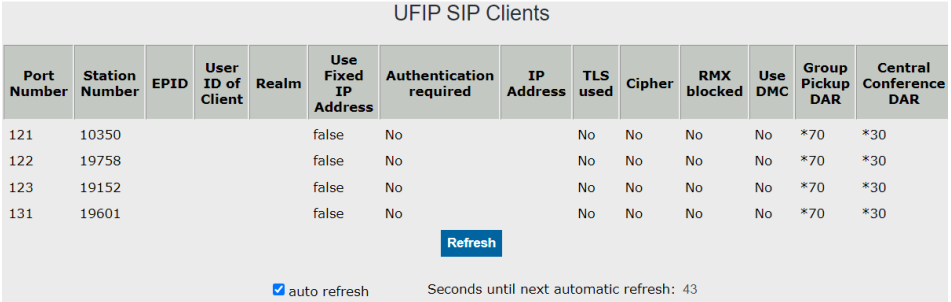
6.5.9.2 UFIP SIP

Sie können die eingerichteten UFIP-SIP-Clients im IP-Netz ansehen

Sie können die Einstellungen aller UFIP-SIP-Clients in einer Tabelle ansehen.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Clients* > *UFIP SIP* > *UFIP-SIP-Clients*



Eine dicke Linie zeigt an, dass der SIP-Client erfolgreich registriert wurde.

Die Tabelle *SIP-Clients* wird angezeigt. Sie können die folgenden Felder anzeigen:

- *Port number (Anschlussnummer): Zeigt die interne OpenScape 4000-Gerätekennung des SIP-Clients an.*
- *Teilnehmerrufnummer*: Zeigt die interne Durchwahl des SIP-Clients an.
- EPID: Zeigt die Endpunktkennung (ID des physischen Geräts) des SIP-Clients an.
- *User-Id of Client (Benutzer-ID des Clients)*: Zeigt den Benutzernamen für den SIP-Client-Zugang an. *Authentication Required* (Authentifizierung erforderlich) muss aktiviert sein.
- *Realm (Bereich)*: Zeigt den Bereich (die Sicherheitszone) für die vertrauliche Authentifizierung gegenüber dem SIP-Client an. *Authentication Required* (Authentifizierung erforderlich) muss aktiviert sein.
- *Authentication Required (Authentifizierung erforderlich)*: Konfigurationsparameter in OpenScape 4000, der angibt, dass der SIP-Client eine Authentifizierung (Benutzername und Passwort) erfordert.
- IP Address (IP-Adresse) Zeigt die IP-Adresse oder den Hostnamen des SIP-Clients an.
- TLS verwendet: Zeigt an, ob der SIP-Client zur Registrierung TLS verwendet hat.
- Cipher (Ziffer): Konfigurationsparameter in OpenScape 4000 (AMO SDAT-Parameter CLASSEC) des SIP-Client.

- *Use DMC (DMC verwenden)*DMC (Direct Media Connection) wird für den direkten Austausch der Nutzdaten zwischen zwei SIP-Endpunkten im IP-Netzwerk verwendet. Standard: Ja.
- *Use Instant DMC (Instant-DMC verwenden)*
- *Gesperrt: OpenScape 4000-Parameter des SIP-Clients.*
- Use DMC (DMC verwenden) OpenScape 4000-Parameter des SIP-Clients.
- Group Pickup DAR (Anrufübernahme DAR, Digit Analysis Result): OpenScape 4000-Parameter des SIP-Clients.
- Central Conference DAR (Konferenz DAR, Digit Analysis Result): OpenScape 4000-Parameter des SIP-Clients.

Schaltfläche

Aktualisieren: Klicken Sie auf diese Schaltfläche, um die Tabelle zu aktualisieren.

Kontrollkästchen

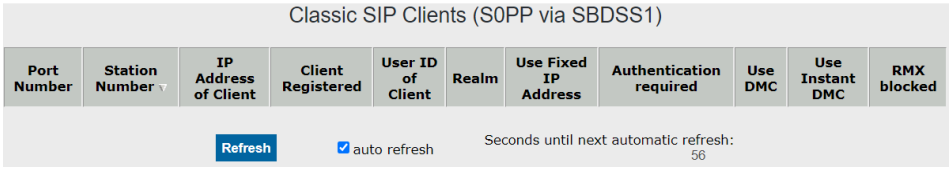
Aktualisieren: Aktivierbar/Deaktivierbar. Wenn die Checkbox aktiviert ist, wird die Tabelle 'SIP-Clients' in regelmäßigen Zeitabständen aktualisiert, wie im Eingabefeld *Sekunden bis zur nächsten Aktualisierung* angegeben.

6.5.9.3 Klassische SIP-Clients

WBM-Pfad:

WBM > Konfiguration > Sprachgateway > Clients > *Klassische SIP-Clients* > *Klassische SIP-Clients (S0PP über SBDSS1)*

Sie können die Einstellungen aller klassischen SIP-Clients in einer Tabelle ansehen.



6.5.10 ISDN Classmarks (nicht für HG 3575)

Sie können die Einstellungen der ISDN Classmarks für den CorNet-N Transport ansehen oder ändern.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *ISDN Classmarks (nicht für HG 3575)*

Sie können die Einstellungen für ISDN Classmarks ansehen.

Der Dialog *ISDN Classmarks für CorNet-N Transport* wird angezeigt.

Sie können folgende Felder ändern:

- *Externe Verbindung*: Markieren Sie dieses Feld, um externe Verbindungen zu erlauben. Ist das Feld nicht markiert, sind nur interne Verbindungen möglich.

- *Halten/Übergeben*: Markieren Sie dieses Feld, um die Funktionen Halten und Gesprächsübergabe zu erlauben.
- *Anrufumleitung*: Markieren Sie dieses Feld, um Anrufumleitungen zu erlauben.
- *Rückruf*: Markieren Sie dieses Feld, um Rückrufe zu erlauben.

Klicken Sie auf *Übernehmen*, um die Daten zu aktualisieren. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen.

6.6 Payload

Payload ermöglicht Ihnen die Anzeige und Konfiguration von Anschlusstypen und Protokollen im Gateway, von Media Stream Control (MSC) und von Erweiterungsmodulen des Gateways.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Payload*

Die Baumstruktur für *Payload* wird angezeigt.

Einträge in der Baumstruktur *Payload*:

1) *Devices Protokolle QoS Data Collection Media Stream Control (MSC) HW-Module Fax/Modem Ton-Behandlung*

Mikey

6.6.1 Devices

'Devices' ist ein Sammelbegriff für Teilnehmer, Leistungsmerkmale und Funktionen, die Kanäle benötigen.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Payload* **>** *Devices*

Klicken Sie auf das Pluszeichen (+) neben *Devices*, um ein Menü mit den folgenden Einträgen anzuzeigen:

1) *Globale Device-Einstellungen Auf Lieferzustand zurücksetzen*

IMPORTANT: Jedem Device sind in der Baumdarstellung so viele B-Kanäle zugeordnet, wie maximal für dieses Gerät verfügbar sind.

6.6.1.1 Globale Device-Einstellungen

Sie können die Einstellungen, die für alle Devices gelten, ansehen.

WBM > Konfiguration > Payload > Sprachgateway **>** Devices > *Globale Device-Einstellungen*

Der Dialog *Globale Device-Einstellungen* wird angezeigt. Es werden der Typ Codec-Typ des globalen Gateways, die maximale Anzahl verfügbarer und lizen-

zierter B-Kanäle, sowie die maximale Anzahl von LAN-Clients an einem Kanal für Music on Hold (überzählige Anrufe werden nicht durchgeschaltet) angezeigt.

6.6.1.2 Auf Lieferzustand zurücksetzen

Sie können für alle Device-Einstellungen global die ursprünglichen Einstellungen wiederherstellen.

WBM > Konfiguration > Sprachgateway **>** Payload > Devices > *Auf Lieferzustand zurücksetzen* **>** *Device-Einstellungen auf Lieferzustand zurücksetzen*

Der Dialog *Device-Einstellungen auf Lieferzustand zurücksetzen* wird angezeigt und enthält eine Warnung.

Klicken Sie anschließend auf *Auf Lieferzustand zurücksetzen* und im Bestätigungsdialog auf *OK*.

6.6.1.3 Device-Liste

Sie können die Einstellungen für ein Device ansehen.

WBM-Pfad:

WBM > Konfiguration > Sprachgateway **>** Payload > Devices > *Device-Liste* **>** *ausgewähltes Device* > *Device-Einstellungen*

Der Dialog *Device-Einstellungen* wird angezeigt. Zur Information werden die Bezeichnung des Devices (Device-Typ), der aktuelle Betriebszustand und gegebenenfalls das zugeordnete Kommunikationsprotokoll angezeigt.

Symbol	Bedeutung
	Grüner Punkt: Das Device ist verwendbar (up).
	Roter Punkt: Das Device ist nicht verwendbar (down).
	Grauer Punkt: Das Device befindet sich in einem nicht definierten Zustand oder wird gerade getestet.

6.6.2 Protokolle

NOTICE: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* **>** *Payload* > *Protokolle*

Klicken Sie auf das Pluszeichen (+) neben Protokolle, um die folgenden Einträge anzuzeigen:

1) *DSS1 CNQ*

6.6.2.1 DSS1

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Payload* > *Protokolle* > *DSS1* > *Protokoll-Varianten-Parameter ändern*

Parameter anzeigen

Das Fenster *Protokoll-Varianten-Parameter* für das Signalisierungsprotokoll DSS1 (**D**igital **S**ubscriber Signaling **S**ystem Nr. 1) wird angezeigt. Es enthält die folgenden Bereiche: *Allgemein*, *Parameter*, *Zeichenkettenparameter* und *Timer*.

Parameter ändern

Das Fenster *Protokoll-Varianten-Parameter ändern* für das Signalisierungsprotokoll DSS1 wird angezeigt.

6.6.2.2 CNQ

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Payload* > *Protokolle* > *CNQ* > *Protokoll-Varianten-Parameter ändern*

Parameter anzeigen

Das Fenster *Protokoll-Varianten-Parameter* für das Signalisierungsprotokoll CNQ wird angezeigt. Es enthält die folgenden Bereiche: *Allgemein*, *Parameter*, *Zeichenkettenparameter* und *Timer*.

Parameter ändern

Das Fenster *Protokoll-Varianten-Parameter ändern* für das Signalisierungsprotokoll CNQ wird angezeigt.

6.6.3 QoS Data Collection

Quality of Service Data Collection (QDC) – Aufgaben und Funktionen:

Mit dem OpenScape-IP-Service 'QoS-Data-Collection' steht ein Tool zur Verfügung, das Daten von OpenScape-Produkten sammelt. Diese Daten werden zur Analyse der Sprach- und Netzwerk-Qualität der Produkte verwendet.

Ziele des 'QoS-Data-Collection'-Service mit seinen Leistungsmerkmalen sind:

- Reduzierung der allgemeinen Aufwendungen bei der Analyse von QoS-Problemen.
- Erhöhung der 'remote clearance rate'.
- Frühzeitiges Erkennen von Netzwerkproblemen zur Vorbeugung gegen Störungen der Sprachqualität.

Das führt zu:

- Reduzierung der Service-Aufwendungen und Kosten.
- Konkurrenzfähigen Wartungsverträgen.

- Schnellen und qualifizierten Antworten zu einem Kundenproblem.
- Erhöhung der allgemeinen Kundenzufriedenheit mit dem Produkt und der Technologie.
- Möglichkeit, Änderungen in der Netzwerkumgebung des Kunden zu erkennen und die Marketing-Aktivitäten von OpenScape-Services entsprechend auszurichten.

Durch den Einsatz von QDC können wichtige Verbesserungen im gesamten Service-Prozess (break/fix process) erzielt werden.

Hintergrundinformationen:

Siehe Section 9.3, "Quality of Service (QoS)"

WBM-Pfad:

WBM **>** Konfiguration **>** *Sprachgateway* **>** *Payload* **>** *QoS Data Collection* **>** *Quality of Service Data Collection*

Der Dialog *Quality of Service Data Collection* wird angezeigt.

Sie können die aktuellen Einstellungen zu QoS-Data-Collection anzeigen und bearbeiten.

QDC-Konfiguration

- *Senden an QCU*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an die QCU gesendet werden sollen. Standardwert: Kontrollkästchen deaktiviert.
- *QCU-IP-Adresse*: Geben Sie hier die IP-Adresse oder den Name des QCU-Host ein. Standardwert: 0.0.0.0.
- *QCU-Empfangsport*: Empfangsport für QCU. Geben Sie hier die Portnummer des QCU-Host ein. Standardwert: 12010.
- *Senden an Network Management aktiv*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an das Network Management-System gesendet werden sollen. Standardwert: Kontrollkästchen deaktiviert.

IMPORTANT: Wenn eines der Kontrollkästchen **Senden an QCU** oder **Senden an Network Management aktiv** aktiviert ist (Haken gesetzt), werden QoS-Reports erzeugt.

QDC-Reportmodus

- *Sende Bericht, wenn*: Wählen Sie aus dem Listenfeld den gewünschten Zeitpunkt zur Berichtübertragung aus. Es stehen die folgenden Optionen zur Verfügung:
- – *Session-Ende und Schwellwert überschritten*: Ein Report wird nur am Ende einer Session gesendet und nur wenn der Schwellwert erreicht wurde.
  – *Ende des Berichtsintervalls und Schwellwert überschritten*: Ein Report wird in jedem Berichtsintervall gesendet, wenn der Schwellwert erreicht wurde.
  – *Session-Ende, unbedingt*: Am Session-Ende wird immer ein Report gesendet.
  – *Ende des Berichtsintervalls, unbedingt*: Am Ende des Berichtsintervalls wird immer ein Report gesendet.
- *Berichtsintervall (Sek.)*: Geben Sie das Intervall (in Sekunden) ein, in dem die Berichte gesendet werden sollen. Für jeden Berichtsintervall wird ein

QoS-Report gesendet wenn der Reportmodus entsprechend gesetzt wurde. Standardwert: 60 Sek. Gültige Werte: 0 ... 65535

- *Beobachtungszeitraum (s)*: Dieser Parameter kann nicht eingestellt werden. Standardwert: 10 Sek.
- *Minimale Session-Dauer (*100 ms)*: Geben Sie hier die Mindets-Session-Dauer (*100 ms) ein. Besteht eine Session (z. B. eine Gesprächsverbindung) kürzer als dieses Minimum, dann wird kein QoS-Report gesendet. Standardwert: 20 (2 s) Gültige Werte: 0 ... 255

IMPORTANT: Die Zeitskala ist im Beobachtungszeitraum und im Berichtsintervall segmentiert. Jeder Beobachtungszeitraum wird auf eine Schwellwertüberschreitung geprüft. Für jeden Berichtsintervall wird ein QoS-Report gesendet, wenn der Reportmodus entsprechend gesetzt wurde.

QDC-Schwellwerte

- *Oberer Jitter-Schwellwert (ms)*: Geben Sie hier den oberen Jitter-Schwellwert für die Reportauslösung ein. Der Jitter wird gegen diesen Schwellwert geprüft und zwischen zwei aufeinanderfolgenden RTP Paketen gemessen. Standardwert: 20 ms Gültige Werte: 0 ... 255
- *Schwellwert für durchschn. Paketlaufzeitverzögerung (ms)*: Die Paketlaufzeitverzögerung spiegelt die Gesamtlaufzeiten in beiden Richtungen wider. , ; geben Sie in dieses Feld den Schwellwert für die durchschnittliche Paketlaufzeitverzögerung ein, der die Reportauslösung bewirkt. Standardwert: 100msec, Gültige Werte: 0 ... 65535
- *Schwellwerte für Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl in Paketen der Schwellwerte für die Komprimierungs-Codec ein. Es stehen die folgenden Optionen zur Verfügung:
- – *Verlorene Pakete (pro 1000 Pakete)*: Geben Sie hier den Schwellwert für die Pakete ein, welche bei der Sprachdecodierung verlorengegangen sind. Der Wert ist das Verhältnis von verlorenen Paketen zur Gesamtzahl der Pakete. Standardwert: 10 Gültige Werte: 0 ... 255
  - *Aufeinanderfolgend verlorene Pakete*: Geben Sie hier den Schwellwert für die aufeinanderfolgend verlorenen Pakete ein. Es wird gezählt, wie viele Pakete aufeinanderfolgend (ohne Unterbrechung durch fehlerfreie Pakete) verloren gegangen sind. Wenn der gezählte Wert größer als der angegebene Wert ist, liegt eine Schwellwertüberschreitung vor. Standardwert: 2 Gültige Werte: 0 ... 255
  - *Aufeinanderfolgend verarbeitete Pakete*: Geben Sie hier den Schwellwert der aufeinanderfolgend verarbeiteten Pakete ein. Es wird gezählt, wie viele Pakete hintereinander fehlerfrei waren, ohne durch verlorene Pakete unterbrochen zu sein. Wenn der gezählte Wert kleiner als der angegebene Wert ist, liegt eine Schwellwertüberschreitung vor. Standardwert: 8. Gültige Werte: 0 ... 255
- *Schwellwerte für Nicht-Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl von Paketen für die Schwellwerte der Nicht-Komprimierungs-Codec ein. Es stehen die folgenden Optionen zur Verfügung:
- – *Verlorene Pakete (pro 1000 Pakete)*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.
  - *Aufeinanderfolgend verlorene Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

– *Aufeinanderfolgend verarbeitete Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

Erklärung und Verwendung von Komprimierungs- und Nicht-Komprimierungs-Codec:

Table 4: Codec - Betriebsarten

Codec	Audio-Mode	Anwendung
Hohe Qualität bevorzugt	Unkomprimierte Sprachübertragung.	Unkomprimierte Sprachübertragung verwenden. Geeignet für breitbandige Intranetverbindungen.
Niedrige Bandbreite bevorzugt	Bevorzugt komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit unterschiedlicher Bandbreite.
Nur geringe Bandbreite	Ausschließlich komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit geringer Bandbreite.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Der Dialog *Quality of Service Data Collection* wird angezeigt.

6.6.4 Media Stream Control (MSC)

Die Medienstromsteuerung (MSC) überwacht und verwaltet die Medienströme, die durch das HG 3500/3575 geleitet werden. Sie sorgt für die Übermittlung von Mediendaten zwischen LAN und ISDN.

Hintergrundinformationen:

Siehe Section 9.1, "Umgebungsanforderungen für VoIP" Siehe Section 9.2, "Bandbreitenbedarf in LAN/WAN-Umgebungen"

WBM-Pfad:

WBM > Konfiguration > Payload > *Media Stream Control (MSC)*

Klicken Sie auf das Pluszeichen (+) neben *Media Stream Control (MSC)*, um die folgenden Einträge anzuzeigen:

1) *MSC-Einstellungen ändern MSC-Einstellungen auf Lieferzustand zurücksetzen*

Sie können die aktuellen Einstellungen zur Medienstromsteuerung (MSC) ansehen.

Der Dialog *MSC-Einstellungen* wird angezeigt.

6.6.4.1 MSC-Einstellungen ändern

Sie können die aktuellen Einstellungen zur Medienstromsteuerung (MSC) bearbeiten.

IMPORTANT: Die Medienstromsteuerung sollte nur von Spezialisten umkonfiguriert werden. Die verfügbaren Parameter beeinflussen die Übertragungsqualität auf komplexe Weise, die zu beschreiben den Rahmen dieses Handbuchs sprengen würde.

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sprachgateway* **>** *Payload* > Media Stream Control (MSC) > *MSC-Einstellungen ändern*

Der Dialog *MSC-Einstellungen ändern* wird angezeigt.

- *Untere Grenze für RTP/RTCP-Ports*: Dieses Feld enthält den unteren Wert des zur Verfügung stehenden Portnummernbereiches für UDP-Ports. Voreingestellt ist die Portnummer 15000. Einträge von 1024 bis 65535 sind möglich. Dieser Wert ist bei HG 3575 nicht einstellbar.
- *Obere Grenze für RTP/RTCP-Ports*: Dieses Feld enthält den oberen Wert des zur Verfügung stehenden Portnummernbereiches für UDP-Ports. Voreingestellt ist die Portnummer 30000. Einträge von 1024 bis 65535 sind möglich. Das Feld ist bei HG 3575 nicht vorhanden.

  IMPORTANT: Bei der Portbelegung wird beginnend mit der im Feld *Untere Grenze für TRP/RTCP Ports* eingestellten Portnummer geprüft, welcher Port frei ist. Der erste freie Port wird dem RTP-Port der anstehenden Verbindung zugeordnet. Der entsprechende Port für RTCP ist der nächsthöhere Port. So wird z. B. für die erste Verbindung Port 15000 für RTP und Port 15001 für RTCP, für die zweite Verbindung Port 15002 für RTP und Port 15003 für RTCP benutzt. Bei maximal 60 möglichen Sprachverbindungen kann z. B. für die untere Grenze 15000 und für die obere Grenze 15119 eingetragen werden.

- *Verkehrsstatistik (nur SNMP)*: Mit diesem Feld schalten Sie die 'Per-Call-Statistik' ein oder aus. Falls die Statistik ausgeschaltet ist, ist kein Zugang zu den Daten der 'Per-Call-Statistik' des Gateways über SNMP möglich.
- *Intervall für Generierung von RTCP Paketen (s)*: Geben Sie in diesem Feld die Anzahl Sekunden ein, nach der RTCP-Pakete generiert werden.
- Melden schlechter Payload-Qualität (nur für HG 3575):
- Die folgenden Werte werden angezeigt, sind aber nicht einstellbar:
  - Unterer Grenzwert für 'Average Network Delay' (ms): 120
  - Oberer Grenzwert für 'Average Network Delay' (ms): 200
  - Unterer Grenzwert für Glättungsfaktor: 2
  - Oberer Grenzwert für Glättungsfaktor: 3

  Wenn einer dieser Grenzwerte unter- bzw. überschritten wird, erfolgt eine Meldung wegen schlechter Payload-Qualität.

  Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Der Dialog *MSC-Einstellungen* wird erneut angezeigt.

6.6.4.2 MSC-Einstellungen auf Lieferzustand zurücksetzen

Sie können für alle MSC-Einstellungen global die ursprünglichen Einstellungen wiederherstellen.

WBM > Konfiguration > *Sprachgateway* **>**Payload > Media Stream Control (MSC) > *MSC-Einstellungen auf Lieferzustand zurücksetzen* **>** *MSC-Einstellungen auf Lieferzustand zurücksetzen*

Der Dialog *MSC-Einstellungen auf Lieferzustand zurücksetzen* wird angezeigt und enthält eine Warnung.

Klicken Sie anschließend auf *Auf Lieferzustand zurücksetzen* und im Bestätigungsdialog auf *OK*.

6.6.5 HW-Module

Das HG 3500/3575 ist mit DSP-Modulen (DSP – digitaler Signalprozessor) ausgestattet, die Funktionalität für Sprache, Modem und Fax bieten. Wenn die Maximalanzahl der Module installiert ist, steht diese Funktionalität für bis zu 60 Sprachkanäle gleichzeitig zur Verfügung. V.90-Modem wird einschließlich PPP unterstützt (HG 3500/3575 als Server), jedoch nicht bei IP-Networking.

Sie können die DSP-Module verwalten.

WBM-Pfad:

WBM > Konfiguration > Sprachgateway **>** Payload > *HW-Module* > *DSP-Einstellungen*

Durch einen Klick auf *HW-Module* werden folgende Einträge angezeigt:

1) *DSP Jitter-Einstellungen anzeigen Alle HW-Module anzeigen*

Sie können die aktuellen Einstellungen für die DSP-Module bearbeiten.

Hintergrundinformationen:

Siehe Section 9.4, "Statischer und adaptiver Jitter-Buffer"

Der Dialog *DSP-Einstellungen* wird angezeigt. Folgende Felder können bearbeitet werden:

Allgemein:

- *Echokompensationsglied*: Echokompensation (EC) unterdrückt die Audio-Rückkoppelung (Echo-Effekt) bei Sprachübertragungen. Die Funktion entspricht G.168. Wenn Sie diese Funktion nicht zur Verfügung stellen wollen, deaktivieren Sie diese Option. Im Normalfall sollte EC jedoch stets aktiviert sein.
- *MFV-Außerband-Signalisierung*: Wenn diese Option aktiviert ist, werden MFV-Signale in einem separaten Signalisierungskanal (Außerband) übertragen. Wenn sie deaktiviert ist, werden die MFV-Signale im normalen Sprachkanal übertragen.
- *Pulsdauer eines MFV-Tons (ms):* Die Pulsdauer ist so einzustellen, dass der MFV-Ton von einer analogen Vermittlungsstelle sicher erkannt werden kann. Normalerweise liegt dieser Wert zwischen 50 und 100 ms, wobei der häufigste Wert 70 ms beträgt. Der Wertebereich für dieses Eingabefeld beträgt 50–300 ms. Der Standardwert beträgt 90 ms.

- *Pausendauer eines MFV-Tons (ms):* Die Pausendauer ist so einzustellen, dass die MFV-Töne zeitlich soweit auseinander liegen, dass sie von einer analogen Vermittlungsstelle sicher erkannt werden können. Gewöhnlich werden Pausen zwischen 20 und 50 ms eingestellt. Der Wertebereich für dieses Eingabefeld beträgt 50–300 ms. Der Standardwert beträgt 70 ms.
- *Max. Anz. Bytes für G.711:* 960. Wird nur angezeigt, kann nicht geändert werden.
- *Max. Anz. Bytes für G.723:* 96. Wird nur angezeigt, kann nicht geändert werden.
- *Max. Anz. Bytes für G.729:* 120. Wird nur angezeigt, kann nicht geändert werden.

Fax-Parameter:

- *Fehler-Korrektur-Modus*: Wenn diese Option aktiviert ist, wird einer von 2 möglichen Fehlerkorrekturmechanismen ausgewählt, die das T.38-Fax-Protokoll über UDP zur Verfügung stellt. Beide Mechanismen dienen dazu, dass eine Faxübertragung auch bei begrenzten Paketverlusten im Netzwerk fehlerfrei abläuft.
- *Fax-Kanal* mit ermitteltem Ton öffnen: Ist per Default aktiviert.
- *Anzahl redundanter Pakete*Wählen Sie aus, wie viele redundante Pakete bei den Fehlerkorrekturmechanismen ausgewählt werden. Je größer dieser Wert ist, desto robuster ist die Faxübertragung gegenüber Paketverlusten auf dem Netzwerk. Dafür steigt bei größeren Werten die benötigte Bandbreite an.
- *Maximaler Netzwerk-Jitter (ms)*: Wenn der maximale Jitter im Netzwerk bekannt ist, dann geben Sie ihn in diesem Feld ein. Dadurch verkürzt sich die Übertragungszeit bei einigen Faxgeräten. Der Wert muss als Dezimalzahl eingegeben werden. Wertebereich: 140 ms – 500 ms. Standardeinstellung: Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK* (neuen Konfigurationszustand dauerhaft speichern mit Speichern-Symbol im Steuerbereich). Der Dialog *DSP-Einstellungen* wird erneut angezeigt.

6.6.5.1 DSP Jitter-Einstellungen anzeigen

Sie können die aktuellen Einstellungen für den Jitter-Buffer ansehen.

Detail-/Hintergrundinformationen siehe Section 9.4, "Statischer und adaptiver Jitter-Buffer".

WBM-Pfad:

WBM > Konfiguration > *Sprachgateway* **>** Payload > HW-Module > *DSP Jitter-Einstellungen anzeigen* **>** *DSP Jitter-Buffer-Einstellungen*

Der Dialog *DSP-Jitter-Buffer-Einstellungen* mit den folgenden Werten wird angezeigt:

- *Jitter-Buffer-Typ*[AdaptJitterBufferEnable]: Es wird angezeigt, ob der Jitter-Buffer statisch oder adaptiv arbeitet. 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.

- *Durchschnittl. Verzögerung für Sprache (ms)* [jbAvgDelayVoice]: Es wird angezeigt, wie viele Millisekunden ein IP-Paket bei IP-basierten Sprachübertragungen durchschnittlich im Jitter-Buffer gehalten wird. Beim Jitter-Buffer-Typ *adaptiv* ist der hier vorhandene Wert lediglich ein Anfangswert. Der Wert 40 ist für die meisten Umgebungen nutzbar.
- *Max. Verzögerung für Sprache (ms)* [jbMaxDelayVoice]: Beim Jitter-Buffer-Typ *statisch* ist in dieser Zeile angegeben, 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* ist in dieser Zeile angegeben, wie viele Millisekunden die Durchschnittsverzögerung für Sprache maximal betragen darf. Ist die tatsächlich gemessene Verzögerung höher, gehen Pakete verloren. Bei statischem Jitter-Buffer ist der Wert 80 ein für die meisten Umgebungen nutzbarer Wert; bei adaptivem Jitter-Buffer beträgt der Wert 120. Der Wert ist in jedem Fall höher als derjenige im Feld *Durchschnittl. Verzögerung für Sprache (ms)*.
- *Min. Verzögerung für Sprache (ms)* [jbMinDelayVoice]: Beim Jitter-Buffer-Typ *adaptiv* ist in dieser Zeile angegeben, wie viele Millisekunden die Durchschnittsverzögerung für Sprache minimal beträgt, d. h. die Durchschnittsverzögerung ist in jedem Fall größer oder gleich diesem Wert.
- *Paket-Verlust / Verzögerungspräferenz*[jbPacketLoss]: In dieser Zeile ist für einen adaptiven Jitter-Buffer der Wert 4 eingestellt. Der Wert kann zwischen 0 und 8 betragen und beeinflusst die Gesamtverzögerung von Sprachverbindungen. Der Wert 0 bedeutet minimalen Paketverlust und Inkaufnahme von Verzögerungen im Sprachdatenstrom, der Wert 8 bedeutet minimale Verzögerung im Sprachdatenstrom und Inkaufnahme von Paketverlusten.
- *Durchschnittl. Verzögerung für Daten (ms)*[jbAvgDelayData]: In dieser Zeile ist angegeben, wie viele Millisekunden ein IP-Paket bei Datenübertragungen durchschnittlich im Jitter-Buffer gehalten wird. Der Wert 60 ist für die meisten Umgebungen nutzbar.
- *Max. Verzögerung für Daten (ms)*[jbMaxDelayData]: In dieser Zeile ist angegeben, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen bei einer Datenübertragung betragen darf, bevor der Jitter-Buffer regulierend eingreift. Der Wert 200 ist für die meisten Umgebungen nutzbar. Bei einem größeren Wert (ab ca. 2000) würde ein im Puffer komplett empfangenes Paket den Puffer sofort wieder verlassen.

6.6.5.2 Alle HW-Module anzeigen

Sie können Informationen zu einzelnen HW-Modulen ansehen.

WBM-Pfad:

WBM > Konfiguration **>** *Sprachgateway* > Payload > HW-Module > *Alle HW-Module anzeigen* **>** *HW-Module*

Der Dialog *HW-Module* wird angezeigt. Angezeigt werden der HW-Index, eine interne Identifikationsnummer, der HW-Typ (derzeit sind nur Module des Typs PDM möglich – PMC DSP Modul zur B-Kanal-Erweiterung), sowie eine eventuelle Kurzbeschreibung des Moduls.

6.6.6 Fax/Modem Ton-Behandlung

Mithilfe der Parameter im Dialog *Fax/Modem Ton-Behandlung* bestimmen Sie, ob bestimmte Fax/Modem-Tonsignale ignoriert oder verarbeitet werden sollen.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* **>** *Payload* > *Fax/Modem Ton-Behandlung*

Sie können sich die aktuellen Einstellungen der Parameter anzeigen und bearbeiten.

Der Dialog *Fax/Modem Ton-Behandlung* mit folgenden Parametern wird angezeigt.

- *Ignoriere Verarbeitung des CT Tons*: (ja/nein)
- *Ignoriere Verarbeitung des CNG Tons*: (ja/nein)
- *Ignoriere Verarbeitung des Early ANS/CED Tons*: (ja/nein)
- *Ignoriere Verarbeitung des ANS/CED Tons*: (ja/nein)
- *Ignoriere Verarbeitung des CT Tons*: (Ton, der vom rufenden Modem gesendet wird). Wenn Sie diesen Parameter aktivieren, wird der vom rufenden Modem gesendete CT-Ton ignoriert.
- – Mögliche Einstellungen: Aktiviert/Deaktiviert
  – Standardwert: Deaktiviert
- *Ignoriere Verarbeitung des CNG Tons*: (Ton, der vom rufenden Fax gesendet wird). Wenn Sie diesen Parameter aktivieren, wird der vom rufenden Fax gesendete CNG-Ton ignoriert.
- – Mögliche Einstellungen: Aktiviert/Deaktiviert
  – Standardwert: Deaktiviert
- *Ignoriere Verarbeitung des Early ANS/CED Tons*: (Schnelle Erkennung der Töne vom gerufenen Fax oder Modem.) Wenn Sie diesen Parameter aktivieren, wird der vom gerufenen Fax oder Modem gesendete Early ANS/CED-Ton ignoriert.
- – Mögliche Einstellungen: Aktiviert/Deaktiviert
  – Standardwert: Deaktiviert
- *Ignoriere Verarbeitung des ANS/CED Tons*: (Vom Modem oder Fax gesendeter Rufton.) Wenn Sie diesen Parameter aktivieren, wird der vom gerufenen Fax oder Modem gesendete ANS/CED-Ton ignoriert.
- – Mögliche Einstellungen: Aktiviert/Deaktiviert
  – Standardwert: Deaktiviert

  Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Der Dialog *Fax/Modem Ton-Behandlung* wird wieder angezeigt.

6.6.7 Mikey

Sie können Informationen zum Mikey-Verfahren ansehen (Mikey: Multimedia Internet Keying). Mikey beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln sowie weiteren Sicherheitsparametern zwischen den Teilnehmern, um eine sichere SRTP-Übertragung zu ermöglichen.

WBM-Pfad:

WBM > *Konfiguration* **>** *Sprachgateway* > *Payload* > Mikey

Im Menübaum werden die folgenden Punkte angezeigt:

1) *Mikey-Verfahren SRTP-Sicherheitsrichtlinie Mikey-Statistik*

6.6.7.1 Mikey-Verfahren

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* **>** *Payload* > Mikey > *Mikey-Verfahren*

In einer Tabelle werden Informationen zum verwendeten Mikey-Verfahren, zur Schlüsseltausch-Methode, zum Verschlüsselungsalgorithmus und zum MAC-Algorithmus angezeigt.

6.6.7.2 SRTP-Sicherheitsrichtlinie

WBM-Pfad:

WBM > *Konfiguration* **>** *Sprachgateway* > *Payload* > Mikey > SRTP-Sicherheits-richtlinie

In einer Tabelle werden Informationen zur SRTP-Sicherheitsrichtlinie angezeigt.

Es werden angezeigt:

- *Authentifizierungs-Algorithmus*
- *Länge des Authentifizierungs-Schlüssels*
- *Länge des Salting-Schlüssels*
- *Länge des Authentifizierungs-Tags*
- *Verschlüsselungsalgorithmus*
- *Länge des Verschlüsselungs-Schlüssels*
- *Häufigkeit des Schlüsselwechsels*
- *Schlüsselberechnungsfunktion*
- *SRTP Verschlüsselung aktiv*
- *SRTP Authentifizierung aktiv*
- *Länge des SRTP Vorspanns*
- *SRTCP Verschlüsselung aktiv*

6.6.7.3 Mikey-Statistik

WBM-Pfad:

WBM > *Konfiguration* **>** *Sprachgateway* > *Payload* > Mikey > Mikey-Statistik

Der Dialog wird angezeigt.

- *Schlüsseltauschs insgesamt*
- *Erfolgreich beendete Schlüsseltauschs*
- *Fehlgeschlagene Schlüsseltauschs*
- *Derzeit aktive Schlüsseltauschs*
- *Höchstzahl gleichzeitig aktiver Schlüsseltauschs*

- *Schlüsseltauschs in Initiator-Rolle*
- *Schlüsseltauschs in Responder-Rolle*
- *Schlüsseltauschs in DMC-Proxy-Rolle*

7 Wartung

In diesem Modul finden Sie Funktionen, die für die Wartung und Administration der Gateways HG 3500/3575 erforderlich sind.

WBM-Pfad:

WBM **>** *Wartung*

Links werden die Auswahlmöglichkeiten des Moduls *Wartung* angezeigt.

Auswahlmöglichkeiten im Modul 'Wartung':

1) *Konfiguration und Update Auftragsliste Traces und Ereignisse (Events) SNMP*

7.1 Konfiguration und Update

7.1.1 Konfiguration

Konfigurations- und SSL-Daten können extern gesichert und wieder geladen werden. Ferner ist das Zurücksetzen auf den Lieferzustand möglich.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration*

Die Baumstruktur für *Konfiguration* wird angezeigt.

Einträge in der Baumstruktur *Konfiguration*:

1) *Konfigurationsdaten SSL-Daten*

Saving Local Configuration for Upgrade

Konfiguration auf Lieferzustand zurücksetzen

7.1.2 Konfigurationsdaten

Sie können ein Backup und Restore von Konfigurationsdaten ausführen. Dabei können Sie genau festlegen, welche Daten gesichert oder geladen werden sollen.

Die Konfigurationsdaten sind 'Plaintext' und können mit einem beliebigen Texteditor gelesen oder ausgedruckt werden.

IMPORTANT: Sichern Sie grundsätzlich die aktuellen Konfigurationsdaten, bevor Sie ein neues Software-Image oder andere Konfigurationsdaten laden. Sollten die neu geladenen Konfigurationsdaten oder das neue Software-Image aus irgend einem Grund nicht verwendbar sein, können Sie zumindest auf den letzten Konfigurationsstand zurückgreifen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfigurationsdaten*

Die Baumstruktur für *Konfigurationsdaten* wird angezeigt.

Einträge in der Baumstruktur *Konfigurationsdaten*:

1) *Laden vom Gateway Laden zum Gateway*

7.1.2.1 Laden vom Gateway

Dies ist die Backup-Funktion. Sie können die aktuelle Konfiguration des HG 3500/3575 an einen externen Ort sichern.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfigurationsdaten* **>** *Laden vom Gateway*

Der Dialog *Laden der Konfigurationsdaten vom Gateway über HTTP* wird angezeigt. In diesem Dialog können Sie einstellen, welche Konfigurationsdaten gesichert werden sollen.

Dialog *Laden der Konfigurationsdaten vom Gateway über HTTP*:

In den einzelnen Fensterbereichen können Sie die zu sichernden Daten auswählen:

- *Optionale Parameter*:
- – *Komprimierung verwenden:* Es kann – abhängig vom zur Verfügung stehenden Speicherplatz – festgelegt werden, ob die zu sichernden Daten komprimiert werden sollen.
- *Backup für folgende Tabellen*:
- – *Alle Tabellen selektieren*: Alle nachfolgenden Tabellen werden auf *Alle* gesetzt.
  – *Alle Tabellen deselektieren*: Alle nachfolgenden Tabellen werden auf *Keine* gesetzt.

  Sie können die Tabellen auch einzeln aus- oder abwählen.
- *Trunking-Daten*: (nicht für HG 3575)
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann wird der Tabelleneintrag markiert. Bei *Keine* wird die Markierung aufgehoben.
  – Aufgelistet sind: *Berechtigung*
- *IP-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  – Folgendes kann individuell bezeichnet werden: *Globale IP-Einstellungen*, *Statische Routen*, *IP-Filter*, *MAC-Filter*, *SNTP-Server*
- *PPP/DSL-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben. Die Daten sind nicht einzeln markierbar.
  – Aufgelistet sind:

  - – Bei HG 3500 *Globale PSTN-Daten*, *Globale PSTN-Daten (Scripting)*, *PSTN-Parameter (PPP-Peer)*, *PSTN-Parameter (Rufnummern)*, *PSTN-Partner (ISDN)*, *PSTN-Partner (IP)*
  - – Bei HG 3575 *PSTN-Partner (IP)*
- *LAN-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Folgendes kann individuell bezeichnet werden: *LAN1-Schnittstelle*, *LAN2-Schnittstelle*, *PPTP/PPPoE-Parameter* (nicht für HG 3575)
- *Wahlparameter*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *Nummerntyptabelle*
- *Payload-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *Protokoll-Varianten*, *Media Stream Control (MSC)*, *DSP-Kanal-Konf.*, *QoS-Data-Collection*
- *H.323-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *H.323*, *Endpunkt-Registrierung* (nicht für HG 3575)
- *SIP-Daten*: (nicht für HG 3575)
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *SIP-Parameter*, *Internet-Telefonie-Service Provider*, *DSL-Telefonie-Teilnehmer*, *SIP-Protocol-Manager*, *Ladbare SIP-Profile*, *Sammelanschluss für SIP-Videonutzer*
- *Diagnose-Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *Trace-Komponenten* (nur bei HG 3575), *Globale Trace-einst.*, *Trace-Profile* (nur bei HG 3575), *Event-Log Konf. Event-Reaktionstabelle*, *Trap-Ziel*, *E-Mail-Liste*, *Trace über LAN Konf.*., *CPU-Monitor*, *Service-Center*
- *Sonstige Daten*:
- – *Alle*/*Keine*: Wenn die Einstellung *Alle* gewählt wird, dann werden alle in dieser Tabelle aufgelisteten Daten markiert. Bei *Keine* wird bei allen Daten dieser Tabelle die Markierung aufgehoben.
  - – Aufgelistet sind: *Globale Daten*, *Automatische Aktionen*, *Online-Hilfe*, *TFTP-Server*, *Portverwaltung (global)*, *Portverwaltung (lokal)*, *Versionsinformationen*, *Globale Netzwerk-Routing-Daten* (nicht bei HG 3575),

SCN-Fallback, *Codecs*, *Zie-Codecs*, *Class Mark* (nicht bei HG 3575), *DLS-Adressierung*

Klicken Sie nach Auswahl der zu sichernden Daten auf *Laden*. Ein Hinweisfenster wird angezeigt, das Sie mit *OK* quittieren müssen. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.1.2.2 Laden zum Gateway

Dies ist die Restore-Funktion. Sie können eine extern gespeicherte Konfiguration zum Gateway laden.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfigurationsdaten* **>** *Laden zum Gateway* **>** *Laden über HTTP*.

Der Dialog *Laden der Konfigurations-Daten zum Gateway über HTTP* wird angezeigt.

Dialog 'Laden der Konfigurations-Daten zum Gateway über HTTP':

Es werden angezeigt:

- *Remote-Dateiname (PC-Dateisystem)*: Geben Sie den Dateinamen ein, unter dem die Daten gespeichert werden.
- *Durchsuchen*: Sie können im lokalen Dateisystem nach der Sicherungsdatei suchen.

Klicken Sie am Ende auf *Laden*. Ein Hinweisfenster wird angezeigt, das Sie mit *OK* quittieren müssen. Die Daten werden nun in den Flash-Speicher des Gateways geladen, sind jedoch noch nicht wirksam.

Anschließend wird der Dialog *Wollen Sie die Konfiguration jetzt aktivieren?* angezeigt. In diesem Dialog können Sie einstellen, welche Konfigurationsdaten geladen werden sollen.

In den einzelnen Fensterbereichen können Sie die zu aktivierenden Daten auswählen. Erläuterungen dazu finden Sie im vorhergehenden Abschnitt *Laden vom Gateway*. Klicken Sie abschließend auf *Sofort aktivieren*.

Daten sichern:

Die Änderungen werden automatisch gespeichert. Führen Sie – falls erforderlich – einen Neustart durch (Reset-Symbol beachten! Siehe auch Section 4.3.2, "Symbole im Steuerbereich des WBM-Fensters").

IMPORTANT: Wenn die heruntergeladene Konfigurationsdatei erst später aktiviert werden soll, klicken Sie auf *Nicht aktivieren*. Um die Konfigurationsdaten später zu aktivieren, klicken Sie im Wartungsmenü auf *Auftragsliste* und aktivieren dann den Auftrag (siehe Section 8.3, "Auftragsliste").

IMPORTANT: Parameter für LAN Speed werden weder gespeichert noch wieder hergestellt, weil jeder LAN-Abschnitt u. U. unterschiedliche Parameter für die LAN Speed hat. Falls erforderlich, müssen diese Parameter manuell geändert werden.

7.1.3 SSL-Daten

Die VPN/SSL/SPE-Konfigurationsdaten werden beim Herunterladen vom Gateway verschlüsselt und müssen durch ein Verschlüsselungskennwort geschützt werden. Beim Laden in den Gateway muss dieses Verschlüsselungskennwort wieder angegeben werden.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *SSL-Daten*

Die Baumstruktur für *SSL-Daten* wird angezeigt.

Einträge in der Baumstruktur *SSL-Daten*:

1) *Laden vom Gateway Laden zum Gateway*

7.1.3.1 Laden vom Gateway

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *SSL-Daten* **>** *Laden vom Gateway* **>** *Laden der VPN/SSL/SPE-Konfigurationsdaten vom Gateway über HTTP*

Der Dialog *Laden der VPN/SSL/SPE-Konfigurationsdaten vom Gateway über HTTP* wird angezeigt.

Dialog *Laden der VPN/SSL/SPE-Konfigurationsdaten vom Gateway über HTTP*:

Es werden angezeigt:

- *Verschlüsselungskennwort*: Verschlüsselungskennwort für die VPN/SSL/SPE-Konfigurationsdaten eingeben.
- *Wiederholung des Verschlüsselungskennworts*: Wiederholen Sie das Verschlüsselungskennwort.

Klicken Sie nach Auswahl der zu sichernden Daten auf *Laden*. Ein Hinweisfenster wird angezeigt, das Sie mit *OK* quittieren müssen.

7.1.3.2 Laden zum Gateway

Dies ist die Restore-Funktion. Sie können eine extern gespeicherte Konfiguration zum Gateway laden.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *SSL-Daten* **>** *Laden zum Gateway*.

Der Dialog *Laden der VPN/SSL/SPE-Konfigurationsdaten vom Gateway über HTTP* wird angezeigt.

Dialog *Laden der VPN/SSL/SPE-Konfigurationsdaten vom Gateway über HTTP*:

Es werden angezeigt:

- *Remote-Dateiname (PC-Dateisystem)*: Geben Sie den gewünschten Dateinamen ein, unter dem die Daten gespeichert werden.
- *Durchsuchen*: Sie können im lokalen Dateisystem nach der Sicherungsdatei suchen.

Klicken Sie am Ende auf *Laden*. Ein Hinweisfenster wird angezeigt, das Sie mit *OK* quittieren müssen. Die Daten werden nun in den Flash-Speicher des Gateways geladen, sind jedoch noch nicht wirksam.

Anschließend wird der Dialog *Wollen Sie die Konfiguration jetzt aktivieren?* angezeigt. In diesem Dialog können Sie einstellen, welche Konfigurationsdaten geladen werden sollen.

Daten sichern:

Die Änderungen werden automatisch gespeichert. Führen Sie – falls erforderlich – einen Neustart durch (Reset-Symbol beachten. Siehe auch Section 4.3.2, "Symbole im Steuerbereich des WBM-Fensters").

IMPORTANT: Wenn die heruntergeladene Konfigurationsdatei erst später aktiviert werden soll, klicken Sie auf *Nicht aktivieren*. Um die Konfigurationsdaten später zu aktivieren, klicken Sie im Wartungsmenü auf *Auftragsliste* und aktivieren dann den Auftrag (siehe Section 8.3, "Auftragsliste").

7.1.4 Saving Local Configuration for Upgrade

Die Konfigurationsdaten der Gateways können im lokalen Flash der Baugruppe gespeichert werden. Diese Daten können wiederhergestellt werden und für den lokalen Backup und Restore während eines Loadware-Updates ohne OpenScape 4000 Assistant verwendet werden.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *Saving Local Configuration for Upgrade*

7.1.5 Konfiguration auf Lieferzustand zurücksetzen

Sie können die Konfiguration des Gateways auf die Werkseinstellung zurücksetzen, die bei der Auslieferung voreingestellt war.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *Konfiguration auf Lieferzustand zurücksetzen*

Ein wichtiger Hinweis wird angezeigt, den Sie lesen sollten:

NOTICE: Diese Aktion setzt die komplette Konfiguration auf den Lieferzustand zurück. Alle Administrations- und Kundendaten werden gelöscht! Lediglich IP-Adresse, Netzmaske und IP-Adresse des Default Routers des LAN1

bleiben erhalten. Das Gateway führt während dieser Aktion automatisch einen Reboot durch!

Klicken Sie anschließend auf *Auf Lieferzustand zurücksetzen*. Das HG 3500/3575 führt während dieser Aktion einen automatischen Reboot durch.

7.2 Software-Update

WBM-Pfad:

WBM **>** *Wartung* **>** *Software-Update*

Klicken Sie auf das Pluszeichen (+) neben dem Software-Update, um die folgenden Einträge anzuzeigen:

1) *Laden des Software-Images zum Gateway*

Laden der COMGA-Firmware via HTTP Laden der SENTA-Firmware via HTTP

7.2.1 Laden des Software-Images zum Gateway

WBM-Pfad:

WBM **>** *Wartung* **>** *Software-Update* **>** *Laden des Software-Images zum Gateway (nicht bei HG 3575)*

1) Der Dialog *Laden des Software-Images zum Gateway über HTTP* wird angezeigt. Über die Schaltfläche *Durchsuchen* kann die Datei, die das Software-Image enthält, ausgewählt und danach über die Schaltfläche *Laden* in das Gateway HG 3500/3575 geladen werden.

7.2.2 Laden der COMGA-Firmware via HTTP

WBM-Pfad:

WBM **>** *Wartung* **>** *Software-Update* **>** *Laden der COMGA-Firmware via HTTP*

Der Dialog *Laden der COMGA-Firmware zum Gateway über HTTP* wird angezeigt. Über die Schaltfläche *Durchsuchen* kann die Datei, die die COMGA-Firmware enthält, ausgewählt und danach über die Schaltfläche *Laden* in das Gateway HG 3500/3575 geladen werden.

7.2.3 Laden der SENTA-Firmware via HTTP

WBM-Pfad:

WBM **>** *Wartung* **>** *Software-Update* **>** *Laden der SENTA-Firmware via HTTP*

Der Dialog *Laden der SENTA-Firmware zum Gateway über HTTP* wird angezeigt. Über die Schaltfläche *Durchsuchen* kann die Datei, die die SENTA-Firmware enthält, ausgewählt und danach über die Schaltfläche *Laden* in das Gateway HG 3500/3575 geladen werden.

7.2.4 Zeitgesteuerte Aktivierung der Software

Es kann festgelegt werden, wann ein neues Software-Image für HG 3500/3575 installiert werden soll. Das Software-Image muss zuvor geladen worden sein.

WBM-Pfad:

WBM **>** *Wartung* **>** *Software-Update* **>** *Software-Aktivierung*

Das Fenster *Automatische Aktion* wird angezeigt. In diesem Fenster ist zu sehen, ob die Aktion aktiviert ist, wie oft sie ausgeführt wird und wann.

Aktion ändern

Hier können Sie festlegen, ob die Aktion nach Ablauf einer bestimmten Zeitdauer oder zu einem bestimmen Zeitpunkt durchgeführt werden soll.

Klicken Sie auf *Übernehmen*, um die Änderungen zu speichern. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

Hier können Sie folgende Felder bearbeiten:

- *Aktion aktiviert:* Kreuzen Sie an, ob die Aktion zu den angegebenen Zeiten automatisch gestartet werden soll oder nicht.
- *Startzeit nach Mitternacht*: Geben Sie den Zeitpunkt an, zu dem die Aktion beginnen soll.
- *Aktion an folgenden Wochentagen ausführen*: Kreuzen Sie die Wochentage an, an denen die Aktion zu der angegebenen Uhrzeit gestartet werden soll.
- Kalender verwenden: Sie können einen Kalender anzeigen, um das Datum auszuwählen, an dem die Aktion gestartet werden soll.
- Kalender ausblenden: Wählen Sie diese Option aus, um den Kalender auszublenden.

Aktion starten

Wenn eine automatische Aktion gestoppt ist (roter Listenpunkt in der Baumdarstellung), kann sie gestartet werden. Ausgeführt wird die Aktion dann zum festgelegten Zeitpunkt.

Die Baumdarstellung *Aktionen* wird aktualisiert.

Aktion stoppen

Wenn eine automatische Aktion gestartet ist (grüner Listenpunkt in der Baumdarstellung), kann sie gestoppt werden. Wenn die Aktion zum festgelegten Zeitpunkt des automatischen Starts gestoppt ist, wird sie nicht gestartet.

Die Baumdarstellung *Aktionen* wird aktualisiert.

7.3 Auftragsliste

Die Auftragsliste enthält Einträge für aktuelle Datenübertragungen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Auftragsliste*

Die Auftragsliste wird angezeigt. Die Liste hat folgende Spalten:

- *Typ*: Es wird für jeden Auftrag angezeigt, welche Aufgabe er hat, und auf welchem Weg er gestartet wurde.
- *ID*: Für jeden Auftrag wird eine eindeutige Auftragsnummer angezeigt.
- *Dauer*: Es wird angezeigt, wie viele Sekunden seit dem Start das Auftrags vergangen sind.
- *Status*: Für jeden Auftrag wird angezeigt, ob er noch in Arbeit ist oder bereits abgeschlossen wurde.
- *Aktion*:
- – Über die Schaltfläche *Abbrechen und Auftrag löschen* können Sie den entsprechenden Auftrag widerrufen.
  – Die heruntergeladene Konfiguration wird über die Schaltfläche *Konfiguration aktivieren* aktiviert.

Ferner stehen folgende Schaltflächen zur Verfügung:

- *Aktualisieren*: Die angezeigte Auftragsliste wird neu geladen und zeigt aktuelle Daten an.
- *Alle Aufträge löschen*: Alle Aufträge in der Liste werden auf einmal gelöscht. Ein Hinweisfenster muss mit *OK* bestätigt werden.
- *Alle aktivieren*: Nur dann benutzbar, wenn Aufträge für das Feature 'Multi-Gateway-Administration' vorliegen.
- *Alle speichern:* Nur dann benutzbar, wenn Aufträge für das Feature 'Multi-Gateway-Administration' vorliegen.

7.4 Traces und Ereignisse (Events)

In diesem Abschnitt werden Traces und Ereignisse (Events) im WBM beschrieben.

Weitere Details zu Traces siehe Section 9.7.2, "Traces".

Weitere Details zu Events siehe Section 9.7.3, "Events". Weitere Details zur Protokolldatei von Events siehe Section 9.7.4, "Ereignisprotokolldatei".

7.4.1 Traces

Ein Trace protokolliert eine Ausführung einer Softwarekomponente. Ein Fachmann kann mit Hilfe der Ablaufaufzeichnung die Ursache eines Fehlers finden.

IMPORTANT: Das Aktivieren von Traces kann die Performance des Systems negativ beeinflussen. Bei hoher Last kann es dazu kommen, dass die Baugruppe nicht mehr alle Trace-Informationen verarbeiten kann. Beachten Sie dazu die Informationen in Section 8.4.1.4, "Überlastung der Baugruppe durch Trace-Informationen". Wenn die Tracedatei ihre maximale Größe erreicht, wird sie geschlossen und als 'trace.bak' im gleichen Verzeichnis hinterlegt. Gleichzeitig wird eine neue (leere) 'trace.txt' angelegt.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces*

Die Baumstruktur für *Traces* wird angezeigt.

Einträge in der Baumstruktur *Traces*:

1) *Laden aller Protokolle*

Alle Protokolle löschen

Trace-Konfiguration

Laden des Trace-Protokolls

Trace-Protokoll löschen

Pcap File-Trace

pcap Tracefiles laden

rpcap Dämon

Trace-Profile

Alle Trace-Profile stoppen

Trace-Komponenten

Gestartete Trace-Komponenten anzeigen

Alle Trace-Komponenten stoppen

Secure Trace

M5T-Trace-Komponenten (nicht bei HG 3575)

M5T-Syslog-Trace

Service Center

Bei der Trace-Konfiguration legen Sie fest, ob und wie Traces geloggt werden sollen. Falls die Traces auf dem Gateway in eine Datei geloggt werden, können Sie das Trace-Protokoll dieser Datei sichern und löschen. Mit Hilfe von Trace-Profilen und Trace-Komponenten konfigurieren Sie, welche Traces in welcher Detailtiefe geloggt werden.

7.4.1.1 Laden aller Protokolle

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Laden aller Protokolle*

Der Dialog *Laden aller Protokolle* wird angezeigt.

Optionen

- *Trace-Protokoll*: Aktivierbar/Deaktivierbar. Das Trace-Protokoll kann geladen werden.
- *Event-Protokoll*: Aktivierbar/Deaktivierbar. Das Event-Protokoll kann geladen werden.
- *PPP-Protokoll*: Aktivierbar/Deaktivierbar. Das Trace-Protokoll kann geladen werden.
- *DDC-Protokoll*: Aktivierbar/Deaktivierbar. Das Trace-Protokoll kann geladen werden.

- *RAM-Trace-Protokoll*: Aktivierbar/Deaktivierbar. Das Trace-Protokoll kann geladen werden.
- *CPU-Protokoll*: Aktivierbar/Deaktivierbar. Das Trace-Protokoll kann geladen werden.

Schaltflächen

- *Keine*: Die aktivierten Kontrollkästchen werden deaktiviert.
- *Laden*: Die ausgewählten Protokolle werden geladen.
- Rückgängig: Die Änderungen werden verworfen.

7.4.1.2 Alle Protokolle löschen

Sie können alle Protokolle, die auf dem Gateway gespeichert sind, löschen. Beispiel: Trace-, Event-, PPP-, CPU- und PostMortem-Protokolle sowie Core-Logs.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Alle Protokolle löschen*

Klicken Sie zum Löschen aller Protokolle auf *Alle Protokolle löschen* löschen.

7.4.1.3 Trace-Konfiguration

Sie können überprüfen/festlegen, über welche Schnittstelle die Trace-Daten ausgegeben werden sollen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Trace-Konfiguration*

Die Trace-Konfiguration wird angezeigt. Folgende Felder können bearbeitet werden:

Konsolen-Trace

- *Synchronen Konsolen-Trace aktivieren*: Wenn diese Option aktiviert ist, erfolgt keine Pufferung von Trace-Meldungen, d.h. wenn Trace-Meldungen gerufen werden, werden diese unmittelbar auf der Konsole ausgegeben. Diese Art des Tracens bremst den Softwareablauf und sollte nur zur Diagnose eingesetzt werden. Sie ist speziell für das Tracen vor Systemabstürzen geeignet. Durch Aktivieren der Option werden alle anderen Trace-Interfaces deaktiviert.
- *Konsolen-Trace aktivieren*: Kreuzen Sie diese Option an, um die Trace-Daten auf die Konsole am V.24-Anschluss ausgeben zu lassen.

Datei-Trace

- *Datei-Trace aktivieren*: Kreuzen Sie diese Option an, um die Trace-Daten in eine Protokolldatei schreiben zu lassen.

Folgende Felder werden zur Information angezeigt:

- *Max. Größe der Trace-Datei (Byte)* : Die maximale Größe der Protokolldatei, falls die Option *Datei-Trace aktivieren* aktiviert ist.
- *Trace-Timer (s)*: Die Verzögerungszeit in Sekunden, bis Daten in die Trace-Datei geschrieben werden, falls die Option Datei-Trace aktivieren aktiviert ist.

Trace über rpcap (Wireshark)

- *rpcap Dämonen/Interface-Status*: Der Status wird angezeigt, z. B. Bereit (Dämon läuft, Server-Port 2002 ist geöffnet).
- *Trace via rpcap wurde gestartet um*: Der Status wird angezeigt, z. B. 'noch nicht begonnen'.

Allgemeine Trace-Konfiguration

- *Trace-Level überstehen Upgrade*: Aktivieren Sie diese Option, um Upgrade-Probleme zu verfolgen.

Trace über LAN (XTracer)

- *Trace über LAN (XTracer) aktivieren*: Aktivieren Sie diese Option, um die Trace-Daten über die LAN-Schnittstelle übertragen zu lassen. Beim Aktivieren wird ein Server-Port geöffnet, der für Verbindungen von einem LAN-Tracer Client aus genutzt wird. Nach dem Deaktivieren bleibt der Server Port bis zum nächsten Neustart geöffnet.

Folgende Felder werden zur Information angezeigt:

- *XTracer ist verbunden*: Angabe, ob der XTracer verbunden ist oder nicht.
- *Timer-Wert (s)*: Die Verzögerungszeit in Sekunden, bis Daten übertragen werden, falls die Option *Trace über LAN aktivieren* aktiviert ist.
- *Server Port*: Server-Port für Verbindungen von einem LAN-Tracer-Client aus.

IMPORTANT: Alle anderen Trace-Interfaces sind automatisch deaktiviert, wenn die Trace-Ausgabe über ServiceCenter/CSDA, rpcap/wireshark oder XTracer erfolgt.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.1.4 Überlastung der Baugruppe durch Trace-Informationen

Unter hoher Last können so viele Trace-Informationen anfallen, dass diese von der Baugruppe nicht mehr verarbeitet werden können. Angezeigt wird eine Überlastung an der Konsole durch die Meldung `OAM Msg Queue [...] full.. Remove Messages`'. In diesem Fall können Sie schrittweise folgendes ausprobieren:

1) Die Option *Konsolen-Trace aktivieren* deaktivieren. Sollte die Überlastung andauern:

2) Die Option *Datei-Trace aktivieren* deaktivieren. Sollte die Überlastung weiterhin andauern:

3) Aktivieren Sie die Option *Trace über LAN aktivieren*. In Verbindung mit einem Trace-Tool werden die Trace-Daten dann nicht mehr über die Baugruppe, sondern über das angeschlossene LAN verarbeitet.

Sollte die Überlast bei deaktiviertem Konsolen-Trace andauern, sind die Eventlogs auch in der Eventlog-Datei auf der Baugruppe enthalten. Die Eventlog-Datei kann von der Baugruppe geholt und angezeigt werden. So kann festgestellt werden, ob die Überlast noch anhält.

7.4.1.5 Laden des Trace-Protokolls

Wenn Datei-Trace aktiviert ist (siehe Section 8.4.1.3, "Trace-Konfiguration"), können Sie die Protokolldatei vom Gateway auf den Administrations-PC oder einen anderen Rechner laden. Außerdem können Sie die Protokolldatei löschen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Laden des Trace-Protokolls*

Laden über HTTP

Sie können die Trace-Protokolldatei vom HG 3500/3575 auf dem Administrations-PC speichern.

Nach der Auswahl des Menüpunktes *Laden über HTTP* startet das Laden der Daten. Es wird die Meldung 'Die Datei wird geladen. Bitte warten!â angezeigt.

IMPORTANT: Der Ladevorgang nimmt eine längere Zeit in Anspruch und muss von Ihnen unbedingt abgewartet werden. Wenn Sie während dieser Zeit im WBM eine andere Funktion aufrufen, wird der Ladevorgang abgebrochen.

Nachdem die Datei übertragen wurde, wird sie direkt im System-Editor angezeigt.

7.4.1.6 Trace-Protokoll löschen

Die Protokoll-Datei kann aus dem Flash-Speicher des Gateways gelöscht werden. Dies ist sinnvoll, wenn Sie zuvor ein Laden über HTTP ausgeführt haben.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Trace-Protokoll löschen*

Ein wichtiger Warnhinweis wird angezeigt. Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

7.4.1.7 Pcap File-Trace

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Pcap File-Trace*

Pcap File-Trace ist ein Diagnosemechanismus zur Aufzeichnung von pcap-Paketen an der LAN-Schnittstelle. Die Pakete werden auf eine lokale RAM-Disk geschrieben und können über WBM geladen und mit der Wireshark-Software angezeigt werden.

Konfiguration des pcap File-Tracing:

- *File-Tracing via pcap aktivieren*: Aktivierbar/Deaktivierbar. Default: deaktiviert.
- *Zeit zwischen Rotate des Tracefiles (s):* Das Protokoll verwendet die pcap-Größe und die geschätzte Zeit als Kriterien für die Erstellung neuer und die Komprimierung alter Protokolldateien.

7.4.1.8 pcap Tracefiles laden

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *pcap Tracefiles laden*

Der Dialog *pcap Tracefiles laden* wird angezeigt.

- *Dateiname*
- *Geändert*
- *Größe (in Byte)*

7.4.1.9 rpcap Dämon

NOTICE: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *rpcap Dämon* **>** *rpcap Dämon starten*

Das Fenster *rpcap starten* wird angezeigt. Gehen Sie vor, wie im Section 8.4.1.10, "Überwachung von IP-Datenpaketen mit rpcap und Wireshark (Ethereal)" beschrieben.

rpcap Dämon stoppen

Das Fenster *rpcap Dämon stoppen* wird angezeigt. Gehen Sie vor, wie im Section 8.4.1.10, "Überwachung von IP-Datenpaketen mit rpcap und Wireshark (Ethereal)" beschrieben.

7.4.1.10 Überwachung von IP-Datenpaketen mit rpcap und Wireshark (Ethereal)

IMPORTANT: Zusätzlich zu diesem Abschnitt werden im Fenster 'rpcap Dämon starten' (Wartung **>** Traces und Ereignisse (Events) **>** *Traces* **>** *rpcap Dämon*) wichtige Hinweise gegeben, die Sie beachten sollten.

Übersicht

Tracen über die HIP-Schnittstelle

Die Schnittstelle zwischen OpenScape 4000 und HG 3500 lasst sich nicht direkt tracen. Es sind allerdings externe Verbindungen zur Schnittstelle über die LAN-Schnittstellen (LAN1: emac0 oder LAN2: emac1) tracebar. Durch das Starten des rpcap-Dienstes wird ein Server-Port der HG 3500 geöffnet. Dies ermöglicht einen direkten Zugriff auf TCP/IP-Pakete durch ein IP-Tracetool, wie z. B. Wireshark (Ethereal).

Wireshark ist ein Programm zur Analyse von Netzwerk-Kommunikationsverbindungen. Es zeichnet die Datenpakete der HG 3500 auf und stellt sie übersichtlich in einer Tabelle dar.

rpcap (Remote Packet Capture)

Das Protokoll rpcap erlaubt, ein Programm wie z.B. Wireshark als Server auf dem Zielsystem laufen zu lassen, welches Datenpakete erfasst und zu einem Client überträgt. Vom Client werden die Datenpakete bearbeitet, analysiert und archiviert.

Überwachung durchführen

Für die Überwachung der HG 3500-Datenpakete sind im WBM der HG 3500 der rpcap-Dienst und auf dem Administrator-PC das IP-Tracetool Wireshark einzurichten und zu starten.

1) rpcap-Dienst der HG 3500 einrichten und starten

2) Gehen Sie im WBM der HG 3500 wie folgt vor:

a) WBM starten.

Als Entwickler anmelden.

Über Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *rpcap Dämon* **>**das Fenster *rpcap-Dämon starten* öffnen.

Im Feld *IP-Adresse (numerisch oder literal)* die folgenden Eingaben vornehmen:

a) IP-Adresse der HG 3500 (numerisch oder literal)

b) • Port der HG 3500

Auf *Übernehmen* klicken, um den rpcap Dämon zu starten. Ein Server-Port der HG 3500 wird geöffnet.

3) Wireshark einrichten und Überwachung starten

4) Gehen Sie im Wireshark wie folgt vor:

   a) Programm starten.

   Über *Erfassung -> Optionen* das Fenster 'Wireshark: Erfassungsoptionen' öffnen.

   Im Auswahl- und Eingabefeld 'Interface:' Folgendes eintragen:

   `rpcap://<IP-Adresse der HG 3500>/emac0`

   oder:

   `rpcap://<IP-Adresse der HG 3500>/emac1`

   Es werden nur die HG 3500-Datenpakete überwacht.

   Im Auswahl- und Eingabefeld 'Capture Filter:' Folgendes eintragen:

   `not host <IP-Adresse des Administrator-PCs>`

   Die Datenpakete des Administrator-PCs werden ausgeschlossen.

   Ggf. weitere Einstellungen vornehmen, siehe www.wireshark.org.

   Auf *Start* klicken, um mit der Erfassung der Datenpakete zu beginnen. Der Datenstrom, der von der HG 3500 kommt, wird angezeigt.

5) **Überwachung beenden**

6) Gehen Sie zum Beenden der Überwachung unbedingt in der folgenden Reihenfolge vor, um einen Absturz der HG 3500 zu vermeiden:

   a) Wireshark stoppen über *Capture -> Stop*.

   Den rpcap Dämon der HG 3500 stoppen:

   Im WBM überWartung **>** Traces und Ereignisse (Events) **>** *Traces* **>** rpcap Dämon das Fenster 'rpcap-Dämon stoppen' öffnen. Unter 'Client-Identifikation für Zugriffskontrolle' wird im Feld 'IP-Adresse (numerisch oder literal):' die oben eingegebene IP-Adresse der HG 3500 angezeigt.

   Auf *Übernehmen* klicken, um den rpcap Dämon zu stoppen. Der Server-Port der HG 3500 wird geschlossen, ein Zugriff z. B. über Wireshark ist nicht mehr möglich.

7.4.1.11 Trace-Profile

Trace-Profile legen fest, welche Daten in welcher Detailtiefe geloggt werden sollen. Einem Trace-Profil werden Trace-Komponenten (siehe Section 8.4.2, "Ereignisse (Events)") zugewiesen. Auf diese Weise wird festgelegt, für welche Gateway-Komponenten ein Trace-Profil Prozess- und Zustandsinformationen loggen soll. Die Detailtiefe der Logs kann über Trace-Levels eingestellt werden.

Sie können eigene Trace-Profile anlegen, ändern und löschen. Darüber hinaus stehen vordefinierte Trace-Profile zur Verfügung. Alle Trace-Profile können Sie gemeinsam stoppen und einzeln starten oder stoppen. Durch Starten eines Trace-Profils wird das Logging dieses Profils aktiviert, und durch Stoppen deaktiviert.

Siehe auch: Section 10.1.2, "Trace-Profile".

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Trace-Profile*

Klicken Sie auf das Pluszeichen (+) neben *Trace-Profile* , um die einzelnen Trace-Profile anzuzeigen. Trace-Profile mit einem grünen Listenpunkt sind gestartet, und Trace-Profile mit rotem Listenpunkt sind gestoppt.

Sie können eine Liste aller vordefinierten und selbst erstellten Trace-Profile ansehen.

Der Dialog *Liste der Trace-Profile* wird angezeigt. Für jedes Trace-Profil wird der Profilname angezeigt, sowie die Statusinformation, ob das Trace-Profil gestartet ist oder nicht.

Alle Trace-Profile anzeigen

Sie können eine Liste aller vordefinierten und selbst erstellten Trace-Profile ansehen.

Der Dialog *Trace-Profil: [Name]* wird angezeigt. Angezeigt wird der Profilname, sowie die Statusinformationen, ob das Trace-Profil schreibgeschützt ist, und ob es aktuell gestartet ist oder nicht. In der Tabelle unterhalb wird aufgelistet, welche Trace-Komponenten in dem Trace-Profil berücksichtigt sind, und welche Trace-Levels dabei eingestellt sind.

7.4.1.12 Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)

Sie können ein neues, eigenes Trace-Profil erstellen. Das Profil übernimmt dabei alle aktuell gestarteten Trace-Komponenten und deren eingestellte Trace-Levels (siehe Section 8.4.2, "Ereignisse (Events)" und Section 8.4.1.17, "Secure Trace").

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Trace-Profile* **>** *Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)*

Der Dialog *Trace-Profil hinzufügen* wird angezeigt. Folgendes Feld können Sie bearbeiten:

- *Profilname*: Geben Sie dem Profil einen sinnvollen Namen.

In der Tabelle unterhalb werden die aktuell gestarteten Trace-Komponenten aufgelistet. In der linken Spalte steht jeweils der Name der Trace-Komponente. Die beiden nächsten Spalten können Sie für jede Trace-Komponente bearbeiten:

- *Enthalten*: Kreuzen Sie das Feld an, wenn die entsprechende Trace-Komponente in diesem Trace-Profil berücksichtigt werden soll.
- *Level*: Geben Sie an, mit welcher Genauigkeit (Trace-Level) die entsprechende Trace-Komponente in diesem Profil arbeiten soll. Trace-Level haben einen Wertebereich von 0 bis 9. Dabei steht 0 für die geringste und 9 für die größte Detailinformation. Mit steigender Zahl steigt also die Anzahl der Trace-Informationen.

Folgende Schaltflächen stehen am Tabellenende zur Verfügung:

- *Keine* oder *Alle* (in der Spalte *Enthalten*): Klicken Sie auf diese Schaltfläche, um alle aufgelisteten Trace-Komponenten auf einmal in dem aktuellen Profil zu berücksichtigen oder keine davon.
- *Alle setzen auf 0*, *Alle setzen auf 3*, *Alle setzen auf 6* oder *Alle setzen auf 9* in der Spalte *Level*: Klicken Sie auf diese Schaltfläche, um einen

einheitlichen Trace-Level zu konfigurieren. Wiederholen Sie dies gegebenenfalls.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Das angelegte Trace-Profil erscheint nun in der Baumdarstellung der *Ereignisse (Events)* und in der Liste der Trace-Profile (siehe Section 8.4.1.11, "Alle Trace-Profile anzeigen").

7.4.1.13 Alle Trace-Profile stoppen

Sie können alle gestarteten Trace-Profile (siehe Section 8.4.1.14, "Trace-Komponenten") auf einmal stoppen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** Traces **>** *Alle Trace-Profile stoppen*

Die Baumdarstellung *Traces* wird aktualisiert.

7.4.1.14 Trace-Komponenten

Trace-Komponenten sind Gateway-Komponenten, für die Prozess- und Zustandsinformationen geloggt werden können. Sie können die Einstellungen von Trace-Komponenten ändern und ansehen sowie die Überwachung durch Trace-Komponenten ein- und ausschalten.

Siehe auch: Section 10.1.1, "Trace-Komponenten".

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** *Trace-Komponenten*

Trace-Komponenten (Ordner):

Klicken Sie auf das Pluszeichen (+) neben *Trace-Komponenten*, um die einzelnen Trace-Komponenten anzuzeigen. Trace-Komponenten mit einem grünen Listenpunkt sind gestartet, und Trace-Komponenten mit rotem Listenpunkt sind gestoppt.

Der Dialog *Alle Trace-Komponenten* bearbeiten wird angezeigt. Für jedes Trace-Profil wird der Subsystem-Name angezeigt, der Komponenten-Index, das eingestellte Trace-Level sowie die Statusinformation, ob die Trace-Komponente aktuell gestartet ist oder nicht.

Sie können eine Liste aller aktuell gestarteten Trace-Komponenten ansehen.

Für jedes Trace-Profil werden der Subsystem-Name und das eingestellte Trace-Level angezeigt.

Sie können eine Liste aller Trace-Komponenten mit Detaildaten aufrufen und dabei Angaben zum Trace-Level ändern.

Für jedes Trace-Profil wird der Subsystem-Name angezeigt. Folgende Felder können bearbeitet werden:

- *Trace-Level*: Geben Sie an, mit welcher Genauigkeit (Trace-Level) die entsprechende Trace-Komponente arbeiten soll. Trace-Level haben einen

Wertebereich von 0 bis 9. Dabei steht 0 für die geringste und 9 für die größte Detailinformation. Mit steigender Zahl steigt also die Anzahl der Trace-Informationen.

- *Trace an*: Kreuzen Sie das Feld an, um die entsprechende Trace-Komponente zu starten.

IMPORTANT: Es gibt Trace-Komponenten, die nicht oder nur eingeschränkt änderbar sind. Nicht änderbare Elemente einer Trace-Komponente sind grau dargestellt.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.1.15 Gestartete Trace-Komponenten anzeigen

Sie können Detail-Daten zu einer einzelnen Trace-Komponente ansehen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Traces* **>** ausgewählte Trace-Komponente **>** *Liste der gestarteten Trace-Komponenten*

Der Dialog *Trace-Komponente: [Name]* wird angezeigt. Angezeigt wird der Trace-Komponenten-Index, der Subsystem-Name, das eingestellte Trace-Level, und ob das Trace-Level aktuell gestartet ist oder nicht. Im Bereich *In der Trace-Ausgabe enthaltene Daten* wird aufgelistet, welche Trace-Daten zu dieser Trace-Komponente geloggt werden. Genaue Feldbeschreibungen siehe Section 8.4.1.14, "Trace-Komponenten".

7.4.1.16 Alle Trace-Komponenten stoppen

Sie können eine Liste aller aktuell gestoppten Trace-Komponenten ansehen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** Traces **>** *Gestoppte Trace-Komponenten anzeigen*

Der Dialog *Liste der gestoppten Trace-Komponenten* wird angezeigt.

7.4.1.17 Secure Trace

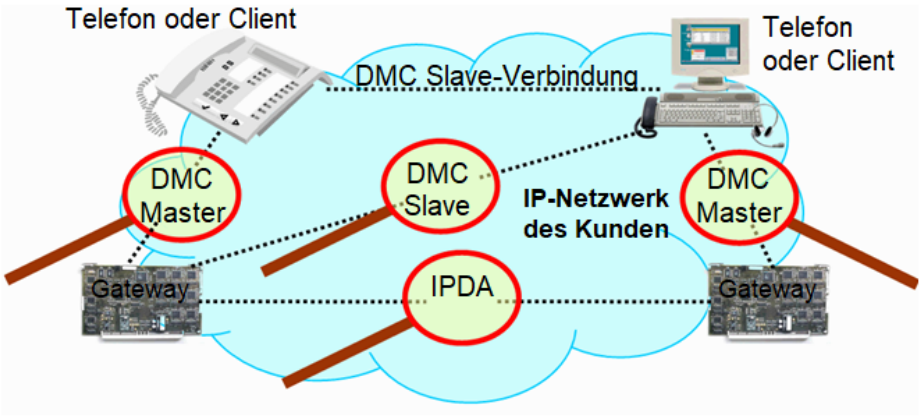
WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *Secure Trace*

Was ist ein Secure Trace?

Secure Trace ist eine Funktion zur Erkennung von Fehlfunktionen im OpenScape-System. Sie erzeugt Informationen zu verschlüsselten VoIP Benutzer- und Signalisierungsdatenströmen vom und zum Common Gateway.

IMPORTANT: In diesem Dokument bezieht sich der Begriff Gateway auf das HG 3500 Gateway von OpenScape 4000 V10.



Ein Secure Trace kann für die folgenden Verbindungen aufgezeichnet werden:

- DMC Master-Verbindungen (Gateway<-> Client/Telefon)
- DMC Slave-Verbindungen (Gateway<-> Client/Telefon)
- Standard SIP-Verbindungen (Gateway <-> Client/Telefon)
- CorNet-IP NQ Vernetzung (Gateway <-> Gateway)
- SIP-Q Vernetzung (Gateway <-> Gateway)
- IPDA Connectivity (SL200 <-> Gateway)

Der Secure Trace enthält verschlüsselte Aufzeichnungen. Die darin enthaltenen Informationen können vom Entwickler mit einem passenden Schlüssel entschlüsselt werden.

Ablauf der Secure Trace-Erstellung:

Zum Erstellen eines Secure Trace ist der folgende Ablauf einzuhalten:

1) Der Servicetechniker stellt ein Problem im Netzwerk des Kunden fest. In einer Besprechung mit dem Entwickler wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.

2) Der Kunde wird von der Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Danach gibt der Kunde eine Bestellung zum Erzeugen eines Secure Trace auf, in der Beginn und Ende (mit Datum und Uhrzeit) der Überwachung genannt sind.

3) Der Entwickler erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit dem Schlüsselpaar kann nur ein einziger Secure Trace erstellt werden. Die Zertifikate werden folgendermaßen verwendet:

4)
- Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden.
- Das Zertifikat mit dem öffentlichen Schlüssel wird an den Servicetechniker übergeben.

5) Der Servicetechniker informiert den Kunden über den Beginn der Trace-Aktivitäten. Der Kunde muss die betroffenen Teilnehmer informieren.

IMPORTANT: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, wenn die betroffenen Teilnehmer nicht informiert wurden.

1) Der Servicetechniker stellt den CGWs, für die ein Secure Trace zu erstellen ist, das Zertifikat zur Verfügung, siehe Section 8.4.1.18, "Secure Trace Einstellungen".
2) Der Servicetechniker aktiviert die Secure Trace-Funktion. Ein Secure Trace wird erstellt. Die Aktivierung und die spätere Deaktivierung werden von den beteiligten OpenScape-Systemen protokolliert.
3) Nachdem der Secure Trace erstellt wurde, wird der Kunde über das Ende der Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom System.
4) Der Secure Trace wird dem Entwickler zur Verfügung gestellt.
5) Der Entwickler entschlüsselt den Secure Trace, indem er den privaten Schlüssel anwendet. Danach analysiert er die entschlüsselten Aufzeichnungen.
6) Nach dem Ende der Analyse müssen alle relevanten Materialien und Daten auf eine sichere Art und Weise zerstört werden. Dies beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie des Secure Trace nicht mehr entschlüsselt werden kann.

7.4.1.18 Secure Trace Einstellungen

Sie können Eigenschaften und Einstellungen des Gateways ansehen und ändern.

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *Secure Trace* **>** *Secure Trace Einstellungen*

Secure Trace Status

In diesem Dialog können Sie feststellen, ob gerade ein Secure Trace erstellt wird.

Der Dialog *Secure Trace Status* erscheint. Folgende Daten werden angezeigt:

- *Secure Trace aktiviert*: Dieses Feld zeigt an, ob gerade ein Secure Trace erstellt wird.
- *Automatischer Deaktivierungszeitpunkt*: Diese Feld zeigt an, wann der Secure Trace voraussichtlich abgeschlossen ist und die Secure Trace-Funktion automatisch deaktiviert wird.
- *Secure Trace für folgende Protokolle*: Dieses Feld zeigt an, für welche Protokolle der Secure Trace erstellt wird. Verfügbare Optionen: Das können sein: TC (TLS), H.323 Core/HSA (TLS), MMX (PEP), SIP Core/SSA (TLS), MSC (SRTP).

7.4.1.19 Secure Trace einschalten

Voraussetzungen:

Sie können den Secure Trace nur dann einschalten, wenn die folgenden Voraussetzungen vorliegen:

- Der Secure Trace ist noch nicht aktiviert.
- Der Kunde hat die Erstellung des Secure Trace veranlasst und möchte seine *Secure Trace Aktivierungs-Passphrase* in das WBM eingeben (Passphrase: ein aus mehreren Wörten bestehendes Passwort, 20 Zeichen maximale Länge).
- Sie haben einen öffentlichen Schlüssel vom Entwickler bekommen und in das WBM geladen.

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *Secure Trace* **>** *Secure Trace einschalten*

Vorgehensweise:

Führen Sie zum Starten des Secure Trace die folgenden Schritte durch:

1) Auswählen:WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *Secure Trace* **>** *Secure Trace starten.* Der Dialog *Secure Trace einschalten* wird angezeigt.
2) Geben Sie im Feld 'Start Parameter' die folgenden Daten ein:
3) • *Secure Trace Aktivierungs-Passphrase*: Um die Nutzung der Secure Trace-Funktion zu begrenzen, wird die Aktivierung durch eine besondere Passphrase, die nur der Kunde kennt, geschützt. Somit ist diese Passphrase der Schlüssel des Kunden und das Zertifikat der Schlüssel des Servicetechnikers. Beide Schlüssel sind notwendig, um die Secure Trace-Funktion zu aktivieren.
   • *Dauer des Secure Trace (s)*: Das ist ein Pflichtfeld.
4) Legen Sie die Protokolle fest, für die ein Secure Trace erstellt werden soll: Alle Protokolle im Bereich 'Secure Trace für folgende Protokolle' sind standardmäßig aktiviert. Deaktivieren Sie die Protokolle für die kein Secure Trace erstellt werden soll:
5) • TC (TLS)
   • H.323 Core/HSA (TLS)
   • MMX (PEP)
   • SIP Core/SSA (TLS)
   • MSC (SRTP)
6) Klicken Sie auf die Schaltfläche *Secure Trace einschalten*. Der Secure Trace wird erstellt.

7.4.1.20 Secure Trace beenden

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** *Secure Trace* **>** *Secure Trace beenden*

Vorgehensweise:

Klicken Sie im Fenster 'Secure Trace beenden' auf die Schaltfläche *Secure Trace beenden*.

7.4.1.21 Secure Trace Zertifikat

WBM-Pfad:

WBM > Wartung > Traces und Ereignisse (Events) > Traces > Secure Trace > *Secure Trace Zertifikat (nur für HG 3575)*

Nachdem das Secure Trace Zertifikat importiert wurde, wird es hier angezeigt, siehe Abschnitt: Section 8.4.1.21, "Secure Trace Zertifikat"

7.4.1.22 Zertifikat importieren (PEM oder Binär-Format)

Zertifikat:

Dieses Zertifikat ist die Voraussetzung dafür, dass ein Secure Trace erstellt werden kann. Sie bekommen es vom Entwickler. Es enthält den öffentlichen Schlüssel und muss im PEM- oder im binären Format vorliegen. Das Zertifikat ist maximal einen Monat gültig.

WBM-Pfad:

WBM > Wartung > Traces und Ereignisse (Events) > Traces > *Secure Trace* > *Zertifikat importieren (PEM oder Binär-Format)* > *Laden des Secure Trace Zertifikats über HTTP.*

Vorgehensweise:

Führen Sie zum Importieren des Zertifikats die folgenden Schritte durch:

1) Auswählen:WBM > Wartung > Traces und Ereignisse (Events) > Traces > *Secure Trace* > *Zertifikat importieren (PEM oder Binär-Format)* > *Laden des Secure Trace Zertifikats über HTTP*. Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
2) Wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus, die das Zertifikat enthält und bestätigen Sie mit *Öffnen*. Die Datei wird geladen.
3) Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

Prüfen Sie den Fingerabdruck (hexadezimale Zahl). Wenn ein Zertifikat verändert wurde, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden, darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.

Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

1) Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

Das Erstellen des Secure Trace ist nun möglich.

7.4.1.23 M5T-Trace-Komponenten (nicht bei HG 3575)

WBM-Pfad:

WBM **>** Wartung **&gt** Traces und Ereignisse (Events) **&gt** Traces **&gt** M5T-Trace-Komponenten (nicht bei HG 3575) *Alle Trace-Komponenten bearbeiten*

Der Dialog *Alle Trace-Komponenten bearbeiten* wird angezeigt. Die Tabelle enthält die folgenden Parameter:

- *Package-Name*: Name der Trace-Komponente, nicht änderbar
- *Trace-Level*: Wertebereich 0 bis 9
- *Trace an*: Ja/Nein

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

Package anzeigen

Im Dialog *M5T-Trace-Package: <Name der Trace-Komponente>* wird das Package der Trace-Komponente angezeigt. Beschreibung der einzelnen Parameter, siehe M5T-Trace-Package.

M5T-Trace-Package

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T-Trace-Komponenten (nicht bei HG 3575) **>** *<Trace-Komponente>* **>** *M5T-Trace-Package*

Der Dialog *M5T-Trace-Package: <Name der Trace-Komponente>* wird angezeigt. Das Package enthält die folgenden Parameter:

- *Package-Name*: Name der Trace-Komponente, nicht änderbar
- *Index*: Nicht änderbar
- *Trace-Level*: Wertebereich 0 bis 9
- *Trace an*: Ja/Nein

Trace-Komponente starten

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T-Trace-Komponenten (nicht bei HG 3575) *<Nicht aktive Trace-Komponente>* **>** *Trace an*

Der Trace wird gestartet. Das Symbol vor dem Modulnamen wechselt von schwarz (Standard) auf grün.

Trace-Komponente stoppen

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T-Trace-Komponenten (nicht bei HG 3575) *<Aktive Trace-Komponente>* **>** *Trace aus*

Der Trace wird gestoppt. Das Symbol vor dem Modulnamen wechselt von schwarz (Standard) auf rot.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.1.24 M5T-Syslog-Trace

Das Fenster M5T-Syslog-Trace wird angezeigt. Angezeigt wird folgender Parameter:

Adresse, an die der M5T-Trace gesendet werden soll:

- IP Address (IP-Adresse)
- Port: Z. B. (6000)

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.1.25 Service Center

Das Service Center ist ein zusätzliches Diagnosetool für Entwickler.

NOTICE: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T-Trace-Komponenten (nicht bei HG 3575) *Service Center*

Das Fenster *Service Center* wird angezeigt. Es enthält die Einstellungen des Service Centers, d. h. ob es aktiviert ist und dessen Server-Port.

Über das Kontrollkästchen *Service Center aktivieren* kann das Service Center aktiviert oder deaktiviert werden.

7.4.2 Ereignisse (Events)

Ereignisse (Events) informieren über Probleme im System. Der Administrator sollte die Konfiguration des Netzwerks oder des Gateways überprüfen, um die irreguläre Situation zu korrigieren.

Weitere Details zu Events siehe Section 9.7.3, "Events". Weitere Details zur Protokolldatei von Events siehe Section 9.7.4, "Ereignisprotokolldatei".

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Ereignisse (Events)*

Klicken Sie auf das Pluszeichen (+) neben *Ereignisse (Events)*, um die folgenden Einträge anzuzeigen:

1) *Event-Konfiguration E-Mail Reaktionstabelle Diagnose Logs holen*

Diagnose Logs löschen

7.4.2.1 Event-Konfiguration

Sie können die Einstellungen der Event-Konfiguration ansehen und einstellen, ob die Event-Protokollierung über ein LAN übertragen werden soll.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Ereignisse (Events)* **>** *Event-Konfiguration*

Sie können die aktuellen Einstellungen der Event-Konfiguration ansehen.

Der Dialog *Event-Konfiguration* wird angezeigt. Feldbeschreibungen siehe unten.

Event-Konfiguration ändern

Für die Event-Protokollierung über LAN wird ein Tool wie z. B. TMT-Tracer oder X-Trace benötigt. Sie können die Event-Protokollierung über LAN ein- und ausschalten.

Event-Datei-Einstellungen

Folgende Felder werden zur Information angezeigt:

- *Max. Größe des Event-Buffers (Byte)*: Die Menge an Protokolldaten, die im Zwischenspeicher gehalten wird.
- *Max. Größe der Event-Datei (Byte)*: Die maximale Größe der Protokolldatei.
- *Event-Timer (s)*: Die Verzögerungszeit in Sekunden, bis Daten in die Protokolldatei geschrieben werden.

Event über LAN (XTracer)

Folgendes Feld können Sie bearbeiten:

- *Event-Protokollierung über LAN aktivieren*: Mit dieser Option können Sie die Event-Protokollierung aktivieren und deaktivieren.

Folgendes Feld wird zur Information angezeigt:

- *Timer-Wert (s)*: Die Verzögerungszeit in Sekunden, bis Daten übertragen werden.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.2.2 E-Mail

Sie können überprüfen und einstellen, an welche E-Mail-Adresse bei Eintreten eines Events eine Warnung gesendet wird.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Ereignisse (Events)* **>** *E-Mail-Einstellungen*

Sie können Detaildaten für den Mailversand bei Eintreten eines Events ansehen.

Der Dialog *E-Mail-Einstellungen* wird angezeigt. Feldbeschreibungen siehe Section 8.4.2.2, "E-Mail-Einstellungen bearbeiten".

E-Mail-Einstellungen bearbeiten

Sie können Detaildaten für den Mailversand bei Eintreten eines Events ändern.

Der Dialog *E-Mail-Einstellungen* wird angezeigt. Folgende Felder können bearbeitet werden:

- *SMTP-Server (IP-Adresse)*: Geben Sie die IP-Adresse des Rechners an, über den die Mails via SMTP-Protokoll versendet werden. Wählen Sie einen SMTP-Server ohne Authentifizierung aus, da das HG 3500/3575 bezüglich SMTP keinen Authentifizierungsmechanismus unterstützt.
- *SMTP-Server (Port)*: Geben Sie den Server-Port für das SMTP-Protokoll ein. Default-Wert ist 25.

- *SMTP-Domäne* Geben Sie den Domain-Namen des Rechners an, über den die Mails via SMTP-Protokoll versendet werden. Die SMTP-Domain entspricht dem Domain-Namen des Mail-Servers.

  IMPORTANT: Halten Sie die Konventionen gemäß RFC 821 und RFC 822 ein. Die SMTP-Server-Einstellungen sind erforderlich, weil das HG 3500/3575 nur die 'Relay-Agent'-Funktion unterstützt und selbst nicht als SMTP-Server eingesetzt werden kann.

- *Absender*: Geben Sie ein, was in den Benachrichtigung-E-Mails im Absender-Feld angezeigt werden soll.
- *Betreff*: Geben Sie ein, was in den Benachrichtigung-E-Mails im Betreff-Feld angezeigt werden soll. Der Betreff sollte eindeutig auf eine Meldung aus dem Eventlog hindeuten.
- *Empfänger 1* bis *Empfänger 5*: Geben Sie in diesen Feldern bis zu fünf E-Mail-Adressen ein. Benachrichtigungs-E-Mails werden an alle eingetragenen Mail-Adressen geschickt.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.2.3 Reaktionstabelle

Sie können für *Ereignisse (Events)* getrennt einstellen, wie bei einem Eintreten reagiert werden soll.

NOTICE: Die Events in dieser Reaktionstabelle sind beschrieben im *Übersicht: Event-Codes*.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** *Ereignisse (Events)* **>** *Reaktionstabelle* **>** *Einstellung der Reaktionen zu Events*

Reaktionstabelle (Ordner):

Klicken Sie auf das Pluszeichen (+) neben *Reaktionstabelle*, um die einzelnen Trace-Profile anzuzeigen. Klicken Sie auf eine einzelne Event-Meldung, um das Fenster *Einstellung der Reaktionen zu Events* anzuzeigen.

Alle Events bearbeiten

Im Dialog *Einstellung der Reaktionen zu Events* werden Details der einzelnen Events übersichtlich in einer einzigen Tabelle dargestellt.

Für jedes Event werden folgende Informationen angezeigt:

- *Event-Name*: Der interne Name des Events wird angezeigt.
- *SNMP-Traps senden*: Es wird angezeigt, ob bei Eintreten des Events ein SNMP-Trap gesendet wird (siehe Section 8.5.3, "Traps").

Für jedes Event können folgende Einstellungen geändert werden:

- *E-Mail versenden*: Wenn diese Option angekreuzt ist, wird beim Auftreten dieses Events eine E-Mail versandt (siehe Section 8.4.2.2, "E-Mail").

- *Zugeordnetes Trace-Profil*: Sie können diesem Event eines der vorhandenen Trace-Profile zuordnen (siehe Section 8.4.2, "Ereignisse (Events)").
- *Trace-Profil starten/stoppen*: Sie können festlegen, ob das gewählte Trace-Profil durch dieses Event gestartet oder gestoppt werden soll.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

WBM-Pfad:

WBM **>** *Wartung* **>**Traces und Ereignisse (Events) **>** *Ereignisse (Events)* **>** *Reaktionstabelle* **>** ausgewähltes Event **>** *Einstellung der Reaktionen zu Events*

Der Dialog *Einstellung der Reaktionen zu Events* wird angezeigt. Feldbeschreibungen siehe Section 8.4.2.3, "Event bearbeiten".

Event bearbeiten

Folgende Felder werden zur Information angezeigt:

- *Event-Name*: Der interne Name des Events wird angezeigt.
- *SNMP-Traps senden*: Es wird angezeigt, ob bei Eintreten des Events ein SNMP-Trap gesendet wird (siehe Section 8.5.3, "Traps").
- *Gateway neu starten*: Es wird angezeigt, ob bei Eintreten des Events das Gateway neu gestartet werden muss.
- *OpenScape benachrichtigen*: Es wird angezeigt, ob bei Eintreten des Events eine Meldung an das OpenScape-System erfolgt.

Folgende Felder können bearbeitet werden:

- *E-Mail versenden***:** Wenn diese Option angekreuzt ist, wird beim Auftreten dieses Events eine E-Mail versandt (siehe Section 8.4.2.2, "E-Mail").
- *Zugeordnetes Trace-Profil*: Sie können diesem Event eines der vorhandenen Trace-Profile zuordnen (siehe Section 8.4.2, "Ereignisse (Events)").
- *Trace-Profil starten/stoppen*: Sie können festlegen, ob das gewählte Trace-Profil durch dieses Event gestartet oder gestoppt werden soll.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.2.4 Diagnose Logs holen

WBM-Pfad:

WBM **>** *Wartung* **>**Traces und Ereignisse (Events) **>** *Ereignisse (Events)* **>** *Diagnose Logs holen* **>** *Laden der Diagnose Logs vom Gateway über HTTP*

Sie können die vom Gateway erzeugten Diagnose Logs in einer Tabelle ansehen und über HTTP laden.

Die Tabelle *Laden der Diagnose Logs vom Gateway über HTTP* wird angezeigt. Es werden zu jedem verfügbaren Log der zugehörige Dateiname, die Dateigröße in Bytes, der Zeitpunkt der letzten Änderung und die Dateiattribute angezeigt.

7.4.2.5 Diagnose Logs löschen

Sie können die Diagnose Logs löschen.

WBM-Pfad:

WBM **>** *Wartung* **>**Traces und Ereignisse (Events) **>** *Ereignisse (Events)* **>** *Diagnose Logs löschen*

Das Löschen der Diagnose Logs muss von Ihnen durch Klicken auf die Schaltfläche *Protokoll löschen* bestätigt werden.

7.4.3 Admin.-Protokoll

Das Administrationsprotokoll wird auf dem Gateway erzeugt. Protokolliert werden Logins auf dem Gateway. Sie können die Sprache des Protokolls überprüfen und einstellen. Ferner können Sie die Protokolldatei vom Gateway herunterladen.

WBM-Pfad:

WBM **>** *Wartung* **>** Traces und Ereignisse (Events) **>** *Admin.-Protokoll*

Klicken Sie auf das Pluszeichen (+) neben *Admin.-Protokoll*, um die folgenden Einträge anzuzeigen:

1) *Konfiguration Admin.-Protokoll-Daten laden*

7.4.3.1 Konfiguration

Sie können die Sprache des Administrationsprotokolls auf dem Gateway überprüfen und einstellen.

WBM-Pfad:

WBM **>** *Wartung* **>**Traces und Ereignisse (Events) **>** *Admin.-Protokoll* **>** *Konfiguration* **>** *Admin.-Protokoll-Konfiguration*

Sie können eine andere Sprache für das Administrationsprotokoll einstellen.

Der Dialog *Admin.-Protokoll-Konfiguration* wird angezeigt. Folgendes Feld können Sie bearbeiten:

- *Admin.-Protokoll-Sprache*: Wählen Sie die gewünschte Sprache aus. Zur Auswahl stehen Englisch und Deutsch.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.4.3.2 Admin.-Protokoll-Daten laden

Sie können das Admin.-Protokoll vom Gateway herunterladen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Admin.-Protokoll* **>** Traces und Ereignisse (Events) **>** *Laden Admin.-Protokoll-Daten*

Laden über HTTP

Sie können die Administrations-Protokolldatei vom HG 3500/3575 zu dem Rechner übertragen, über den Sie das Gateway administrieren.

Nachdem die Datei übertragen wurde, wird sie direkt im System-Editor angezeigt.

7.5 SNMP

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) ist in Verbindung mit Netzwerkmanagementsystemen (NMS) zu verwenden. NMS benutzen SNMP, um die Verwaltung von Netzwerkelementen verschiedener Hersteller zu integrieren.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP*

Die Baumstruktur für *SNMP* wird angezeigt.

Einträge in der Baumstruktur *SNMP*:

Communities

Bei Problemen im Gateway werden Traps erzeugt, um den Administrator über Fehler und Ausfälle zu informieren. Zugriffsberechtigungen auf SNMP-Daten werden durch Communities geregelt. Hinter einer Community verbirgt sich jeweils eine IP-Adresse.

7.5.1 SNMP-Management

SNMP (Simple Network Management Protocol) ist dazu gedacht, in Verbindung mit Netzwerkmanagementsystemen (NMS) verwendet zu werden. NMS benutzen SNMP, um die Verwaltung von Netzwerkelementen verschiedener Hersteller zu integrieren.

Das Gateway enthält einen SNMP-Agenten, der auf eine Standard-MIB-2 sowie eine für das Gateway spezifische private MIB zugreift. Über SNMP können autorisierte Administratoren Administrations- und Konfigurationsdaten auslesen. Einige Einstellungen im Gateway können über SNMP geändert werden.

Wenn eine Standardbetriebsumgebung (wie HP OpenView) verwendet wird, stehen dem Administrator beide MIBs zur Verfügung.

Das Gateway kann den SNMP-Zugriff auf bestimmte IP-Adressen beschränken, so dass die Daten nur von einem autorisierten Administrator über das NMS ausgelesen bzw. geändert werden können.

Lesende Zugriffe

- MIB II (Management Interface Base); RFC 1213
- HiPathCommonMonitoringMIB (nur commonNotificationGroup)

Schreibende Zugriffe

- MIB II (System group, TrapDestTable)
- HiPathCommonMonitoringMIB (IPConnControlTable)

SNMP-Traps

SNMP kann zur Erzeugung von Traps eingesetzt werden. Ein Trap übermittelt Änderungen festgelegter Gegebenheiten oder den Status des Gateways in Echtzeit. Wenn ein Trap erzeugt wird, sendet das Gateway eine Trap-PDU (Protocol Data Unit) an den SNMP-Agenten, der sie dann an das NMS weiter-

leitet. Ab Version V7 R2 bietet OpenScape 4000 Assistant die Möglichkeit, den Lese- und Schreibzugriff sowie die Trap-Ziele zentral vom Assistant aus zu konfigurieren.

Hierbei überschreibt der Assistant alle lokal konfigurierten Eintrage im Gateway.

Im WBM können Sie feststellen, ob ein Eintrag vom Assistant oder vom WMB erstellt wurde.

7.5.2 Communities

Communities sind IP-Adressen mit bestimmten SNMP-Berechtigungen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities*

Klicken Sie auf das Pluszeichen (+) neben *Communities*, um ein Menü mit den folgenden Einträgen anzuzeigen:

1) *Lesende Communities Schreibende Communities Trap-Communities*

Dies sind die möglichen Community-Typen bzw. Zugriffsberechtigungsklassen.

7.5.2.1 Lesende Communities

Sie können sich eine Liste aller SNMP-Communities anzeigen lassen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Lesende Communities*

Der Dialog *Liste aller Communities* wird angezeigt. Für jede Community wird die IP-Adresse angezeigt, der Community-Name sowie der Berechtigungstyp (lesende Community, schreibende Community oder Trap-Community).

Lesende Communities haben folgende Zugriffsberechtigungen:

- MIB II (Management Interface Base); RFC 1213,
- HG1500MIB (HLB2-Konfiguration und -Statistiken),
- RG2500MIB (MIB für einige Routingfunktionen),
- HiPathCommonMonitoringMIB (nur commonNotificationGroup).

Klicken Sie auf das Pluszeichen (+) neben *Lesende Communities*, um die folgenden Einträge anzuzeigen:

1) *Lesende Community hinzufügen*

7.5.2.2 Lesende Community hinzufügen

Sie können eine neue IP-Adresse zu den lesenden Communities hinzufügen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Lesende Communities* **>** *Lesende Community hinzufügen*

Der Dialog *Lesende Community hinzufügen* wird angezeigt. Folgende Felder können bearbeitet werden:

- *IP-Adresse*: Geben Sie in dieses Feld die IP-Adresse des neuen Trap-Empfängers ein.
- *Community*: Dieses Feld legt die SNMP-Berechtigungen fest. Geben Sie die Community als Zeichenkette ein.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.5.2.3 Schreibende Communities

Schreibende Communities haben folgende Zugriffsberechtigungen:

- MIB II (System group, TrapDestTable),
- HG1500MIB (Control group),
- HiPathCommonMonitoringMIB (IPConnControlTable).

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Schreibende Communities*

Klicken Sie auf das Pluszeichen (+) neben *Schreibende Communities*, um die folgenden Einträge anzuzeigen:

1) *Schreibende Community hinzufügen*

Klicken Sie auf *Schreibende Communities*, um alle IP-Adressen (Communities) anzuzeigen, die zu diesem Community-Typ gehören.

7.5.2.4 Schreibende Community hinzufügen

Sie können eine neue IP-Adresse zu den schreibenden Communities hinzufügen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Schreibende Communities* **>** *Schreibende Community hinzufügen*

Der Dialog *Schreibende Community hinzufügen* wird angezeigt. Folgende Felder können bearbeitet werden:

- *IP-Adresse*: Geben Sie in dieses Feld die IP-Adresse des neuen Trap-Empfängers ein.
- *Community*: Dieses Feld legt die SNMP-Berechtigungen fest. Geben Sie die Community als Zeichenkette ein.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.5.2.5 Trap-Communities

Trap-Communities haben Trap-Berechtigung.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Trap-Communities*

Klicken Sie auf das Pluszeichen (+) neben *Trap-Communities*, um ein Menü mit den folgenden Einträgen anzuzeigen:

1) *Trap-Community hinzufügen*

Klicken Sie auf *Trap-Communities*, um alle IP-Adressen (Communities) anzuzeigen, die zu diesem Community-Typ gehören.

7.5.2.6 Trap-Community hinzufügen

Sie können eine neue IP-Adresse zu den Trap-Communities hinzufügen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Communities* **>** *Trap-Communities* **>** *Trap-Community hinzufügen*

Der Dialog *Trap-Communitiy hinzufügen* wird angezeigt. Folgende Felder können bearbeitet werden:

- *IP-Adresse*: Geben Sie in dieses Feld die IP-Adresse des neuen Trap-Empfängers ein.
- *Community*: Dieses Feld legt die SNMP-Zugriffsrechte fest. Geben Sie die Community als Zeichenkette ein.

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*.

7.5.3 Traps

Bei Problemen im Gateway werden Traps erzeugt, um den Administrator über Fehler und Ausfälle zu informieren. Es gibt folgende Arten von Traps:

- System-Traps (Systemfehler, die sofortige Maßnahmen zur Behebung erfordern)
- Leistungs-Traps (Informationen zu Leistungsproblemen, die jedoch keine Behebung erfordern)

Weitere Details zu Traps siehe Section 9.7.1, "Traps".

Traps sind nach ihrer Auswirkung klassifiziert und entsprechend in der Baumdarstellung farblich markiert:

Table 5: Auswirkungsklassen von Traps

Auswirkungsklasse	Farbe des Listenpunkts
Critical	Rot
groß	Rot
klein	orange
Warning	Gelb
gelöscht	Grün
informativ	grau

Auswirkungsklasse	Farbe des Listenpunkts
Zwischenzustand	grau
sonstige Traps	grau

Die Sortierung der Traps in der Baumdarstellung erfolgt in der Reihenfolge ihres Auftretens im System.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Traps*

Klicken Sie auf *Traps*, um ein Menü mit folgenden Einträgen anzuzeigen:

1) *Alle Traps anzeigen Alle kritischen Traps anzeigen Aktualisieren*

Traps (Ordner):

Wenn Traps vorhanden sind, wird der Eintrag *Traps* in der Baumstruktur als Ordnersymbol dargestellt. Durch Doppelklicken auf *Traps* wird die Baumstruktur um die vorhandenen Traps erweitert. Dabei ist folgende Funktion möglich:

1) *Trap anzeigen*

7.5.3.1 Alle Traps anzeigen

Sie können sich eine Liste mit Detaildaten aller aktuell im System vorhandenen Traps anzeigen lassen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Traps* **>** *Alle Traps anzeigen*

Der Dialog *Liste aller Traps* wird angezeigt. Die Tabelle ist nach der Reihenfolge des Auftretens der Traps im System sortiert. Die Anzeige wird automatisch alle 30 Sekunden aktualisiert. Durch Anklicken von *Aktualisieren* können Sie die Aktualisierung jedoch jederzeit erzwingen.

7.5.3.2 Alle kritischen Traps anzeigen

Sie können sich eine Liste mit Detaildaten systemkritischer Traps anzeigen lassen (solche mit rotem Listenpunkt).

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Traps* **>** *Alle kritischen Traps anzeigen*

Der Dialog *Liste aller kritischen Traps* wird angezeigt. Die Tabelle ist nach der Reihenfolge des Auftretens der Traps im System sortiert. Die Anzeige wird automatisch alle 30 Sekunden aktualisiert. Durch Anklicken von *Aktualisieren* können Sie die Aktualisierung jedoch jederzeit erzwingen.

7.5.3.3 Aktualisieren

Sie können die Baumdarstellung der Traps jederzeit aktualisieren.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Traps* **>** *Aktualisieren*

Die Baumdarstellung wird aktualisiert.

7.5.3.4 Trap anzeigen

Sie können Detaildaten zu einem einzelnen Trap ansehen.

WBM-Pfad:

WBM **>** *Wartung* **>** *SNMP* **>** *Traps* **>** gewünschter Trap **>** *Trap anzeigen*

Folgende Trap-Informationen werden angezeigt: Die ersten vier angezeigten Einträge haben folgende Bedeutung:

- Wertigkeit des Traps (z. B. Information)
- Name des Traps
- Erläuterungen zu diesem Trap
- Typ des Traps (1 = Software, 2 = Hardware)

7.6 Plattform-Diagnose (nicht bei HG 3575)

WBM-Pfad:

WBM **>** *Wartung* **>** *Plattform-Diagnose*

Die Funktionen in diesem Bereich dürfen nur von Entwicklern benutzt werden.

7.7 Applikat.- Diagnose (nicht bei HG 3575)

WBM-Pfad:

WBM **>** *Wartung* **>** *Applikat.- Diagnose*

Die Funktionen in diesem Bereich dürfen nur von Entwicklern benutzt werden.

8 Technische Konzepte

Einige administrierbare Funktionen des Gateways erfordern ein tieferes Verständnis technischer Details. In diesem Kapitel finden Sie Abschnitte, in denen solche technische Details behandelt werden.

8.1 Umgebungsanforderungen für VoIP

Relevante WBM-Funktionen:

Siehe Section 7.4.1.1, "LAN1 (LAN1)" Siehe Section 7.4.1.2, "*LAN2 (Redundantes LAN1) [nur für HG 3500]*" Siehe Section 7.6.4, "Media Stream Control (MSC)" Siehe Section 7.6.5, "HW-Module" Siehe Section 7.2.2, "MSC-Statistiken"

Um die Qualität der Sprachübertragung sicherzustellen, müssen die verwendeten Netzwerke bestimmte Anforderungen erfüllen, die insbesondere für die Vermeidung inakzeptabler Verzögerungen wichtig sind.

8.1.1 Umgebungsanforderungen im LAN

Für LANs, die für VoIP genutzt werden, gelten folgende Anforderungen:

- Mindestens 256 Kbit/s Übertragungskapazität pro Gerät im Netzwerk
- Höchstens 50 ms Verzögerung in einer Richtung (One Way Delay); höchstens 150 ms Gesamtverzögerung
- Höchstens 1% Paketverlust
- Unterstützung für QoS – IEEE 802.1p, DiffServ (RFC 2474) oder TOS (RFC 791)
- Jedes HG 3500/3575 muss über einen Switch oder einen dedizierten Port eines Routers angeschlossen sein.
- Wir empfehlen, die VoIP-Anwendung über ein getrenntes VLAN anzuschließen, um Kollisionen mit anderen Übertragungen zu minimieren. Wenn alle beteiligten Geräte VLAN (nach IEEE 802.1q) unterstützen, kann der gesamte VoIP-Verkehr in ein separates VLAN ausgelagert werden. Die LAN-Switches müssen für den Administrationszugriff in diesem Fall einzelnen PC ermöglichen, auf mehrere VLAN-Segmente zuzugreifen.
- Nicht mehr als 20% der verfügbaren Bandbreite sollte genutzt werden.
- Höchstens 10% des gesamten Datenverkehrs sollten Broadcast-Pakete sein.
- Die Fehlerrate sollte höchstens 1% des Datenverkehrs ausmachen und aktuell nicht zunehmen.

8.1.2 Umgebungsanforderungen im WAN

Wenn VoIP in LANs, die über WANs gekoppelt sind, LAN-übergreifend eingesetzt wird, gelten folgende Mindestanforderungen:

- Die LANs müssen jeweils über einen DSL-Anschluss mit fester IP-Adresse mit dem Internet verbunden sein.
- Unterstützung für QoS – IEEE 802.1p, DiffServ (RFC 2474) oder TOS (RFC 791) – über die gesamte Verbindung

- Die für die Gespräche benötigte Bandbreite muss jederzeit sowohl in Netz- als auch in Nutzerrichtung zur Verfügung stehen.
- Höchstens 50 ms Verzögerung in einer Richtung (One Way Delay); höchstens 150 ms Gesamtverzögerung
- Höchstens 3% Paketverlust
- Höchstens 3% Fehlerrate
- Höchstens 10% Jitter
- Möglichst wenig Broadcast- und Multicast-Verkehr im Netz. Dies kann ggf. durch Strukturierung des Netzes – etwa per VPN – mithilfe geeignete Layer-3-Switches und -Router geschehen oder durch den Einsatz von Layer-2-Switches, die Multicasting erkennen.
- Höchstens 40% Netzwerkauslastung (ohne VoIP-Verkehr)
- Möglichst unter 40 Broadcast-Pakete pro Sekunde

8.2 Bandbreitenbedarf in LAN/WAN-Umgebungen

Relevante WBM-Funktionen:

Siehe Section 7.4.1.1, "LAN1 (LAN1)" Siehe Section 7.4.1.2, "*LAN2 (Redundantes LAN1) [nur für HG 3500]*" Siehe Section 7.5.3, "Codec-Parameter"

Das HG 3500/3575 ist auf Optimierung der Bandbreitennutzung ausgelegt. Es implementiert dazu unter anderem folgende Funktionen:

- Stille-Unterdrückung
- Entdeckung und Unterdrückung von Hintergrundgeräuschen
- dynamische Feststellung von Sprache und Fax

Verfügbare Bandbreite

Die für Sprache benötigte Bandbreite muss im Netzwerk jederzeit verfügbar sein. Dazu sind vor der Installation der Komponenten Netzwerk-Mess- und -Analyseverfahren erforderlich.

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer LAN-Umgebung:

Die erforderliche Bandbreite für Sprachübertragung in einem IP-Netzwerk lässt sich mit Hilfe der folgenden Tabelle berechnen:

Table 6: Bandbreitenbedarf nach Codec

Codec-Typ	Paketierungs-Parameter	Paketabstand/ Rahmengröße (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl.) header (kBit/s)
G.711	20	20	160	230	44 %	92
G.711	30	30	240	310	29 %	82,7
G.711	40	40	320	390	22 %	78
G.711	60	60	480	550	15 %	73,3

Codec-Typ	Paketierungs-Parameter	Paketabstand/ Rahmengröße (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl.) header (kBit/s)
G.723.1,	1	30	24	94	292 %	25,1
G.723.1,	2	60	48	118	146 %	15,7
G.729A	1	20	20	90	350 %	36
G.729A	2	40	40	110	175 %	22
G.729A	3	60	60	130	117 %	17,3
RTCP		5.000		280		0,4

Der Load im LAN ist für eine Richtung kalkuliert. Für Payload-Verbindungen in beide Richtungen ist die doppelte Bandbreite erforderlich. Mit HG 3500/3575 wird VAD mit Codec G.7231A und G.729AB unterstützt. Werden diese Codes verwendet, nimmt die Bandbreitenanforderung abhängig vom Umfang der Ruheperioden in Sprachsignalen ab.

Die Berechnung schließt VLAN-Tagging entsprechend IEEE 802 1q ein. Ohne VLAN-Tagging ist die Länge eines Pakets um 4 Bytes kürzer.

Der Overhead berechnet sich wie folgt:

Table 7: Overhead-Berechnung

Protokoll	Bytes
RTP-Header	12
UDP-Header	8.
IP-Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Gesamt	**70**

Table 8: Kontrolle Payload-Verbindung mit parallelem RTCP (Real-time Transport Control Protocol)

Report-Typ	Report Intervall (s)	Durchschnittl. Ethernet-Paketgröße (Bytes)	EthernetLoad (inkl.) Kopf (kBit/s)
Sender-Report	5	140	0,2
Empfänger-Report	5	140	0,2
Gesamt			0,4

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer WAN-Umgebung:

Für Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer WAN-Umgebung errechnen sich folgende Werte:

Table 9: WAN-Bandbreitenbedarf nach Codec

Codec	Paketierungs-Parameter	Paketabstand Rahmen (ms)	Payload (Bytes)	Paketlänge (Bytes)	Payload-Paket (Overhead in %)	WAN Load (kBit/s)	Paketlänge mit Header-Kompre (Bytes)	WAN Load mit Header-Kompression (kBit/s)
G.711	20	20	160	206	29 %	82,4		
G.711	30	30	240	286	19 %	76,3		
G.711	40	40	320	366	14 %	73,2		
G.711	60	60	480	526	10 %	70,1		
G.723.1,	1	30	24	70	192 %	18,7	32	8,5
G.723.1,	2	60	48	94	96 %	12,5	56	7,5
G.729A	1	20	20	66	230 %	26,4	28	11,2
G.729A	2	40	40	86	115 %	17,2	48	9,6
G.729A	3	60	60	106	77 %	14,1	68	9,1
RTCP		5.000		230		0,4		0,4

Der WAN-Load ist für eine Richtung kalkuliert. Da WAN-Kanäle gewöhnlich Kanäle in beide Richtungen beinhalten, ist dies gleichbedeutend mit der erforderlichen Bandbreite für z.B. einen ISDN-Kanal.

Der Overhead berechnet sich wie folgt:

Table 10: Overhead-Berechnung

Protokoll	Bytes
RTP-Header	12
UDP-Header	8.
IP-Header	20
PPP	9
Gesamt	**46**
Komprimierte Header	8.

Für RTP/UDP/IP-Header-Kompression wird gewöhnlich ein 'komprimierter Header' verwendet. Zusätzlich wird alle 5 Sekunden ein voller Header (46 Bytes) gesendet.

Die Daumenregel zum Berechnen der erforderlichen Bandbreite für n parallele VoIP-Verbindungen mit G.711 (ein Frame pro RTP-Paket) lautet:

BandbreiteLAN = n Ã— (180Voice-Payload + 0,4RTPC)

BandbreiteWAN = n Ã— (82Voice-Payload + 0,4RTPC)

Bei anderen Codecs oder Paketwerten wechseln die Annäherungswerte für Sprach-Payload. Ferner muss die Bandbreite für Attendant P, Gebühreninformationen und andere Anwendungen berücksichtigt werden.

Bandbreitenanforderungen für CAR-Alive / Node Survey

Für CAR-Alive / Node Survey (PBX-Knotenüberwachung) gibt es zwei verschiedene Methoden: entweder ein TCP-basierter Mechanismus, oder ein ICMP-Ping (konfigurierbar über Manage I oder WBM).

Table 11: LAN-Bandbreitenbedarf für CAR-Alive / Node Survey

Knoten Nummer	TCP Load (kBit/s)	Ping Load (kBit/s)	Zeit- intervall
1	0,1	0,1	12
2	0,2	0,3	
3	0,5	0,8	
4	1,0	1,7	
5	1,7	2,8	
6	2,5	4,2	

Table 12: WAN-Bandbreitenbedarf für CAR-Alive / Node Survey

Knoten Nummer	TCP Load (kBit/s)	Ping Load (kBit/s)
1	0,07	0,11
2	0,14	0,22
3	0,41	0,66
4	0,82	1,31
5	1,37	2,19
6	2,06	3,28

Die Daumenregel zum Berechnen der erforderlichen Bandbreite für CAR-Alive zwischen n Knoten lautet:

BandbreiteLAN = n Ã— (n-1) Ã— BytesAliveMsg Ã— 8 Ã· 1000 Ã· TTimeout between ping

Und zum Berechnen der erforderlichen Bandbreite für CAR-Alive zwischen n Knoten an der HG 3500/3575-Schnittstelle:

BandbreiteLAN = (n-1) Ã— (n-1) Ã— BytesAliveMsg Ã— 8 Ã· 1000 Ã· TTimeout between ping

Der Wert für **bytesAliveMsg** beträgt:

im LAN **212** mit PING, oder **127** mit TCP im WAN **188** mit PING, oder **102** mit TCP

Der Default-Timeout zwischen zwei Pings beträgt 12 Sekunden.

Die folgende Tabelle enthält Angaben zur zusätzlich benötigten Bandbreite für Signale:

Table 13: Bandbreitenbedarf für Signale

Gerät/Anwendung	BHCA	Load (kBit/s)
DSS-Server, aus- und eingehende Anrufe	1400	2
Attendant P (beschäftigt)	1400	3
Gebühreninformationen	1400	1
ACD-Informationen	1400	10
Fax über VCAPI, 14400 Baud		2
KDS-Synchronisations-System mit DBFS (TFTP, Burst)		162

8.3 Quality of Service (QoS)

Relevante WBM-Funktionen:

Siehe Section 7.4.1.1, "LAN1 (LAN1)" Siehe Section 7.4.1.2, "*LAN2 (Redundantes LAN1) [nur für HG 3500]*" Siehe Section 7.4.4.4, "PSTN-Partner" Siehe Section 7.1.4, "Quality of Service" Siehe Section 7.6.3, "QoS Data Collection"

Quality of Service umfasst verschiedene Methoden, in paketorientierten Netzen (IP) gewisse Eigenschaften der Übertragung sicherzustellen.

So ist es zum Beispiel für Voice over IP wichtig, eine Mindestbandbreite für die Dauer der Übertragung sicherzustellen. Wenn mehrere Applikationen gleichberechtigt über IP arbeiten, so wird die vorhandene Bandbreite einer Übertragungsstrecke (z. B. ein ISDN-B-Kanal, 64kBit/s) aufgeteilt, so dass unter Umständen eine Sprachverbindung von Paketverlusten betroffen ist, woraus eine schlechte Sprachqualität resultieren kann.

Das HG 3500/3575 verwendet verschiedene Verfahren zur Realisierung von Quality of Service.

Auf der Schicht 2 (nach OSI, Ethernet) kann eine Erweiterung (IEEE 802.1p) gegenüber dem Standard-Ethernet-Format (DIX V2) aktiviert werden, die den Ethernet-Header um einige Informationen erweitert, unter anderem um ein drei Bit breites Datenfeld. Mit diesem Feld wird dem Datenpaket eine

Priorisierungsinformation mitgegeben. Für alle Pakete, die die Baugruppe aus dem LAN erreichen, werden beide Ethernet-Formate (IEEE 802.1p und DIX V2) verstanden, für alle Pakete, die von der Baugruppe ins LAN verschickt werden, kann das Format ausgewählt werden. Bevor dieser Parameter aktiviert wird, sollte geprüft werden, ob alle Komponenten im Netzwerk dieses Format unterstützen. Andernfalls ist unter Umständen vom LAN aus kein Zugang auf das HG 3500/3575 mehr möglich.

Beim Übergang auf ein anderes Transportmedium (z. B. ISDN) wird der Ethernet-Header nicht weitertransportiert. Ein IP-Router (wie der des HG 3500/3575) kann allerdings die Informationen zur Priorisierung nutzen, die im IP-Header enthalten sind. Die Priorisierung auf IP-Ebene können aber auch reine IP-Router nutzen, die zum Beispiel zwei Netzsegmente miteinander verbinden. Als QoS-Verfahren werden entweder drei Bit (IP-Präzedenz nach RFC 791, älterer Standard) oder sechs Bit (Differentiated Services oder DiffServ, nach RFC 2474) zur Bildung von unterschiedlichen Klassen ausgewertet. Der IP-Router des HG 3500/3575 stellt diesen Klassen unterschiedliche Bandbreiten zur Verfügung, so dass etwa Sprachpakete vorrangig behandelt werden können.

Für das DiffServ-Verfahren werden verschiedene sogenannte Codepunkte ('Grundeinstellungen > AF/EF-Codepunkte') definiert und anhand dieser Codepunkte zwei verschiedene Verfahren für die Behandlung der Payload verschieden markierter Datenströme genutzt:

Das Verfahren 'Expedited Forwarded' (EF) – nach RFC 2598 – garantiert eine konstante Bandbreite für die Daten dieser Klasse. Wird der definierte Wert erreicht, werden alle Pakete, die diese Bandbreite überschreiten würden, verworfen. Auf dem HG 3500/3575 ist für EF eine eigene Klasse definiert. Für diese Klasse kann die Bandbreite für jeden ISDN-Partner in Prozent definiert werden (QoS-Bandbreite für EF).

Das Verfahren 'Assured Forwarding' (AF) – nach RFC 2597 – garantiert eine minimale Bandbreite für die Daten einer (von mehreren) Klassen. Die Klassen niedrigerer Priorität teilen sich jeweils die von EF bzw. den höher priorisierten Klassen nicht genutzte Bandbreite. Innerhalb jeder Klasse kann über den Dropping Level zusätzlich definiert werden, wie schnell Pakete verworfen werden sollen, wenn sie nicht schnell genug weitertransportiert werden können. So ist es bei Sprachpaketen nicht sinnvoll, sie lange zwischenzuspeichern (dadurch erhöht sich nur das Delay, die Verzögerung). Bei einer gesicherten Datenübertragung (z. B. einem Dateitransfer) ist es hingegen vorteilhaft, einen größeren Zwischenspeicher zu haben, da es andernfalls ohnehin zu Paketwiederholungen zwischen den beiden Endstellen kommen würde.

Auf dem HG 3500/3575 sind vier Klassen für AF reserviert: AF1x (hohe Priorität), AF2x, AF3x und AF4x (niedrige Priorität), wobei 'x' für einen von drei Dropping-Stufen steht: niedrig (1), mittel (2) und hoch (3). Bei 'niedrig' werden Pakete lange zwischengespeichert, bei 'hoch' werden Pakete früh verworfen, wenn sie nicht weitertransportiert werden können. Unmarkierte IP-Pakete (TOS-Feld=00) werden mit niedrigster Priorität behandelt.

Wenn ein Routing-Partner nur mit einem der beiden Standards (DiffServ oder IP-Präzedenz) arbeiten kann (z. B. ein älterer Router, der nur mit IP-Präzedenz arbeitet), so kann das HG 3500/3575 das TOS-Feld entsprechend übersetzen. Dies kann bei jedem PSTN-Partner bzw. bei der LAN-Schnittstelle eingestellt werden. Im Default 'identisch' wird nichts übersetzt, mit den beiden Werten 'DiffServ' bzw. 'IP-Präzedenz' findet jeweils eine Übersetzung gemäß der untenstehenden Tabelle statt, wenn das Feld nicht nach dem eingestellten Standard versorgt ist.

Bei IP-Datenverkehr werden die IP-Pakete, die das HG 3500/3575 selbst generiert, in fünf Gruppen aufgeteilt (z. B. der VCAPI-Server, H.323-Gateway). Für vier dieser Gruppen kann eingestellt werden, mit welchem Codepunkt die Pakete markiert werden sollen.

- Voice-Payload für die IP-Telefonie (Voice over IP)
- Call Signaling für den Verbindungsaufbau bei H.323/SIP
- Data Payload zum Beispiel für IP-Vernetzung mit Fax oder Modem
- Network Control zum Beispiel SNMP-Traps

Der übrige Datenverkehr wird mit 'deaktiviert', also 00 markiert.

Die verschiedenen DiffServ-Codepunkte und die Defaulteinstellungen sind in der folgenden Tabelle dargestellt.

Table 14: Codepunkt-Umsetzung

Layer 3 QoS Werte										
DSCP (Differentiated Services Code Point)							Standard	TOS-Byte gesamt		
				Drop-Level						
Name	binär	hex	dez	high	med	low		binär	hex	dez
DE (Standard)	0	0	0				alle übrigen Pakete	0	0	0
AF 11	1.010	0A	10			x		101000	28	40
AF 12	1.100	0C,	12		x			110000	30	48
AF 13	1110	0E,	14	x				111000	38	56
AF 21	10010	12	18			x		1001000	48	72
AF 22	10100	14	20		x			1010000	50	80
AF 23	10110	16	22	x				1011000	58	88
AF 31	11010	1A	26			x	Signali-sierung	1101000	68	104
AF 32	11100	1C	28		x			1110000	70	112
AF 33	11110	1E	30	x				1111000	78	120
AF 41	100010	22	34			x		10001000	88	136
AF 42	100100	24	36		x			10010000	90	144
AF 43	100110	26	38	x				10011000	98	152
EF	101110	2E	46				Sprache/ Fax/ Modem	10111000	B8	184
CS7	111000	38	56		x		Netzwerk-steuerung	11100000	E0	224

Table 15: Codepunkt-Umsetzung

Layer 2 QoS Werte		
binär	hex	Standard
000	0	alle übrigen Pakete
000	0	Netzwerksteuerung
011	3	Signalisierung
110	5	Fax/Modem
110	5	Sprache

Wenn nur Layer 3-Prioritäten vorliegen, wie z.B. bei Routing-Strecken, werden nur für solche Pakete Layer 2-Tags gesetzt, deren Layer 3-TOS-Wert übereinstimmt mit dem TOS-Wert einer der 4 Prioritätsklassen wie sie in Grundeinstellungen -> Quality of Service festgelegt werden.

8.4 Statischer und adaptiver Jitter-Buffer

Der Jitter-Buffer des HG 3500/3575 kann auf die Verbindungsbedingungen des jeweiligen Netzwerks eingestellt werden.

Relevante WBM-Funktionen:

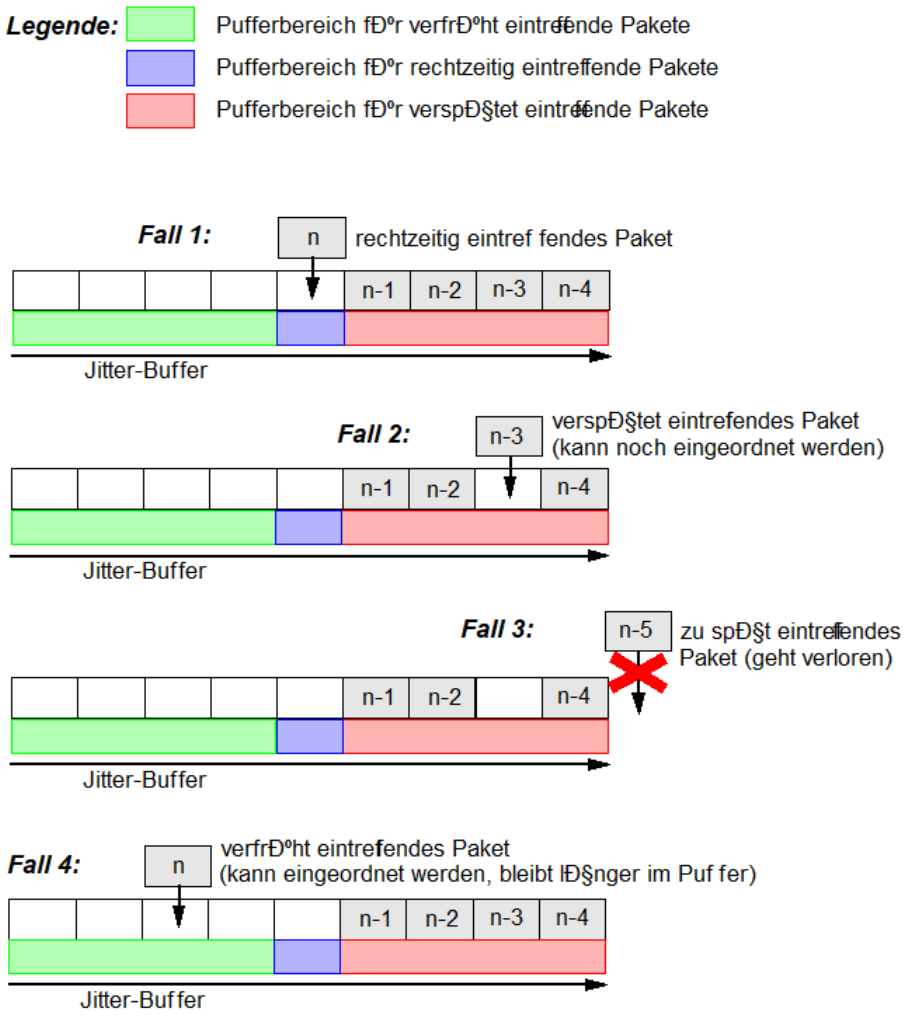
Siehe Section 7.1.4, "Quality of Service" Siehe Section 7.6.5, "HW-Module"

8.4.1 Funktionalität des Jitter-Buffers

In TCP/IP-basierten Netzwerken können Pakete einer Übertragung unterschiedlich schnell eintreffen. Da sich dieser Effekt vor allem bei Sprachsignalübertragungen 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 normal 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; 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.

Die folgende Illustration verdeutlicht die Arbeitsweise 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.

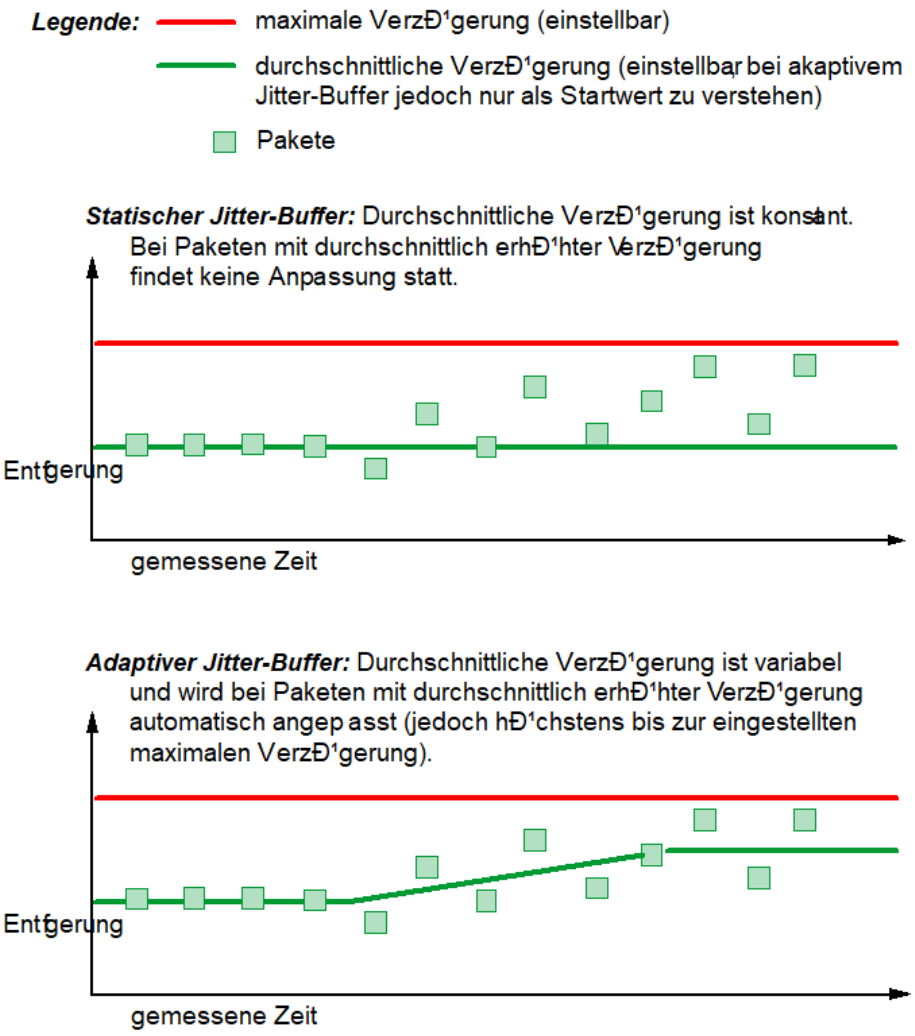
8.4.2 Arbeitsweisen des Jitter-Buffers

Der Jitter-Buffer bietet drei verschiedene Arbeitsweisen an. Davon sind zwei für Sprachübertragung geeignet, und eine für Datenübertragungen (z. B. transparentes Fax, transparentes Modem oder ISDN-Daten):

- **statischer** Jitter-Buffer für Sprache
- **statischer** Jitter-Buffer für Daten
- **adaptiver** (dynamischer) Jitter-Buffer für Sprache

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. Die folgende Illustration verdeutlicht den Unterschied

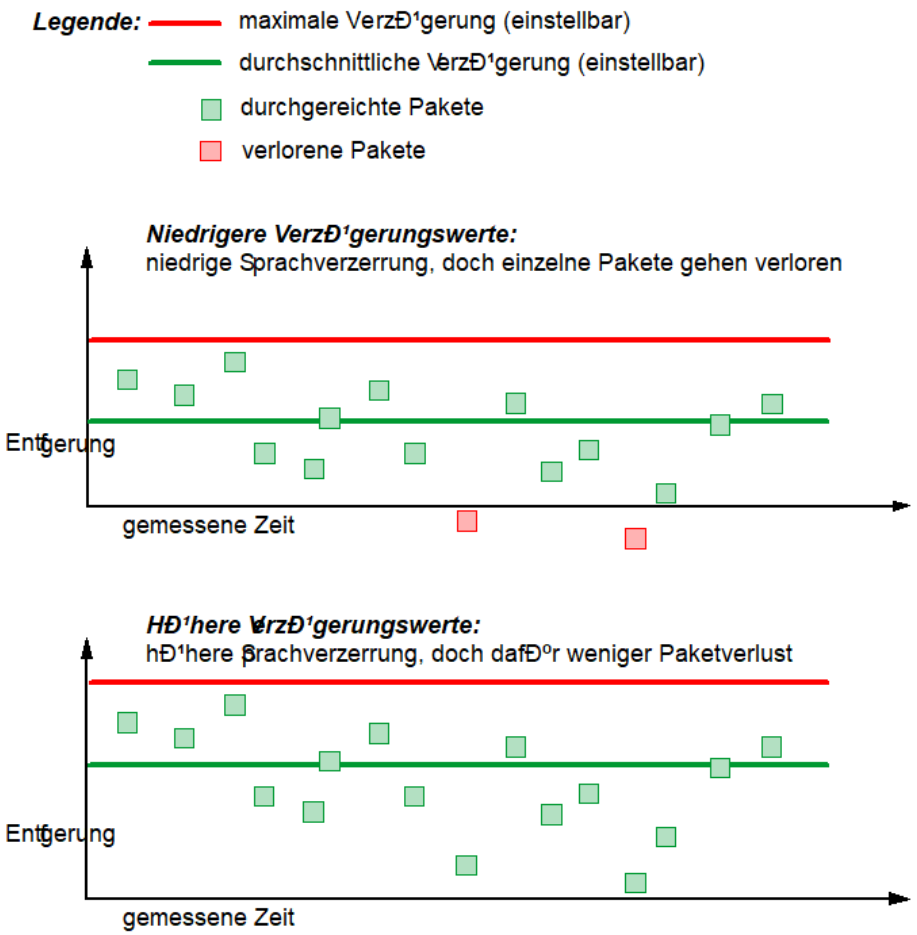
zwischen statischem und adaptivem Jitter-Buffer anhand einer Situation, in der vermehrt Pakete mit erhöhter Verzögerung eintreffen:



Die einstellbare durchschnittliche Verzögerung (grüne Linie) ist beim adaptiven Jitter-Buffer lediglich der Startwert.

8.4.3 Abwägungen beim Einstellen der Verzögerung bei statischem Jitter-Buffer

Je niedriger durchschnittliche und maximale Verzögerung eingestellt werden, desto verzerrungsfreier ist vor allem die Übertragung von Sprache. Dafür steigt die Gefahr des Paketverlusts. Bei höheren Werten für die Verzögerung können weniger Pakete verloren gehen, doch dafür steigt der Verzerrungsfaktor. Die folgende Illustration verdeutlicht diesen Zusammenhang:

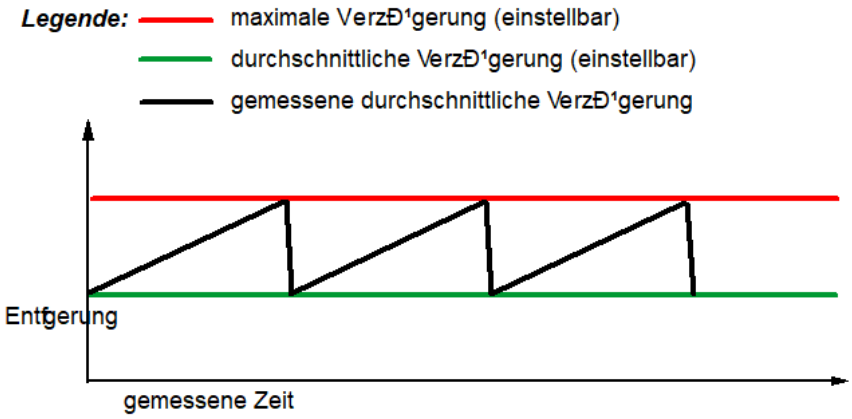


Die HG-Baugruppe ist auf Mittelwerte voreingestellt, die sich in den meisten Umgebungen bewährt haben.

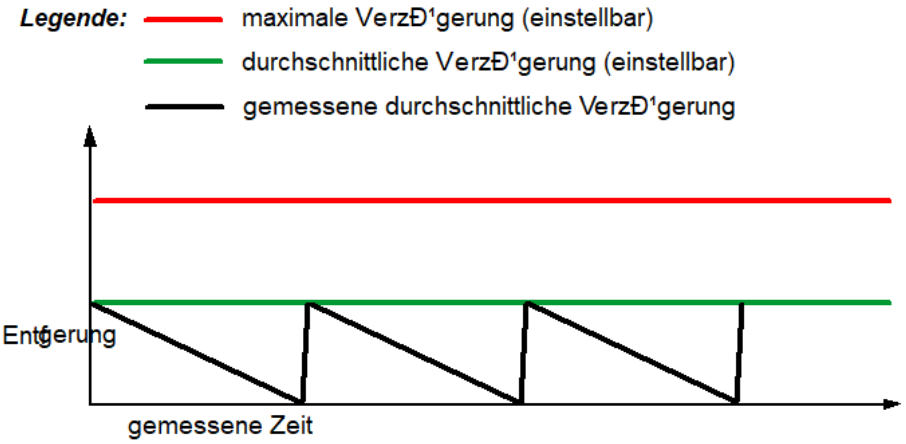
8.4.4 Clock Drift bei statischem Jitter-Buffer

Für die Zeitstempel der Pakete einer IP-basierten Sprachübertragung sorgt gemessene Uhrzeit. Wenn die Zeitmessung auf Sender- und Empfängerseite nicht exakt übereinstimmt, führt dies dazu, dass auf der Sendeseite mehr oder weniger Pakete pro Sekunde erzeugt werden, als auf Empfängerseite erwartet werden. Diese Diskrepanz wird als Clock Drift bezeichnet.

Wenn auf Empfängerseite mehr Pakete erzeugt werden, als im Jitter-Buffer der HG-Baugruppe erwartet werden, 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:

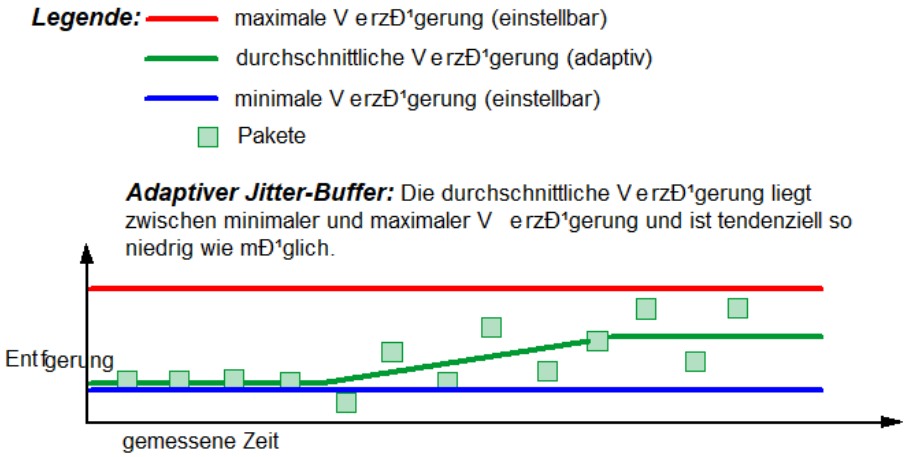


Wenn auf Empfängerseite wenger Pakete erzeugt werden, als im Jitter-Buffer der HG-Baugruppe erwartet werden, gelangen weniger Pakete in den Jitter-Buffer als vorgesehen. Das führt zu einer ständigen Verringerung der gemessenen durchschnittlichen Verzögerung. Wenn dies dazu führt, dass sich gar keine 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. Der gesamte Vorgang beginnt von Neuem. In diesem Fall gehen keine Pakete verloren. Die folgende Abbildung verdeutlicht den Vorgang:



8.4.5 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:



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

8.4.6 Paketverlustkontrolle bei adaptivem Jitter-Buffer

Um zu hohen Paketverlust zu vermeiden, wird die tatsächliche Berechnung der durchschnittlichen Verzögerung beim adaptiven Jitter-Buffer durch zwei Faktoren beeinflusst: 1. durch die laufend gemessene Verzögerung 2. durch die Anzahl verlorener Pakete.

Der Wirkungsgrad des zweiten Faktors ist durch einen 'Präferenz'-Parameter in der HG-Baugruppe 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).

Als Daumenregel gilt: der Wert 0 wird ca. 10ms höhere Durchschnittsverzögerung bewirken als der mittlere Wert 4, und der Wert 8 ca. 10ms geringere Durchschnittsverzögerung als der mittlere Wert 4.

8.5 H.235 Security

H.235 ist ein Ergänzungsprotokoll, welches das H.323-Protokoll (und andere) um Sicherheitsfunktionen zur Authentifizierung, Datenschutz und Datenintegrität erweitert. H.235 unterstützt verschiedene Verschlüsselungsalgorithmen und einstellbare Optionen wie z. B. die Länge von Schlüsseln.

Das HG 3500/3575 unterstützt das H.235-Protokoll. Die Grundeinstellungen dazu gehören jedoch nicht zum Konfigurationsumfang des Gateways, sondern werden im OpenScape 4000 Manager vorgenommen.

8.6 SNMP benutzen

Das HG 3500/3575 bietet SNMP-Unterstützung an.

Relevante WBM-Funktionen:

siehe Section 8.5, "SNMP"

Die Applikation zur Nutzung der SNMP-Funktionalität ist ein MIB-Browser, zum Beispiel als Bestandteil des 'Network Node Managers' von Hewlett-Packard.

8.6.1 SNMP-Traps

Table 16: Generische SNMP-Traps (MIB-2)

Trap
COLD START
WARM START
INTERFACE UP
INTERFACE DOWN
AUTHENTICATION ERROR (falscher SNMP Community-Name)

Folgende HG 3500/3575-spezifische Trap-Klassen gibt es:

- Allgemeine Traps
- Reboot-Traps
- Treshold/Statistik-, Ressourcen/Diagnose-Traps,
- Sicherheits-Traps
- Lizenz-Traps
- Traps für interne Fehler

Die nachfolgenden Tabellen listen für jede dieser Klassen die einzelnen Traps auf. Bei 'Typ' wird zwischen Hardware-Traps (HW) und Software-Traps (SW) unterschieden.

Table 17: Allgemeine Traps (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	MSG_GW_SUCCESSFULLY_-STARTED	Gateway erfolgreich gestartet

Table 18: Reboot Traps (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	*MSG_CAT_H323_REBOOT*	Reboot durch H.323
SW	*MSG_CAT_HSA_REBOOT*	Reboot durch HSA
SW	*MSG_ADMIN_REBOOT*	Reboot durch WBM/CLI-Admin, Software-Upgrade oder Datenwiederherstellung

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	*MSG_SYSTEM_REBOOT*	Automatischer Reboot, z.B. durch Garbage Collection
SW	*MSG_EXCEPTION_REBOOT*	Reboot durch SW-Ausnahme
SW	*MSG_RESTORE_CFG_REBOOT*	Nach Datenwiederherstellung durch HBS erfolgt Neustart
SW	*MSG_GW_OBJ_MEMORY_EXHAUSTED*	Zu viel Speicher reserviert oder nicht mehr genügend Speicher
SW	*MSG_GW_OBJ_ALLOC_FAILED*	Zu viel Speicher reserviert oder nicht mehr genügend Speicher
SW	*MSG_GW_OBJ_MEMORY_INCONSISTENT*	Speicher überschrieben oder bereits freigegebenen Speicher nochmals freigegeben
SW	*ASSERTION_FAILED_EVENT*	Reboot durch erklärte Ausnahme
SW	*EXIT_REBOOT_EVENT*	Reboot durch Ausnahme bei Beenden
SW	*MSG_TLS_POOL_SIZE_EXCEEDED*	Internes Pool-Größen-Konfigurationsproblem.
SW	*MSG_SSM_NUM_OF_CALL_LEGS_2BIG*	Nicht mehr als zwei Call-Legs pro Session möglich
SW	*MSG_SSM_SESSION_CREATION_FAILED*	Keine Session erzeugt, deshalb keine Signalisierung mehr möglich
n/a	*MSG_ASP_REBOOT*	Reboot durch DSP-Treiber
HW	MSG_DSP_REBOOT	Reboot durch DSP-Fehler
HW	*MSG_DELIC_ERROR*	Reboot durch DELIC-Fehler

Table 19: Treshold/Statistik-, Ressourcen/Diagnose-Traps (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message	Erläuterung
HW	MSG_IP_LINK2_FAILURE	IP-Link 1 up/down
HW	MSG_IP_LINK2_FAILURE	IP Link 2 up/down
HW	MSG_OAM_HIGH_TEMPERATURE_EXCEPTION	Temperatur-Limit erreicht (zu heiß)
SW	MSG_GW_OBJ_MEMORY_EXHAUSTED	kein Speicher mehr

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	MSG_GW_OBJ_ALLOC_FAILED	kein Speicher mehr (gemeldet von externem Handler)
SW	MSG_GW_OBJ_MEMORY_INCONSISTENT	Speicher-Inkonsistenz
SW	MSG_TLS_POOL_SIZE_EXCEEDED	keine internen Pools mehr
SW	MSG_OAM_RAM_THRESHOLD_REACHED	RAM-Limit erreicht
SW	MSG_OAM_DMA_RAM_THRESHOLD_REACHED	DMA-RAM-Limit erreicht
SW	MSG_OAM_THRESHOLD_REACHED	Limit erreicht, z.B. bei Flash-Speicher oder IP-Pools
SW	MSG_DVMGR_LAYER2_SERVICE_TRAP	B-Kanal up/down

Table 20: Sicherheits-Traps (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	MSG_HACKER_ON_SNMP_PORT_TRAP	unautorisierter Zugriff auf SNMP-Port

Table 21: Lizenz-Traps (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message	Erläuterung
SW	MSG_LIC_DATA_ACCEPTED	Lizenzdaten akzeptiert
SW	MSG_LIC_DATA_CORRUPTED	Lizenzdaten unvollständig
SW	MSG_LIC_DATA_NOT_ACCEPTED	Lizenzdaten nicht akzeptiert

Table 22: Traps für interne Fehler (HG 3500/3575-spezifisch)

Typ (SW/ HW)	Trap-Message
SW	MSG_WEBSERVER_MAJOR_ERROR
SW	MSG_SSM_NUM_OF_CALL_LEGS_2BIG,
SW	MSG_SSM_SESSION_CREATION_FAILED
SW	MSG_IPNCV_STARTUP_ERROR
SW	MSG_IPNCV_STARTUP_SHUTDOWN

Typ (SW/ HW)	Trap-Message
SW	MSG_IPNCV_INTERNAL_ERROR
SW	MSG_IPNCV_MEMORY_ERROR
SW	MSG_IPNCV_SIGNALING_ERROR

Die Gewichtung der einzelnen Traps kann je nach Schwere des aufgetretenen Ereignisses oder Fehlers variieren und tritt in folgenden Kategorien auf:

- Cleared (Problem bereits gelöst)
- Indeterminate (keine Klassifizierung möglich)
- Critical (kritischer Fehler)
- Major (größerer Fehler)
- Minor (kleinerer Fehler)
- Warning (nur eine Warnung)
- Information (nur zur Information)

Allgemeine Traps wie MSG_GW_SUCCESSFULLY_STARTED werden als 'Information' versendet.

Reboot-Traps sind in jedem Fall Fehler der Ausprägungen 'Critical', 'Major' oder 'Minor'.

Threshold/Ressource-Traps treten wie folgt auf: Beim Eintreten eines Ereignisses wird der Trap mit einer der Kategorien 'Warning', 'Minor' oder 'Major' versendet. Tritt das Trap wiederholt auf, werden Erinnerungen (in zeitlich größeren Abständen) versendet, welche mindestens die Gewichtung des erstmaligen Auftretens besitzen, ggf. auch eine höhere. Konnte das Ereignis korrigiert werden (z. B. 'Link up' oder wieder genügend RAM verfügbar), wird das Trap mit Kategorie 'Cleared' versendet.

8.6.2 SNMP-Funktionen

Die SNMP-Funktionen umfassen:

- mit MIB-Browser und Standard-MIB (nach RFC1213):
- – Abfragen und Verändern von Standardparametern der MIB 2
- mit MIB-Browser und Private-MIB:
- – Abfragen und Verändern von Parametern der Private MIB des HG 3500/3575
- mit OpenScape 4000 Manager:
- – Festlegen von Communities zu Standard-Parametern (Berechtigungsklassen)
  - – Festlegen von Trap-Communities und Stationen, an die Traps gesendet werden
  - – Festlegen der Traplevel für verschiedene Trapgruppen (Empfindlichkeit auf Fehler)
- mit Trap-Empfänger:

- – Empfangen von Traps

  Die MIBs beinhalten für jeden Parameter auch einen Kommentar, der kurz die Bedeutung beschreibt.

  Einige Parameter sind hier beispielhaft aufgeführt:
- mgmt > mib-2 > system > sysUpTime: Zeit seit dem letzten Hochlauf des HG 3500/3575
- HLB2MIB > siemensUnits > pn > hlb2mib > controlGrouphlb20 > sysSoftwareVersion: SW-Release der Baugruppe
- mgmt->mib-2->ip->ipRouteTable: HG 3500/3575Routingtabelle

Das HG 3500/3575 sendet SNMP-Traps (Diagnose und Fehlermeldungen) an die unter 'SNMP > Trap-Communities' eingerichteten Stationen. Diese Meldungen werden in Abhängigkeit von den unter 'SNMP' eingestellten Severity-Stufen verschickt.

Beispiele für von der HG 3500/3575 generierte Traps:

1) Generische Traps, nicht abschaltbar:

2)
- warm start
- cold start
- authentication failure

3) Enterprise Traps, konfigurierbar

4)
- data init (WARNING – erzwungene Neuinitialisierung von Daten)
- memory low (WARNING – Speicherressourcen unterschreiten Schwellwert)
- duplicate mac (MINOR – doppelt vorhandene MAC-Adresse)
- ip firewall (WARNING – IP Firewall Verletzung)
- mac firewall (WARNING – MAC Firewall Verletzung)
- isdn access (WARNING – ISDN Zugangskontrolle)

SNMP-Informationen können auch als E-Mails an eine über WBM konfigurierbare Mailadresse gesendet werden.

8.7 Fehlererkennung durch Traps, Traces und Events

Es gibt folgende Möglichkeiten, Fehler der Baugruppe zu erkennen und zu verfolgen:

- **Traps** zeigen irreguläre Zustände, kritische Fehler oder wichtige Systeminformationen an.
- **Traces** protokollieren die Ausführung einer Softwarekomponente.
- **Ereignisse (Events)** melden Systemprobleme oder Systeminformationen.

Traces und Ereignisse werden in jeweils eigene Ereignisprotokolldateien geschrieben.

Relevante WBM-Funktionen:

Siehe Section 8.5.3, "Traps" Siehe Section 8.4, "Traces und Ereignisse (Events)" Siehe Section 8.4.2, "Ereignisse (Events)"

Referenz der Trace-Komponenten, Trace-Profile und Events:

Siehe Section 10.1, "Traces" Siehe Section 10.2, "Events"

8.7.1 Traps

Bei Problemen in der Baugruppe werden Traps erzeugt, um den Administrator über Fehler zu informieren. Es gibt folgende Arten von Traps:

- System-Traps
- Leistungs-Traps

Die Darstellung der Traps im WBM ist dynamisch. Alle 30 Sekunden wird die Liste der Traps aufgefrischt. Zusätzlich können Sie die Darstellung manuell aktualisieren.

System-Traps

Diese Traps:

- zeigen Systemfehler an und erfordern Gegenmaßnahmen des Administrators,
- oder geben wichtige Systeminformation weiter.

Table 23: System-Traps

Trap	Empfohlene Maßnahme
Baugruppe wurde erfolgreich gestartet	Nur zur Information, keine Maßnahme erforderlich
Neustart ausgelöst von Administrator, Speicherbereinigung, VxWorks, H.323 oder H.323 Stack Adapter (HSA)	Der Neustart wird ausgeführt, keine Maßnahme erforderlich
Speicherprobleme (Speicher voll, Speicherzuweisung schlug fehl, Speicher ist inkonsistent)	Der Neustart wird automatisch durchgeführt, keine Maßnahme erforderlich
Internes Softwareproblem (Überprüfung schlug fehl, 'Exit'-Ereignis, Problem bei der Konfiguration der Poolgröße, Einrichten einer Sitzung schlug fehl)	Der Neustart wird automatisch durchgeführt, keine Maßnahme erforderlich
Kapazität des Flash-Speichers ist erreicht	Entfernen Sie nicht benötigte Dateien aus dem Flash-Speicher (sollte nur von einem Systemspezialisten durchgeführt werden)
Ressourcen des IP-Netzstacks sind ausgeschöpft	Überprüfen Sie die IP-Konfiguration des Gateways und der Router
Fehler der SCN-Verbindung	Nur zur Information, keine Maßnahme erforderlich

Leistungs-Traps

Diese Traps zeigen Leistungsprobleme an.

Table 24: Leistungs-Traps

Trap	Empfohlene Maßnahme
Systemspeicher ist voll	keine
DMA-Speicher ist voll	keine
Temperaturschwellwert auf der Baugruppe wird überschritten	Bei Verwendung eines Lüfterkits: Überprüfen Sie die korrekte Funktion des Lüfters.

8.7.2 Traces

Ein Trace protokolliert eine Ausführung einer Softwarekomponente. Ein Fachmann kann mit Hilfe dieser Ablaufaufzeichnung die Ursache eines Fehlers finden.

Die Trace-Ergebnisse können:

- in einer Protokolldatei gespeichert werden und/oder
- über eine LAN-Verbindung direkt auf einen PC gespeichert werden.

Folgende Trace-Funktionen stehen Ihnen zur Verfügung:

Table 25: Trace-Funktionen

Trace-Funktion	Beschreibung
Trace-Format-Konfiguration	Festlegen, welche Header-Daten im Trace enthalten und wie die Trace-Daten für die Ausgabe aufbereitet werden sollen.
Trace-Ausgabe-Interfaces	Festlegen, über welche Schnittstelle die Trace-Daten ausgegeben werden sollen.
Trace-Protokoll	Lädt die Trace-Ergebnisse als Protokolldatei via HTTP von der Baugruppe auf einen Zielrechner und ermöglicht das Löschen der Trace-Daten von der Baugruppe.
Kunden-Trace-Protokoll	Das Kunden-Trace-Protokoll des HG 3500/3575 kann angezeigt, über HTTP zum Administrations-PC geladen und aus dem Flash-Speicher des Gateways gelöscht werden.
Trace-Profile	Fasst die Überwachung einzelner Komponenten in selbst definierte Profile zusammen. Die Profile können neu erstellt, geändert, gestartet oder gelöscht werden.
Trace-Komponenten	Für jede einzelne Komponente kann die Überwachung ein- oder ausgeschaltet oder gestartet werden. Zusätzlich können für jede Komponente die einzutragenden Daten festgelegt werden.

Die Einstellmöglichkeiten sind im Section 8.4, "Traces und Ereignisse (Events)" beschrieben.

Bei hoher Last kann es dazu kommen, dass die Baugruppe nicht mehr alle Trace-Informationen verarbeiten kann. Beachten Sie dazu die Informationen in Section 8.4.1.4, "Überlastung der Baugruppe durch Trace-Informationen".

8.7.3 Events

Ereignisse (Events) informieren Sie über Mängel des Systems. Sie sollten die Konfiguration des Netzwerks und/oder des Gateways überprüfen, um die abnormale Situation zu bereinigen.

Abhängig von der Einstellung und der Problemklasse können Ereignisse einen SNMP-Trap erzeugen, eine Nachricht an die OpenScape-Anlage senden, eine E-Mail auslösen, eine Trace-Überwachung starten und die Baugruppe neu starten.

Ereignisse werden immer in eine Protokolldatei geschrieben (siehe Section 9.7.4, "Ereignisprotokolldatei").

8.7.4 Ereignisprotokolldatei

Alle Ereignisse werden in eine Protokolldatei beschränkter Größe geschrieben. Wenn die maximale Größe der Datei überschritten wird, überschreiben neue Meldungen die ältesten Einträge.

Der Name der Ereignisprotokolldatei ist:

evtlog.txt

Sie ist in folgendem Verzeichnis im Flash-Speicher des HG 3500/3575 gespeichert:

\tffs\evtlog

Das Ereignisprotokoll kann auf einen PC übertragen werden. Verwenden Sie dazu die Wartungsfunktion 'Laden über HTTP' des WBM.

Die einzelnen Einträge haben folgende Bedeutungen:

Table 26: Bedeutungen von Einträgen in der Ereignisprotokolldatei

Eintrag in der Protokolldatei	Bedeutung
IFTABLE	Name der Komponente, die das Ereignis ausgelöst hat
tH323-CLP	Name der Task, die das Ereignis ausgelöst hat
03/17/2000	Datum des Ereignisses
08:13:56.828020	Zeitpunkt des Ereignisses in hh:mm:ss (Sekunden mit sechs Nachkommastellen)

Eintrag in der Protokolldatei	Bedeutung
ciftable01.cpp 433	Name der Quelldatei und Nummer der Zeile, bei der das Ereignis auftrat
csevWarning	Ereignisklasse
MSG_DVMGR_INTERROR_DEVID	Interner Code des Ereignisses
Geräte-ID (0XFFFFFFFF): CIIfTable:: fCheckConsistency Persistency files and hw_specification inconsistent!	Text in der Ereignisdatei

9 Anhang: Traces und Events

In diesem Referenz-Kapitel finden Sie:

- *Traces*, beschrieben nach einzelnen Trace-Komponenten und Trace-Profilen. Traces sind über das WBM administrierbar (siehe Section 8.4, "Traces und Ereignisse (Events)", speziell Section 8.4.2, "Ereignisse (Events)" und Section 8.4.2, "Ereignisse (Events)").
- *Events*, beschrieben nach einzelnen Event-Codes. Events sind über das WBM administrierbar (siehe Section 8.4.2, "Ereignisse (Events)").

9.1 Traces

NOTICE: Wenn Traces vom Service angefordert werden, dann werden auch die zu tracenden Komponenten und Profile mitgeteilt.

9.1.1 Trace-Komponenten

Die Tabelle dient dem schnelleren Auffinden der Trace-Komponenten. Die Trace-Komponenten sind in derselben Reihenfolge angelegt wie im WBM.

Übersicht der Trace-Komponenten
ADMIN
ASP
ASP_DSP
ASP_DSP_EVENT
ASP_DSP_IFTASK
ASP_DSP_INIT
ASP_DSP_IOCTL
ASP_DSP_STAT
ASP_FAX
ASP_PS
ASP_VMOD
ASP_VMUX
CARDADM
CFG_CODECS
CFG_H235
CFG_H323

Übersicht der Trace-Komponenten
CFG_H323ENDPOINT
CFG_H323GKI
CFG_H323GWI
CFG_H323I
CG
CMGMT
CNQ
CNQIWK
COMMUNITIES
CPMSG
CPUTRACE
CTS
DELIC_DRIVER
DEVMGR
DISPATCH
DLSC
DMC
DSP
DSP_TRACE
DSS1
EMAIL_MANAGER
EMIWK
EVTLOG
EVTLOGTRAP
FAXCONV_IF
FAXCONV_LOGT
FAXCONV_OS
FAXCONV_T30DOWN
FAXCONV_T30INT
FAXCONV_T30UP
FAXCONVERTER

Übersicht der Trace-Komponenten
FMSEM
GATEWAY
GWGLOBAL_DATA
GWGLOBAL_SI_DOWNL_PORTFUNC (nur HG 3500)
GWSI (nur HG 3500)
H323
H323_EPT
H323_GLOBAL_SI_DOWNLOADS
H323_SPE
H323IWK
H323MSG
HFAC (nur HG 3500)
HSA_H225_CS
HSA_H225_RAS
HSA_H245
HSA_H323_NSD
HSA_RV_LOG
HSA_SPE
HSA_SYSTEM
ICC
IFTABLE
IP_ROUTES
IPMONITOR
IPSTACK
IPSTACK_1LAN_IF
IPSTACK_2LAN_IF
IPSTACK_GLOBAL
IPSTACK_IPFILTER
IPSTACK_MACFILTER
IPSTACK_NAT
IPSTACK_ROUTE

Übersicht der Trace-Komponenten
IPSTACK_SNTPS
ISDN_FM
LAN
LICMGMT
LOCSERV
LOCSERV_CFG
LOCSERV_QUERY
LOCSERV_REG
LOG_MSG
LSDCL
LTUC
MANAGER
MAT_STREAM
MCP
MGAF_TBL
MIKEY
MMX (nur HG 3575)
MPH
MSC
MSC_DSP
MSC_QM
MSC_RTCP
MSC_SPECIFIC_STAT
MSC_TMT
MSP_CAPI_IF
MSP_HDLC
MSP_PPP_IF
MSP_RTP_MOD
NWRS
OAM
OAM_ACTIONLIST

Übersicht der Trace-Komponenten
OSF_PCS
PERFM_PL
PERFM_SIG
PLATFORM
PORT
PORT_MGR
PPP_CC
PPP_STACK_DBG_IF
PPP_STACK_PROC
PPPM_TBAS
PPPM_TEXT
PPPM_TSTD
PPTP_DBG_IF
PPTP_PROC
Q931
QDC
QDC_UDPPING
ROUTE98
RTPQM
SACCOB_DRV (nur HG 3500)
SCN
SCNPAY
SDR
SECURE_TRACE
SECURITY_SVC
SENDTMT
SENTA_API
SERVICE_TRACE
SESSION_MGMT
SI
SIP

Übersicht der Trace-Komponenten
SIP_CFG
SIP_CFG_INT
SIP_FM
SIP_GLOBAL_SI_DOWNLOADS
SIP_HT
SIP_REG
SIP_SA
SIP_TRK
SIP_TRK_FM
SIU_STARTUP
SLMO_HFA
SNMP
SPE_SVC
SPL
SS
SSL_UTIL
SSM
STACKTRACE
STATIC_ROUTES
STB (nur HG 3575)
STRC
STREAMS
SWCONF
SYSTEM
T90
TC (nur HG 3500)
TCP_IP_CONF (nur HG 3575)
TCPMOT_WT (nur HG 3575)
TCPSIG (nur HG 3575)
TCPSIG_WT (nur HG 3575)
TCPSUV (nur HG 3575)

Übersicht der Trace-Komponenten
TCPSUV_WT (nur HG 3575)
TESTLW
TIME_SYNC
TIME_SYNCH_TASK (nur HG 3575)
TOOLS
TRAP
TSA (nur HG 3500)
WAN
WEBAPPL
WEBSERVER
WEBSERVER_STATISTIC
WEBSRV_CLIENT_IF
WEBSRV_SYS_IF
X25
X75
XMLUTILS

ADMIN

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Eingehende und ausgehende Admin-Meldungen mit allen Details. Dies beeinflusst die System-Performance.

Trace-Level **9** (DETAIL): Eingehende und ausgehende Admin-Meldungen mit allen Details, ebenso interne Admin-Meldungen wie z. B. Poll-Informationen. Dies beeinflusst die System-Performance stark.

ASP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Informationen zum Verbindungsaufbau und -abbau.

Trace-Level **9** (DETAIL): Detaillierte Informationen zu Verbindungsaufbau und Verbindungsabbau von MSP (mit Ausnahme von DSP-DD)

ASP_DSP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_DSP_EVENT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Informationen zu erkannten Tonwahl- oder Fax-Geräten oder Modems

ASP_DSP_IFTASK

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_DSP_INIT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_DSP_IOCTL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Detaillierte Informationen zu Verbindungsaufbau und Verbindungsabbau (mit allen Parametern).

ASP_DSP_STAT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Informationen zur Datenkanal-Konfiguration nach Verbindungsaufbau (Fax, Modem, V.110).

ASP_FAX

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_PS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_VMOD

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ASP_VMUX

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CARDADM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_CODECS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_H235

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_H323

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_H323ENDPOINT

Konfiguriertes Default-Trace-Level: 0 (STATUS)

CFG_H323GKI

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_H323GWI

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CFG_H323I

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CG

konfiguriertes Default-Trace-Level: n/a

CMGMT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusausgabe (0) Detailinformationen (9) zu CLI-Aktionen. Bitte diese Trace-Komponente nur nach Absprache mit der Entwicklung verwenden!

CNQ

Konfiguriertes Default-Trace-Level: 3

Trace-Level **0**: ISDN-Trace

Trace-Level **1**:ISDN-Trace mit Daten

Trace-Level **2**:Transportcontainer-Trace

Trace-Level **3**:Trace aller Parameter einschließlich Transportcontainer

Trace-Level **4**:TMT-Trace

Trace-Level **5**:TMT-Trace und ISDN-Trace

Trace-Level **6**:TMT-Trace und ISDN-Trace mit Daten

Trace-Level **7**:TMT-TMT-Trace und Transportcontainer

Trace-Level **8**:TMT-TMT-Trace und alle Parameter einschließlich Transportcontainer

Trace-Level **9**:TMT-TMT-Trace und alle Parameter einschließlich Transportcontainer und ASN.1-Trace

CNQIWK

Konfiguriertes Default-Trace-Level: **3**

Trace-Level **0**–9 siehe *CNQ*

COMMUNITIES

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Hinzufügen, Löschen oder Ändern von lesenden, schreibenden oder Trap-Communities für SNMP. Empfang von SNMP-Trap-Zielen über automatisches Auffinden.

CPMSG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CPUTRACE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

CTS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

DELIC_DRIVER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zum DELIC-Treiber (SWC). Nur für Entwickler.

DEVMGR

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Zeigt CP-Schnittstellenfunktionen für Verbindungsaufbau und -fehler an.

DISPATCH

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Listing der Kopfdaten aller über den Dispatcher gesendeten Meldungen. Dies beeinflusst die System-Performance. Die Einstellung ist zu bevorzugen, um einen Überblick über alle über den Dispatcher gesendeten Meldungen zu erhalten.

Trace-Level **6** (INTRA): Dies beeinflusst die System-Performance erheblich. Die Einstellung sollte nur benutzt werden, um Meldungs-Details zu erhalten.

Trace-Level **6/9** (INTRA/DETAIL): Probleme mit der logischen Meldungswarteschlange (siehe Bemerkungen oberhalb). Falsch kodiertes Komponenten-Meldungs-Handling, interne Software-Probleme: - Meldung nicht unregistriert (falscher RecvListType) - Meldung nicht registriert (falscher RecvListType) - Posten der Meldung nicht erfolgreich (falscher RecvListType) - Senden der Meldung nicht erfolgreich (falscher RecvListType) - Unregistriertes Posten der Meldung - Unregistriertes Senden der Meldung

DLSC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

DMC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

DSP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level 3–**9** siehe Vom DSP ausgegebene und vom DSB-Treiber angezeigte Meldungen.

DSP_TRACE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

DSS1

Konfiguriertes Default-Trace-Level: **3**

Trace-Level **0**–9 siehe *CNQ*

EMAIL_MANAGER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Informationen zum Mailversand und zu Verbindungen zum Mailserver.

EMIWK

Konfiguriertes Default-Trace-Level: **0** (STATUS)

EVTLOG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Stellen Sie sicher, dass Ereignisse auch auf der Konsole / im Trace-Log / über LAN-Trace sichtbar sind.

Trace-Level **6** (INTRA): Mutex-Blocking-Situationen.

EVTLOGTRAP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Aktivierung/Deaktivierung eines Trace-Profils für ein registriertes Ereignis.

FAXCONV_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu CAPI-Schnittstellenaktionen des Faxkonverters. Nur für Entwickler.

FAXCONV_LOGT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Kunden-Trace zum Anzeigen fehlerhafter Faxübertragungen.

FAXCONV_OS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu OS-Schnittstellenaktionen des Faxkonverters. Nur für Entwickler.

FAXCONV_T30DOWN

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Downstream-Schnittstellenaktionen des Faxkonverter-T.30-Moduls. Nur für Entwickler.

FAXCONV_T30INT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Aktionen des Faxkonverter-T.30-Moduls. Nur für Entwickler.

FAXCONV_T30UP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Upstream-Schnittstellenaktionen des Faxkonverter-T.30-Moduls. Nur für Entwickler.

FAXCONVERTER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Routinen und Datenfluss-Schnittstellenaktionen des Faxkonverters. Nur für Entwickler.

FMSEM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

GATEWAY

Konfiguriertes Default-Trace-Level: **0** (STATUS)

GWGLOBAL_DATA

Konfiguriertes Default-Trace-Level: **0** (STATUS)

GWGLOBAL_SI_DOWNL_PORTFUNC (nur HG 3500)

Konfiguriertes Default-Trace-Level: **3** (INTER)

Informationen, wenn Port/Kanal-Downloaddaten vom System-Interface ankommen, die Informationen über den Funktionstyp und die Anzahl der B-Kanäle für einen Port/Kanal enthalten.

GWSI (nur HG 3500)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

H323

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Allgemeine Informationen.

Trace-Level **3** (INTER): Empfang von Dispatcher-Meldungen, Admin-Empfänger.

Trace-Level **6** (INTRA): Posten/Senden von Meldungen an andere Komponenten.

Trace-Level **9** (DETAIL): Trace für Funktion/Parameter.

H323_EPT

Konfiguriertes Default-Trace-Level: **9** (DETAIL)

H323_GLOBAL_SI_DOWNLOADS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Trace für Download-Daten.

H323_SPE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): H.323-Protokoll-Manager: SPE 2-Traces

Trace-Level 3 (INTER)

Trace-Level **6** (INTRA)

Trace-Level 9 (DETAIL)

H323IWK

Konfiguriertes Default-Trace-Level: **0** (STATUS)

H323MSG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

H323STACK

Konfiguriertes Default-Trace-Level: 0 (STATUS)

HFAC (nur HG 3500)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Statusinformation über die HFAC-Komponente, Initialisierung der Komponente.

Trace-Level **3** (INTER): Basis-Kommunikation der anderen Komponenten mit der HFAC-Komponente, Informationen über die basic-connected Clients.

Trace-Level **6** (INTRA): Internal method calls und detailliertere Informationen über die Komponente.

Trace-Level **9** (DETAIL): Informationen zum internen Debugger.

HSA_H225_CS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Allgemeine Informationen, H.323-Stack-API-Fehler.

Trace-Level **3** (INTER): Callbacks, die zu einer Meldung an den H.323-Protokoll-Manager führten; Stack-API-Funktionen, die zu einer LAN-Meldung führten.

Trace-Level **6** (INTRA): PVT-Nutzung des H.323-Stacks.

Trace-Level **9** (DETAIL): Trace für Funktion/Parameter.

HSA_H225_RAS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Allgemeine Informationen.

Trace-Level **3** (INTER): Callbacks, die zu einer Meldung an den H.323-Protokoll-Manager führten; Stack-API-Funktionen, die zu einer LAN-Meldung führten.

Trace-Level **6** (INTRA): Nur in besonderen Situationen verwendet.

Trace-Level **9** (DETAIL): Trace für Funktion/Parameter.

HSA_H245

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Allgemeine Informationen.

Trace-Level **3** (INTER): Callbacks, die zu einer Meldung an den H.323-Protokoll-Manager führten; Stack-API-Funktionen, die zu einer LAN-Meldung führten.

Trace-Level **6** (INTRA): Callbacks, die nur Parameterinformationen sammeln.

Trace-Level **9** (DETAIL): Trace für Funktion/Parameter.

HSA_H323_NSD

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Keine Standard-Daten-Traces.

Trace-Level **6** (INTRA):

HSA_RV_LOG

Konfiguriertes Default-Trace-Level: **6** (DETAIL)

Trace-Level **6** (INTRA): Logging von Traces zum RADVision-Stack.

HSA_SPE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): H.323 Stack-Adapter SPE2-Traces

Trace-Level **3** (INTER)

Trace-Level 6 (INTRA)

Trace-Level 9 (DETAIL)

HSA_SYSTEM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS), Trace-Level **3** (INTER), Trace-Level **6** (INTRA), Trace-Level **9** (DETAIL): Konfigurations- und Start-Angelegenheiten sowie Informationen, die nichts mit dem Protokoll zu tun haben.

ICC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IFTABLE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Zeigt Fehler an.

Trace-Level **6** (INTRA): Kennzeichnet Funktionsaufrufe mit wichtigen Parametern.

Trace-Level **9** (DETAIL): Nicht verwendet.

IP_ROUTES

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IPMONITOR

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IPSTACK

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Fehlersituation mit IP-Accounting-Hash-Funktionen. Nur für Entwickler.

IPSTACK_1LAN_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Handhabung der Konfigurationsdaten.

IPSTACK_2LAN_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Handhabung der Konfigurationsdaten.

IPSTACK_GLOBAL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IPSTACK_IPFILTER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IPSTACK_MACFILTER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

IPSTACK_NAT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Initialisierung.

Trace-Level **6** (INTRA): Detaillierte Informationen über NAT-Prozesse.

Trace-Level **9** (DETAIL): Übersetzte Daten.

IPSTACK_ROUTE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Fehlersituation bei den Routingdaten.

IPSTACK_SNTPS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

ISDN_FM

Konfiguriertes Default-Trace-Level: **3**

Trace-Level **3:** ISDN-FM-Trace (Standard)

LAN

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Zeigt diverse normale Operationsvorgänge und -fehler an.

Trace-Level **6** (INTRA): Zeigt Schnittstellenfunktionen mit wichtigen Parametern an.

Trace-Level **9** (DETAIL): Zeigt detaillierte Informationen an.

LICMGMT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): nicht verwendet.

Trace-Level **3** (INTER): Über Admin-Schnittstelle empfangene und gesendete Meldungen.

Trace-Level **6** (INTRA): Funktionsbeendigungen und Ergebnisse.

Trace-Level **9** (DETAIL): Weitere Einzelheiten.

LOCSERV

Konfiguriertes Default-Trace-Level: **0** (STATUS)

LOCSERV_CFG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

LOCSERV_QUERY

Konfiguriertes Default-Trace-Level: **0** (STATUS)

LOCSERV_REG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

LOG_MSG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

LSDCL

konfiguriertes Default-Trace-Level: n/a

LTUC

konfiguriertes Default-Trace-Level: n/a

MANAGER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Probleme beim Löschen, Hinzufügen oder Ändern von Manager-Objekten.

MAT_STREAM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level 3–**9** siehe Interne Meldungen vom Materna-Speicher-Management.

MCP

Konfiguriertes Default-Trace-Level: **0**

Trace-Level **0** (STATUS): Hoch- und Herunterfahren, Empfangene Fehler von anderen Komponenten.

Trace-Level **3** (INTER): Empfangene/gesendete Nachricht oder Funktionseintrag usw.

Trace-Level **6** (INTRA): Funktionsspezifische Informationen.

Trace-Level **9** (DETAIL): Funktionsspezifische Informationen mit Daten.

MGAF_TBL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Schwere Fehler, z. B. fehlende Parameter, ungültige Session-ID usw.

Trace-Level **3** (INTER): Status-Informationen zu Logins, Logouts und Verbindungen.

Trace-Level **6** (INTRA): Detaillierte Socket-Informationen.

MIKEY

Konfiguriertes Default-Trace-Level: **3** (INTER)

MMX (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

MPH

Konfiguriertes Default-Trace-Level: **0** (STATUS)

MSC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): API zu Magic (Funktionsaufrufe mit Parametern).

Trace-Level **3** (INTER): Zusätzlich festgelegt werden die Ein-/Ausgabe-Controls zum MSP.

Trace-Level **6** (INTRA): Verfolgen MSC-interner Funktionen und Handles/File-Descriptoren.

Trace-Level **9** (DETAIL): Einstellungen von Konfigurationsparametern (MSC, MSP/DSP) werden festgelegt. Detaillierte Informationen zu allen MSC-Funktionen.

MSC_DSP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

MSC_QM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Detaillierte Informationen über alle MSC-Funktionen (nur RTCP-Kontext).

Trace-Level **3** (INTER): Informationen zur Qualitätsüberwachung

MSC_RTCP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Allgemeine Informationen über RTCP-Session, Timer usw.

Trace-Level **3** (INTER): Callback-Funktion von MSP für RTCP-Events.

Trace-Level **6** (INTRA): Interne Funktionen, die während einer RTCP-Session aufgerufen wurden.

Trace-Level **9** (DETAIL): Detaillierte Informationen zu allen MSC-Funktionen (jedoch nur im RTCP-Kontext).

MSC_SPECIFIC_STAT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

MSC_TMT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Von Magic aufgerufene MSC-Funktionen werden verfolgt.

Trace-Level **6** (INTRA): Alle Ein-/Ausgabe-Controls (Schnittstelle zu MSP) werden verfolgt.

MSP_CAPI_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level **3–9**: Interne Meldungen vom CAPI-Schnittstellentreiber.

MSP_HDLC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Detaillierte Information über HDLC-Driver Aktionen – nur für Entwickler.

MSP_PPP_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level **3–9**: Interne Meldungen vom PPP-Schnittstellentreiber.

MSP_RTP_MOD

Konfiguriertes Default-Trace-Level: **0** (STATUS)

NWRS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

OAM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Datenfluss von Uploads und Backup-, Export- und Upgrade-Aktionen (erfordert das Ausführen der Admin-Aktion).

Trace-Level **3** (INTER): Datenfluss von Routing-Wizard-Aktionen (nicht relevant für HG 3500/3575).

Trace-Level **4**: Speicherüberlauf-Informationen für alle Aufgaben.

Trace-Level **5**: Speicherbelegungs-Informationen für alle Aufgaben.

Trace-Level **5**: Ausführung des OAM-Schwellenwert-Timers.

Trace-Level **6** (INTRA): Probleme bei OAM-Aufgabenwarteschlange (Schlange voll usw.).

Trace-Level **6** (INTRA): Probleme beim Konfigurieren der SNTP-Zeitsynchronisation (nicht relevant für HG 3500/3575, verschoben zur Komponente TIME_SYNC).

OAM_ACTIONLIST

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Ausführung automatischer Aktionen (Speicherbereinigung, Gatekeeper-Switchback usw.).

OSF_PCS

Konfiguriertes Default-Trace-Level: **3** (INTER)

PERFM_PL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

PERFM_SIG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Performance-Trace für Signalisierungsteil.

PLATFORM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

PORT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

PORT_MGR

Konfiguriertes Default-Trace-Level: **0** (STATUS)

PPP_CC

Konfiguriertes Default-Trace-Level: **3** (INTER)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level **3** (INTER): Externe Schnittstellen der PPP-Verbindungskontrolle zu anderen Komponenten, z. B. PPP-Manager.

Trace-Level **6** (INTRA): Externe und interne Schnittstellen der PPP-Verbindungskontrolle.

Trace-Level **9** (DETAIL): Externe und interne Schnittstellen sowie Details zu Abläufen innerhalb der PPP-Verbindungskontrolle.

PPP_STACK_DBG_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6**-**9**: Weitere detaillierte Informationen über Ruf-Einstellung/Verbindungsabbau

Trace-Level **3** (INTER): PPP-Stack interne Fehlermeldungen.

PPP_STACK_PROC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6**-**9**: PPP-Stack interner Programmfluss.

Trace-Level **3** (INTER): Status eines PPP-Verbindungsaufbaus/-abbaus.

PPPM_TBAS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6**-**9**: PPP-Verhandlungsphase.

Trace-Level **0** (STATUS): PPP-Manager: Grundkonfiguration und Statusmeldungen, anormale Bedingungen.

PPPM_TEXT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3**–**9**: Erweiterte Informationen über interne Vorgänge im PPP-Manager.

PPPM_TSTD

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3**–**9**: Interner Meldungsfluss des PPP-Manager.

PPTP_DBG_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level 3–**9** siehe Interne Fehlermeldungen vom PPTP für Debugging.

PPTP_PROC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Detaillierte Informationen über MSC-spezifische Qualitätsdaten.

Trace-Level 3 (INTER) Informationen zum Aufbau/Abbau von Gesprächen an der PPP-Management-Schnittstelle.

Q931

Konfiguriertes Default-Trace-Level: **3**

Trace-Level **0**–9 siehe *CNQ*

QDC

Konfiguriertes Default-Trace-Level: **0**

Trace-Level **0**: Statusinformationen über den QDC-Client; Traces werden nur einmal angezeigt.

- Informationen zum Hoch-/Runterfahren des QDC-Client
- Informiert darüber, ob die Übermittlung zum QCU/NetMgr gestartet oder abgebrochen wurde

Trace-Level **3**: Ablaufdiagramme und Fehlermeldungen auf oberster Ebene.

Trace-Level **6**: Ablaufdiagramme und Traces werden bei Eingabe einer Funktion oder Klassenmethode angezeigt.

Trace-Level **9**: Detaillierte Informationen zu internen Daten und Schnittstellendaten:

- Pufferinhalt, z.B. QoS-Report vom MSC/zum QCU
- Schnittstellendaten

QDC_UDPPING

Konfiguriertes Default-Trace-Level: **0**

Trace-Level **0**: Status-Informationen über den QDC- UDP-Ping. Die Traces werden nur einmal angezeigt:

1) Informationen zum Hoch-/Runterfahren des QDC UDP ping.

2) • Informiert darüber, ob das UDP Listening Task gestartet oder abgebrochen wurde.

Trace-Level **3**: Ablaufdiagramme und Fehlermeldungen auf oberster Ebene.

Trace-Level **6**: Ablaufdiagramme:

- Traces werden bei Eingabe einer Funktion oder Klassenmethode angezeigt.

Trace-Level **9**: Detaillierte Informationen zu internen Daten und Schnittstellendaten:

- Schnittstellendaten

REMSURV

konfiguriertes Default-Trace-Level: n/a

ROUTE98

Konfiguriertes Default-Trace-Level: **0** (STATUS)

RTPQM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Trace- für die Funktion 'Fallback auf SCN'.

Trace-Level **3** (INTER): Trace- für die Funktion 'Fallback auf SCN'.

Trace-Level **6** (INTRA): Trace- für die Funktion 'Fallback auf SCN'.

Trace-Level **9** (DETAIL): Trace- für die Funktion 'Fallback auf SCN'.

SACCOB_DRV (nur HG 3500)

Konfiguriertes Default-Trace-Level: 0 (STATUS)

SCN

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Zeigt diverse normale Operationsvorgänge und -fehler an.

Trace-Level **6** (INTRA): Zeigt Schnittstellenfunktionen mit wichtigen Parametern an.

Trace-Level **9** (DETAIL): Zeigt detaillierte Informationen an.

SCNPAY

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SDR

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SECURE_TRACE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SECURITY_SVC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0**: Schwerwiegende Fehler, z. B. fehlende Parameter, unbekannte Kommandos.

Trace-Level **3**: Statusinformationen und Handhabung.

Trace-Level **6**: Detaillierte Informationen, Methodenaufrufe.

SENDTMT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Fehler beim Senden oder Posten einer Meldung (Extra-Info für TMT).

Trace-Level **3** (INTER): Empfangen einer Meldung (Extra-Info für TMT).

SENTA_API

Konfiguriertes Default-Trace-Level: **0**

Trace-Level **3** (INTER): Ein Fehler ist aufgetreten.

Trace-Level **6** (INTRA): Funktionen und Ergebnisse sind vorhanden.

Trace-Level **9** (DETAIL): Details:

SERVICE_TRACE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SESSION_MGMT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Informationen über: GetUserInfo, SessionUpdate, SessionIDVerification

Trace-Level **6** (INTRA): Erzeugen oder Verifizieren einer Admin-Session (nur >= 2.1), Update einer Admin-Session, Löschen einer abgelaufenen Admin-Session, Schließen von Admin-Sessions, Schreibberechtigungsschlüssel/ Zugriffs-Handling (get/release).

Trace-Level **9** (DETAIL): Schreibt fortlaufend Admin-Sessiondaten mit/ohne Synchronisierung.

SI

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SIP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP-Protokoll-Manager: Status-Informations-Trace Trace-Level **3** (INTER): Meldungen an andere Komponenten Trace-Level **6** (INTRA): Meldungen nach SSA Trace-Level **9** (DETAIL): Alle anderen Aktionen

SIP_CFG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Trace der Konfigurationsdaten, die über das WBM erreicht werden.

SIP_CFG_INT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Interner Konfigurationsdaten-Trace.

SIP_FM

Konfiguriertes Default-Trace-Level: **3**

Trace-Level **0**: Nicht verwendet.

Trace-Level **3**: Externe Schnittstellen des SIP-Feature-Managers.

Trace-Level **6**: Externe und interne Schnittstellen des SIP-Feature-Managers.

Trace-Level **9**: Externe und interne Schnittstellen und Details des Verarbeitungsprozesses innerhalb des SIP-Feature-Managers.

SIP_GLOBAL_SI_DOWNLOADS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Trace für die Downloaddaten des System-Interface.

SIP_HT

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP für H.323-Konverter: SIP-Anrufsignalisierung. Trace-Level **3** (INTER): Trace-Level **6** (INTRA): Trace-Level **9** (DETAIL):

SIP_REG

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP-Stack-Adapter: REGISTER und OPTIONEN Trace-Level **3** (INTER): Trace-Level **6** (INTRA): Trace-Level **9** (DETAIL):

SIP_SA

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP-Stack-Adapter Trace-Level **3** (INTER): Trace-Level **6** (INTRA): Trace-Level **9** (DETAIL):

SIP_TRK

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SIP_TRK_FM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SIU_STARTUP

konfiguriertes Default-Trace-Level: n/a

SLMO_HFA

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SMP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SNMP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusausgabe (0) Detailinformationen (9) zu den Konfigurationsdaten (via SNMP) und interne SNMP-Informationen und -Probleme. Bitte diese Trace-Komponente nur nach Absprache mit der Entwicklung verwenden!

SPE_SVC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SPL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SSL_UTIL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

SSM

Konfiguriertes Default-Trace-Level: **0** (STATUS)

STACKTRACE

Konfiguriertes Default-Trace-Level: **0** (STATUS)

STATIC_ROUTES

Konfiguriertes Default-Trace-Level: **0** (STATUS)

STB (nur HG 3575)

Konfiguriertes Default-Trace-Level: **3** (INTER)

Trace-Level **0** (STATUS): Hoch- und Herunterfahren; empfangene Fehler von anderen Komponenten.

Trace-Level **3** (INTER): Empfangene und gesendete Meldungen usw.

Trace-Level **6** (INTRA): Funktionsspezifische Informationen.

Trace-Level **9** (DETAIL): Funktionsspezifische Informationen mit Daten.

STRC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

STREAMS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet.

Trace-Level **3-9**: Interne Meldungen vom Streams-Speicher-Management.

SWCONF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Schwere Fehler, z. B. fehlende Parameter, unbekannte Befehle usw.

Trace-Level **3** (INTER): Status-Informationen zu Job-Handling und Prozess.

Trace-Level **6** (INTRA): Detail-Informationen zu allen Arten von Jobs, z. B. HTTP-Dateiübertragungen, MGAF usw.

SYSTEM

Konfiguriertes Default-Trace-Level: **3** (INTER)

Trace-Level **3** (INTER): Immer an; globale Systeminformation (nicht ändern!).

T90

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Aktionen des T.90-Protokolls. Nur für Entwickler.

TC (nur HG 3500)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Statusinformation über die TC-Komponente, Initialisierung der Komponente.

Trace-Level **3** (INTER): Basis-Kommunikation der anderen Komponenten mit der TC-Komponente.

Trace-Level **6** (INTRA): Internal method calls und detailliertere Informationen über die Komponente.

Trace-Level **9** (DETAIL): Informationen zum internen Debugger.

TCP_IP_CONF (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TCPMOT_WT (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TCPSIG (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TCPSIG_WT (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TCPSUV (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TCPSUV_WT (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TESTLW

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0**–9: Detaillierte Information über TESTLW-Aktionen – nur für Entwickler.

TIME_SYNC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Probleme beim Konfigurieren der SNTP-Zeitsynchronisation (nicht relevant für HG 3500/3575).

TIME_SYNCH_TASK (nur HG 3575)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

TOOLS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Ende eines Threads in der Klasse *OSThread*.

TRAP

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Wichtige Statusinformationen (Trap von IP-Adresse und Port, SNMP-Trap-Version). Schwere Fehler beim Empfangen von Traps.

Trace-Level **6** (INTRA): Statusinformationen wie z. B.: - Trap-Empfang OK - Trap empfangen von localhost oder von woanders - Fehlerinformation Hinzufügen eines Traps in den Trap-Speicher und Löschen eines Traps aus dem Trap-Speicher.

Trace-Level **9** (DETAIL): Detaillierte Informationen.

TSA (nur HG 3500)

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Statusinformation über die TSA-Komponente, Initialisierung der Komponente.

Trace-Level **3** (INTER): Basis-Kommunikation der anderen Komponenten mit der TSA-Komponente.

Trace-Level **6** (INTRA): Internal method calls und detailliertere Informationen über die Komponente.

Trace-Level **9** (DETAIL): Informationen zum internen Debugger.

WAN

Konfiguriertes Default-Trace-Level: **0** (STATUS)

WEBAPPL

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3/6** (INTER/INTRA): Eingang/Ausgang wichtiger Webanwendungs-Funktionen und -Methoden (für Entwickler).

WEBSERVER

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Eingang/Ausgang wichtiger Webserver-Funktionen und -Methoden (für Entwickler).

WEBSERVER_STATISTIC

Konfiguriertes Default-Trace-Level: **0** (STATUS)

WEBSRV_CLIENT_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **1**: Trace aller von einem HTTP-Client (üblicherweise einem Browser) angeforderten URLs und URIs. Nur der Name des URIs wird ausgegeben.

Trace-Level **3** (INTER): HTTP-Socket-Trace (ohne Poll-Anforderungen). HTTP-Daten einschließlich des HTTP-Stacks werden wie vom Browser gesendet ausgegeben. HTTP-Daten einschließlich des HTTP-Stacks dynamischer Seiten (XML) werden wie zum Browser gesendet ausgegeben.

Trace-Level **4**: Trace-Level 3, jedoch zusätzlich mit Poll-Anforderungen.

Trace-Level **6** (INTRA): HTTP-Socket-Trace (ohne Poll-Anforderungen). HTTP-Daten einschließlich des HTTP-Stacks werden wie vom Browser gesendet ausgegeben. HTTP-Daten einschließlich des HTTP-Stacks dynamischer Seiten (XML) und generierter/statischer Seiten (HTML) werden wie zum Browser gesendet ausgegeben.

WEBSRV_SYS_IF

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **2**: Hinweis: Dieser Trace enthält keine Trace-Informationen für Poll-Anforderungen. Vom und zum Gatekeeper gesendete Daten (Gateway-Erkennung, automatisches Auffinden).

Trace-Level **3** (INTER): Trace der Administrations-Schnittstelle. Daten, die zur Administrations-Schnittstelle gesendet werden, und XML-Daten, die von der Administrations-Schnittstelle erhalten werden.

Trace-Level **6** (INTRA): Benutzer- und Kennwortinformationen.

Trace-Level **9** (DETAIL): Zur Administrations-Schnittstelle gesendete Login-Daten, an einen Client gesendete Antwort, sowie interne Parameter-Tabellen-Informationen.

X25

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Aktionen des X.25-Protokolls. Nur für Entwickler.

X75

Konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0–9**: Statusinformationen bis detaillierte Informationen zu Aktionen des X.75-Protokolls. Nur für Entwickler.

XMLUTILS

Konfiguriertes Default-Trace-Level: **0** (STATUS)

9.1.2 Trace-Profile

9.1.2.1 Profile bei Normal-/Hochlast

NOTICE: Diese Profile belasten das System nur schwach und können deshalb bei Normal-/Hochlast gestartet werden.

Übersicht der Profile bei Normal-/Hochlast
'1.1.1(normal) SIP Reg. for Sub. and Trk.'
"1.1.2(normal) SIP Trk. General problems'
"1.1.3(normal) SIP Trk. Payload problems'
"1.1.4(normal) SIP Trk. Fax problems'
"1.2.1(normal) SIP Sub. General problems'
"1.2.2(normal) SIP Sub. Payload problems'

Übersicht der Profile bei Normal-/Hochlast
"1.2.3(normal) SIP Sub. Fax problems'
"1.3(normal) SPE Zusatz für SIP Sub./Trk."
"2.1.1(normal) H.323 Trk. General problems'
"2.1.2(normal) H.323 Trk. Payload problems'
"2.1.3(normal) H.323 Trk. Fax problems'
"2.2.1(normal) HFA-Registrierung"
"2.2.2(normal) HFA allgemeine Probleme"
"2.2.3(normal) HFA Lastprobleme"
"2.3(normal) SPE-Zusatz HFA/H323 Trk."
"3.1(normal) IPDA allgemeine Probleme"
"3.2(normal) IPDA Lastprobleme"
"3.3(normal) IPDA Faxprobleme"
"4.1(normal) WAML (signaling survivability)"

'1.1.1(normal) SIP Reg. for Sub. and Trk.'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – SIP, Level 9
  – SIP_REG, Level 9
  – SIP_SA, Level 9

"1.1.2(normal) SIP Trk. General problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 0
  – DSS1, Level 0
  – SIP, Level 9
  – SIP_SA, Level 9

"1.1.3(normal) SIP Trk. Payload problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – CNQ, Level 0
  – DSS1, Level 0

  - MSC, Level 0
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.1.4(normal) SIP Trk. Fax problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  - ASP_DSP_EVENT, Level 9
  - ASP_DSP_IOCTL, Level 9
  - ASP_FAX, Level 9
  - CNQ, Level 9
  - DMC, Level 9
  - DSS1, Level 9
  - ISDN_FM, Level 9
  - MSC, Level 9
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.1(normal) SIP Sub. General problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 0
  - DSS1, Level 0
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.2(normal) SIP Sub. Payload problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  - ASP_DSP_EVENT, Level 9
  - ASP_DSP_IOCTL, Level 9
  - CNQ, Level 0
  - DSS1, Level 0
  - MSC, Level 0
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.3(normal) SIP Sub. Fax problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:

- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 9
  – CNQ, Level 0
  – DSS1, Level 0
  – MSC, Level 0
  – SENTA_API, Level 9
  – SIP, Level 9
  – SIP_SA, Level 9

"1.3(normal) SPE Zusatz für SIP Sub./Trk."

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist zu aktivieren:
- – ein LAN-Trace (z. B. Wireshark)
  – den Secure Trace, um Trace-Beacons für den LAN-Trace zu erzeugen.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – DEVMGR, Level 9

"2.1.1(normal) H.323 Trk. General problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 0
  – DSS1, Level 0
  – HSA_SYSTEM, Level 1

"2.1.2(normal) H.323 Trk. Payload problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – CNQ, Level 0
  – DSS1, Level 0
  – HSA_SYSTEM, Level 1
  – MSC, Level 0
  – SENTA_API, Level 9

"2.1.3(normal) H.323 Trk. Fax problems'

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 3
  – CNQ, Level 0

  - HSA_SYSTEM, Level 1
  - MSC, Level 0
  - SENTA_API, Level 9

"2.2.1(normal) HFA-Registrierung"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
  - HFAC, Level 6
  - SLMO_HFA, Level 6
  - TC, Level 6

"2.2.2(normal) HFA allgemeine Probleme"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
  - H323, Level 9
  - HSA_SYSTEM, Level 1
  - TSA, Level 9

"2.2.3(normal) HFA Lastprobleme"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
  - ASP, Level 9
  - ASP_DSP_EVENT, Level 9
  - ASP_DSP_IOCTL, Level 9
  - MSC, Level 9
  - SENTA_API, Level 9

"2.3(normal) SPE-Zusatz HFA/H323 Trk."

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist zu aktivieren:
  - ein LAN-Trace (z. B. Wireshark)
  - den Secure Trace, um Trace-Beacons für den LAN-Trace zu erzeugen.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
  - HSA_SPE, Level 3

"3.1(normal) IPDA allgemeine Probleme"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
  - MPH, Level 3
  - MSC, Level 0

"3.2(normal) IPDA Lastprobleme"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:

- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 0

"3.3(normal) IPDA Faxprobleme"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 0

"4.1(normal) WAML (signaling survivability)"

- Kategorie: Kann bei Normal-/Hoch-Last aktiviert werden.
- Zusätzlich: Zusätzlich ist vorzunehmen:
- – einen LAN-Trace (z. B. Wireshark) aktivieren
  – in der Command-shell 'arpShow' und 'mRouteShow' aufrufen
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – MSC, Level 6
  – MSP_HDLC, Level 9

9.1.2.2 Profile bei Schwachlast

NOTICE: Diese Profile führen zu einer starken Systembelastung und dürfen deshalb nur bei Schwachlast gestartet werden!

Übersicht der Profile bei Schwachlast
"1.1.1(detail) SIP Reg. für Sub. und Trk."
"1.1.2(detail) SIP Trk. General problems'
"1.1.3(detail) SIP Trk. Payload problems'
"1.1.4(detail) SIP Trk. Fax problems'
"1.2.1(detail) SIP Sub. General problems'
"1.2.2(detail) SIP Sub. Payload problems'
"1.2.3(detail) SIP Sub. Fax problems'
"1.3(detail) SPE-Zusatz für SIP Sub./Trk."

Übersicht der Profile bei Schwachlast
"2.1.1(detail) H.323 Trk. General problems'
'2.1.2(detail) H.323 Trk. Payload problems'
"2.1.3(detail) H.323 Trk. Fax problems'
"2.2.1(detail) HFA-Registrierung"
"2.2.2(detail) HFA allgemeine Probleme"
"2.2.3(detail) HFA Lastprobleme"
"2.3(detail) SPE-Zusatz für HFA/H323 Trk."
"3.1(detail) IPDA allgemeine Probleme"
"3.2(detail) IPDA Lastprobleme"
"3.3(detail) IPDA Faxprobleme"
"4.1(detail) WAML (signaling survivability)"
"4.2(detail) Signaling survivability Probleme"

"1.1.1(detail) SIP Reg. für Sub. und Trk."

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – SIP, Level 9
  – SIP_REG, Level 9
  – SIP_SA, Level 9

"1.1.2(detail) SIP Trk. General problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 9
  – DMC, Level 9
  – DSS1, Level 9
  – ISDN_FM, Level 9
  – SIP, Level 9
  – SIP_SA, Level 9

"1.1.3(detail) SIP Trk. Payload problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – CNQ, Level 9
  – DMC, Level 9

  - DSS1, Level 9
  - ISDN_FM, Level 9
  - MSC, Level 9
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.1.4(detail) SIP Trk. Fax problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  - ASP_DSP_EVENT, Level 9
  - ASP_DSP_IOCTL, Level 9
  - ASP_FAX, Level 9
  - MSC 0
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.1(detail) SIP Sub. General problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 9
  - DMC, Level 9
  - DSS1, Level 9
  - ISDN_FM, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.2(detail) SIP Sub. Payload problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  - ASP_DSP_EVENT, Level 9
  - ASP_DSP_IOCTL, Level 9
  - CNQ, Level 0
  - DSS1, Level 0
  - MSC, Level 0
  - SENTA_API, Level 9
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.3(detail) SIP Sub. Fax problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:

- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 9
  – CNQ, Level 9
  – DMC, Level 9
  – DSS1, Level 9
  – MSC, Level 9
  – SENTA_API, Level 9
  – SIP, Level 9
  – SIP_SA, Level 9

"1.3(detail) SPE-Zusatz für SIP Sub./Trk."

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist zu aktivieren:
- – ein LAN-Trace (z. B. Wireshark)
  – den Secure Trace, um Trace-Beacons für den LAN-Trace zu erzeugen.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – DEVMGR, Level 9

"2.1.1(detail) H.323 Trk. General problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – CNQ, Level 9
  – DMC, Level 9
  – DSS1, Level 9
  – H323, Level 9
  – HSA_H225_CS, Level 9
  – HSA_H225_RAS, Level 9
  – HSA_H245, Level 9
  – HSA_SYSTEM, Level 9
  – ISDN_FM, Level 9

'2.1.2(detail) H.323 Trk. Payload problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – CNQ, Level 9
  – DMC, Level 9
  – DSS1, Level 9
  – H323, Level 9
  – HSA_SYSTEM, Level 1
  – ISDN_FM, Level 9
  – MSC, Level 9
  – SENTA_API, Level 9

– SPL 3

"2.1.3(detail) H.323 Trk. Fax problems'

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 9
  – CNQ, Level 9
  – DMC, Level 9
  – FMSEM, Level 9
  – H323, Level 9
  – HSA_SYSTEM, Level 1
  – ISDN_FM, Level 9
  – MSC, Level 9
  – SENTA_API, Level 9

"2.2.1(detail) HFA-Registrierung"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – HFAC, Level 6
  – SLMO_HFA, Level 6
  – TC, Level 6

"2.2.2(detail) HFA allgemeine Probleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – H323, Level 9
  – HSA_SYSTEM, Level 1
  – TSA, Level 9

"2.2.3(detail) HFA Lastprobleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – MSC, Level 9
  – SENTA_API, Level 9

"2.3(detail) SPE-Zusatz für HFA/H323 Trk."

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Zusätzlich: Zusätzlich ist zu aktivieren:

- – ein LAN-Trace (z. B. Wireshark)
  – den Secure Trace, um Trace-Beacons für den LAN-Trace zu erzeugen.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – DEVMGR, Level 9
  – H323_SPE, Level 9
  – HSA_SPE, Level 6

"3.1(detail) IPDA allgemeine Probleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ICC, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 9

"3.2(detail) IPDA Lastprobleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 9

"3.3(detail) IPDA Faxprobleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist ein LAN-Trace (z. B. Wireshark) zu aktivieren.
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – ASP, Level 9
  – ASP_DSP_EVENT, Level 9
  – ASP_DSP_IOCTL, Level 9
  – ASP_FAX, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 9

"4.1(detail) WAML (signaling survivability)"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!
- Zusätzlich: Zusätzlich ist vorzunehmen:
- – einen LAN-Trace (z. B. Wireshark) aktivieren
  – in der Command-shell 'arpShow' und 'mRouteShow' aufrufen
- Enthaltene Trace-Komponenten und zugeordnete Trace-Level:
- – MSC, Level 6
  – MSP_HDLC, Level 9

"4.2(detail) Signaling survivability Probleme"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!

"4.4(detail) NCUI Neustart nach TCP-Zeitüberschreitung"

- Kategorie: Darf nur bei Schwachlast aktiviert werden!

9.2 Events

Die nachfolgenden Abschnitte entsprechen dem Inhalt nach den Original-Event-Templates.

Jedem Event ist ein Event-Typ zugeordnet. Folgende Event-Typen sind möglich:

- **Information:** Reine Statusmeldung, keine Problemmeldung.
- **Warning:** Meldung über einen möglicherweise problematischen Vorgang oder Zustand, jedoch keine Fehlermeldung.
- **Minor:** Fehlermeldung. Der Fehler hat jedoch keine problematischen Auswirkungen.
- **Major:** Fehlermeldung. Der Fehler kann problematische Auswirkungen haben.
- **Critical:** Fehlermeldung. Der Fehler hat problematische Auswirkungen.
- **Cleared:** Fehlermeldung. Der Fehler wurde jedoch vom System bereits behoben.
- **Indeterminate:** Fehlermeldung. Die Fehlerursache ist jedoch nicht genau bestimmbar.

Die Beschreibungen enthalten zu jedem Event:

- den Event-Code,
- den Meldungstext im Log-Eintrag oder an der Benutzeroberfläche,
- den Event-Typ (siehe oben),
- Erläuterungen zu Ursachen, Reaktionen des Systems und gegebenenfalls zu möglichen Fehlerbehebungsmaßnahmen.

Einige Meldungstexte (EventTexts) enthalten variable Daten. Diese sind wie folgt gekennzeichnet:

- `%s` bedeutet: Zeichenkette
- `%d` und `%I` bedeuten: positive Dezimalzahl
- `%u` bedeutet: positive oder negative Dezimalzahl
- `%f` bedeutet: Fließkommazahl
- `%p` bedeutet: Zeiger (Speicheradresse)
- `%x` bedeutet: Hexadezimalzahl (mit Kleinbuchstaben)
- `%X` bedeutet: Hexadezimalzahl (mit Großbuchstaben)
- `%c` bedeutet: einzelnes Zeichen

9.2.1 Übersicht: Event-Codes

Die Tabelle dient dem schnelleren Auffinden bestimmter Status- und Fehlermeldungen. Die Tabelle ist nach Event-Codes alphabetisch sortiert. Da alle Event-Codes mit `MSG_` beginnen, beginnt die effektive Sortierung erst beim fünften Zeichen.

Event-Code	Abschnitt
ASSERTION_FAILED_EVENT	10.2.3, 'Reboot-Events'
CCE_GENERAL_ERROR	10.2.49, 'LAN-Signalisierung bezogene Events - CCE'
CCE_PSS_STORE_ERROR	10.2.49, 'LAN-Signalisierung bezogene Events - CCE'
COMGA_NOK_UPGRADE_REG	10.2.2, 'Status-Events'
EXIT_REBOOT_EVENT	10.2.3, 'Reboot-Events'
FP_EVT_CRITICAL	10.2.3, 'Reboot-Events'
FP_EVT_INDETERMINATE	10.2.2, 'Status-Events'
FP_EVT_MAJOR	10.2.3, 'Reboot-Events'
FP_EVT_MINOR	10.2.2, 'Status-Events'
FP_EVT_SNMP_TRAP	10.2.2, 'Status-Events'
FP_EVT_INFORMATION	10.2.2, 'Status-Events'
FP_EVT_TRACE_START	10.2.2, 'Status-Events'
FP_EVT_TRACE_STOP	10.2.2, 'Status-Events'
FP_EVT_WARNING	10.2.3, 'Reboot-Events'
FW_NOK_UPGRADE_REG	10.2.2, 'Status-Events'
H323_NO_IP	10.2.8, 'H.323-Events'
H323_SNMP_TRAP	10.2.8, 'H.323-Events'
MSG_ADMIN_DIDNâT_GET_WRITE_ACCESS	10.2.29, 'OAM-Events'
MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS	10.2.29, 'OAM-Events'
MSG_ADMIN_GOT_WRITE_ACCESS	10.2.29, 'OAM-Events'
MSG_ADMIN_INVALID_LOGIN	10.2.29, 'OAM-Events'
MSG_ADMIN_LOGGED_IN	10.2.29, 'OAM-Events'
MSG_ADMIN_LOGGED_OUT	10.2.29, 'OAM-Events'
MSG_ADMIN_REBOOT	10.2.3, 'Reboot-Events'
MSG_ADMIN_RELEASED_WRITE_ACCESS	10.2.29, 'OAM-Events'
MSG_ADMIN_SESSION_CREATED	10.2.29, 'OAM-Events'
MSG_ADMIN_SESSION_EXPIRED	10.2.29, 'OAM-Events'
MSG_ASC_ERROR	10.2.35, 'Major ASC-Events'
MSG_ASP_ERROR	10.2.36, 'Major ASP-Events'

Event-Code	Abschnitt
MSG_ASP_INFO	10.2.34, 'Wichtige Plattform-Software-Status-Events'
MSG_ASP_INFO	10.2.37, 'Minor ASP Events'
MSG_ASP_REBOOT	10.2.3, 'Reboot-Events'
MSG_BSD44_ACCEPT_DGW_ERR	10.2.12, 'DGW-Events'
MSG_BSD44_ACCEPT_ERROR	10.2.23, 'VCAPI-Events'
MSG_BSD44_DGW_BIND_FAIL	10.2.12, 'DGW-Events'
MSG_BSD44_DGW_CONNECT_FAIL	10.2.12, 'DGW-Events'
MSG_BSD44_DGW_NO_LIST	10.2.12, 'DGW-Events'
MSG_BSD44_DGW_SOCKET_FAIL	10.2.12, 'DGW-Events'
MSG_BSD44_SELECT_ERROR	10.2.23, 'VCAPI-Events'
MSG_BSD44_VCAPI_NO_LIST	10.2.12, 'DGW-Events'
MSG_CAR_ALIVE_IP_CONNECTION_LOST	10.2.13, 'CAR-Events'
MSG_CAR_ALIVE_IP_CONNECTION_LOST	10.2.13, 'CAR-Events'
MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN	10.2.13, 'CAR-Events'
MSG_CAR_CALL_ADDR_REJECTED	10.2.29, 'OAM-Events'
MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB	10.2.13, 'CAR-Events'
MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS	10.2.13, 'CAR-Events'
MSG_CAR_CODEC_ENTRY_DELETED	10.2.13, 'CAR-Events'
MSG_CAR_CODECS_INCONSISTENT	10.2.13, 'CAR-Events'
MSG_CAR_DB_READ_NODE_TABLE_ERROR	10.2.13, 'CAR-Events'
MSG_CAR_DBF_SERVER_INCONSISTENT	10.2.13, 'CAR-Events'
MSG_CAR_DBFS_POSS_CONFLICT	10.2.13, 'CAR-Events'
MSG_CAR_ERROR_WITH_OAM_INTERFACE	10.2.13, 'CAR-Events'
MSG_CAR_FKT_GET_IPADR_FAILED	10.2.13, 'CAR-Events'
MSG_CAR_GENERAL_ERROR	10.2.13, 'CAR-Events'
MSG_CAR_MALLOC_FAILED	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_CAR_NO_FREE_CODEC_TAB_ELE	10.2.13, 'CAR-Events'
MSG_CAR_NO_MAC_ADDRESS	10.2.13, 'CAR-Events'
MSG_CAR_NO_MEMORY	10.2.13, 'CAR-Events'

Event-Code	Abschnitt
MSG_CAR_NODE_INFO_ALREADY_AVAILABLE	10.2.13, 'CAR-Events'
MSG_CAR_PARAM_NOT_FOUND	10.2.13, 'CAR-Events'
MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_NO_MEMORY	10.2.13, 'CAR-Events'
MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_SOH_ERROR	10.2.13, 'CAR-Events'
MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS	10.2.13, 'CAR-Events'
MSG_CAR_START_TCP_LISTENER_FAILED	10.2.13, 'CAR-Events'
MSG_CAR_UNAUTHORIZED_IP_ACCESS	10.2.13, 'CAR-Events'
MSG_CAR_UNEXPECTED_DATA_RECV	10.2.13, 'CAR-Events'
MSG_CAR_UNEXPECTED_MSG_RECV	10.2.13, 'CAR-Events'
MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CAL_ADDRTAB_TOO_BIG	10.2.13, 'CAR-Events'
MSG_CAR_WRONG_EVENT	10.2.13, 'CAR-Events'
MSG_CAR_WRONG_IP_ADDRESS	10.2.13, 'CAR-Events'
MSG_CAR_WRONG_LENGTH	10.2.13, 'CAR-Events'
MSG_CAR_WRONG_NODE_ID	10.2.13, 'CAR-Events'
MSG_CAR_WRONG_SERVICE	10.2.13, 'CAR-Events'
MSG_CAT_H235	10.2.9, 'H.235-Events'
MSG_CAT_H323_REBOOT	10.2.3, 'Reboot-Events'
MSG_CAT_HSA_REBOOT	10.2.2, 'Status-Events'
MSG_CAT_NWRS	10.2.5, 'Routing-Events'
MSG_CLI_LOGGED_IN_FROM_TELNET	10.2.30, 'CLI-Events'
MSG_CLI_LOGGED_IN_FROM_V24	10.2.30, 'CLI-Events'
MSG_CLI_TELNET_ABORTED	10.2.30, 'CLI-Events'
MSG_DELIC_ERROR	10.2.41, 'DELIC-Events'
MSG_DEVM_BINDING_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY	10.2.33, 'MAGIC / Device-Manager-Events'

Event-Code	Abschnitt
MSG_DEVMGR_CLOSE_LEG_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_LEGS_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_WRONG_LEGS	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_WRONG_RES_STATE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CREATE_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_DEVICEID_OUT_OF_RANGE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_DISCONNECT_LEGS_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_CHNID	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_DEVID	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_RESID	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_LAYER2_SERVICE_TRAP	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_LISTEN_WRONG_RES_STATE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_MSCERROR_RESID	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_OPEN_LEG_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_OPEN_WRONG_RES_STATE	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_SCN_TASK_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_UPDATE_LEG_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_DGW_ABORT_SOCK_UNKN	10.2.12, 'DGW-Events'

Event-Code	Abschnitt
MSG_DGW_ACCEPT_FAILED	10.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CHN_CONN_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CHN_RUN_OUT	10.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CONF_ERR	10.2.12, 'DGW-Events'
MSG_DGW_ALLOC_DISC_B3	10.2.12, 'DGW-Events'
MSG_DGW_ALLOC_REQ_ERR	10.2.12, 'DGW-Events'
MSG_DGW_BUFAVAIL_SOCK_UNKN	10.2.12, 'DGW-Events'
MSG_DGW_CONF_ALLOC_ERR	10.2.12, 'DGW-Events'
MSG_DGW_CONN_B3_ACT_IND	10.2.12, 'DGW-Events'
MSG_DGW_CONN_COMPL_ALLOC	10.2.12, 'DGW-Events'
MSG_DGW_CONN_OUT_OF_RANGE	10.2.12, 'DGW-Events'
MSG_DGW_CONN_RUN_OUT	10.2.12, 'DGW-Events'
MSG_DGW_CONNECT_FAILED	10.2.12, 'DGW-Events'
MSG_DGW_DATA_B3_ALLOC_ERR	10.2.12, 'DGW-Events'
MSG_DGW_DISC_B3_IND	10.2.12, 'DGW-Events'
MSG_DGW_DISC_B3_NOT_SEND	10.2.12, 'DGW-Events'
MSG_DGW_FREE_ALLOC_ERR	10.2.12, 'DGW-Events'
MSG_DGW_FREE_CHN_ALLOC_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_FREE_NOT_SEND	10.2.12, 'DGW-Events'
MSG_DGW_FREE_UNKNOWN_ID	10.2.12, 'DGW-Events'
MSG_DGW_IND_ALLOC_ERR	10.2.12, 'DGW-Events'
MSG_DGW_INV_DATA_LEN	10.2.12, 'DGW-Events'
MSG_DGW_INV_MSG_LEN	10.2.12, 'DGW-Events'
MSG_DGW_INVALID_LENGTH	10.2.12, 'DGW-Events'
MSG_DGW_LISTENING_ERR	10.2.12, 'DGW-Events'
MSG_DGW_MGR_NOT_READY	10.2.12, 'DGW-Events'
MSG_DGW_MSG_IGNORED	10.2.12, 'DGW-Events'
MSG_DGW_MSG_RCV_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_NO_PLCI	10.2.12, 'DGW-Events'
MSG_DGW_OPEN_CHN_ALLOC_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_OPEN_CHN_UNKNOWN_ID	10.2.12, 'DGW-Events'

Event-Code	Abschnitt
MSG_DGW_OPEN_CHN_WRONG	10.2.12, 'DGW-Events'
MSG_DGW_RCV_ALLOC_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_RCV_FAILED	10.2.12, 'DGW-Events'
MSG_DGW_RCV_SOCK_UNKN	10.2.12, 'DGW-Events'
MSG_DGW_RECEIVE_ERR	10.2.12, 'DGW-Events'
MSG_DGW_SEC_ALLOC_FAIL	10.2.12, 'DGW-Events'
MSG_DGW_SEND_DATA_ERR	10.2.12, 'DGW-Events'
MSG_DGW_SEND_FAILED	10.2.12, 'DGW-Events'
MSG_DGW_SOCKET_BIND_ERR	10.2.12, 'DGW-Events'
MSG_DGW_SOCKET_NOT_OPEN	10.2.12, 'DGW-Events'
MSG_DGW_SOCKET_UNKNOWN	10.2.12, 'DGW-Events'
MSG_DGW_UNH_MSG_CAPI20_MGR	10.2.12, 'DGW-Events'
MSG_DGW_UNHANDLED_EVENT	10.2.12, 'DGW-Events'
MSG_DGW_UNHANDLED_MSG	10.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_ID_CHANNEL	10.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_NOTIFIC	10.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_PRIMITIVE	10.2.12, 'DGW-Events'
MSG_DGW_WRONG_EVENT_CAPI	10.2.12, 'DGW-Events'
MSG_DGW_WRONG_EVENT_CAPI20	10.2.12, 'DGW-Events'
MSG_DGW_WRONG_STATE	10.2.12, 'DGW-Events'
MSG_DLSC_BOOTSTRAP_OK	10.2.2, 'Status-Events'
MSG_DISP_SENDER_NOT_SET	10.2.29, 'OAM-Events'
MSG_ERH_ADMISSION_ERROR	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_ERROR	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_INFORMATION	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_NO_LICENSE	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'

Event-Code	Abschnitt
MSG_ERH_REGISTRATION_ERROR	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_SECURITY_DENIAL	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_SUB_OUT_OF_SERVICE	10.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_EXCEPTION_REBOOT	10.2.3, 'Reboot-Events'
MSG_FAXCONV_ERROR	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_FIREWALL_ALARM	10.2.2, 'Status-Events'
MSG_FAXCONV_INFO	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_GSA_SNMP	10.2.11, 'GSA-Events'
MSG_GW_OBJ_ALLOC_FAILED	10.2.3, 'Reboot-Events'
MSG_GW_OBJ_MEMORY_EXHAUSTED	10.2.3, 'Reboot-Events'
MSG_GW_OBJ_MEMORY_INCONSISTENT	10.2.3, 'Reboot-Events'
MSG_GW_SUCCESSFULLY_STARTED	10.2.2, 'Status-Events'
MSG_H323_INFORMATION	10.2.8, 'H.323-Events'
MSG_H323_INVALID_CONFIGURATION	10.2.8, 'H.323-Events'
MSG_H323_INVALID_PARAMETER_VALUE	10.2.8, 'H.323-Events'
MSG_H323_INVALID_POINTER	10.2.8, 'H.323-Events'
MSG_H323_LOGIC_ERROR	10.2.8, 'H.323-Events'
MSG_H323_MISSING_PARAMETER	10.2.8, 'H.323-Events'
MSG_H323_OSCAR_NSD_ERROR	10.2.8, 'H.323-Events'
MSG_H323_PROTOCOL_ERROR	10.2.8, 'H.323-Events'
MSG_H323_SNMP_TRAP	10.2.8, 'H.323-Events'
MSG_H323_STACK_ERROR	10.2.8, 'H.323-Events'
MSG_H323_UNEXPECTED_MESSAGE	10.2.8, 'H.323-Events'
MSG_H323_UNEXPECTED_RETURN_VALUE	10.2.8, 'H.323-Events'
MSG_H323CLIENT_INVALID_ADMIN_MSG	10.2.25, 'H.323-Client-Events'

Event-Code	Abschnitt
MSG_H323CLIENT_INVALID_CLIENTID	10.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_INVALID_PARAM	10.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_MAPS_DIFFER	10.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_NWRS_ENTRY_FAILED	10.2.25, 'H.323-Client-Events'
MSG_HBR_WARNING	10.2.2, 'Status-Events'
MSG_HACKER_ON_SNMP_PORT_TRAP	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_HFAA_INTERNAL_ERROR	10.2.18, 'HFA-Adapter-Events'
MSG_HFAA_INTERNAL_EVENT	10.2.18, 'HFA-Adapter-Events'
MSG_HFAA_MEMORY_ERROR	10.2.18, 'HFA-Adapter-Events'
MSG_HFAA_MESSAGE_ERROR	10.2.18, 'HFA-Adapter-Events'
MSG_HFAA_PARAM_ERROR	10.2.18, 'HFA-Adapter-Events'
MSG_HFAM_HAH_ALLOC_CHAN_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_HAH_ALLOC_CONF_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ALGORITM_OBJID_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_BIND_REGISOCK_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_CREATE_REGISOCK_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_IPADR_TOO_LONG_ERR	10.2.17, 'HFA-Manager-Events'

Event-Code	Abschnitt
MSG_HFAM_LIH_LISTEN_REGISOCK_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_MAX_CON_EXCEED_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_PROTOCOL_LIST_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_RETURNED_SOCKET_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_UNEXP_CORNET_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_ILLEG_PORTNO_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_NO_LOGONTIMER_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_MON_NO_MON_TIMER_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_ESTAB_NOTREG_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_INVAL_PWD_LEN_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_LOGIN_NOTREG_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_LOGON_REJECT_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_MISSING_L2INFO_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_RELIN_NOTREG_ERR	10.2.17, 'HFA-Manager-Events'

Event-Code	Abschnitt
MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_SUBNO_TOO_LONG_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_CORNET_LONGER_28_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR	10.2.17, 'HFA-Manager-Events'
MSG_HIP_ALLOC_DEV_OBJ	10.2.31, 'HIP-Events'
MSG_HIP_ALLOC_MES_SI	10.2.31, 'HIP-Events'
MSG_HIP_NO_CLBLK	10.2.31, 'HIP-Events'
MSG_HIP_NO_CLPOOL_ID	10.2.31, 'HIP-Events'
MSG_HIP_NO_CLUSTER	10.2.31, 'HIP-Events'
MSG_HIP_NO_DEVLOAD	10.2.31, 'HIP-Events'
MSG_HIP_NO_DEVSTART	10.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_CL	10.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_CLBLK	10.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_TO_SI	10.2.31, 'HIP-Events'
MSG_HIP_NO_NETPOOL_INIT	10.2.31, 'HIP-Events'
MSG_HIP_NO_OBJ_INIT	10.2.31, 'HIP-Events'
MSG_HIP_NO_PMBLK	10.2.31, 'HIP-Events'
MSG_HIP_PKTLEN_ZERO	10.2.31, 'HIP-Events'
MSG_HIP_PMBLK_ZERO	10.2.31, 'HIP-Events'
MSG_IP_LINK2_FAILURE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK2_FAILURE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK_RESTORE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK2_RESTORE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK_SWITCHOVER	10.2.4, 'Ressourcen-Überwachungs-Events'

Event-Code	Abschnitt
MSG_IP_LINK2_SWITCHOVER	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_RTP_QUALITY_FAILURE	10.2.10, 'RTPQM-Events'
MSG_IP_RTP_QUALITY_WARNING	10.2.10, 'RTPQM-Events'
MSG_IPACCSRV_INTERNAL_ERROR	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_LOGON	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MARK_REACHED	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MEMORY_ERROR	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MESSAGE_ERROR	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_OVERFLOW	10.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_SOCKET_ERROR	10.2.44, 'IP-Accounting-Events'
MSG_IPF_ON_OFF	10.2.38, 'IP-Filter-Events'
MSG_IPF_PARAMETER	10.2.38, 'IP-Filter-Events'
MSG_IPF_STARTED	10.2.38, 'IP-Filter-Events'
MSG_IPF_STOPPED	10.2.38, 'IP-Filter-Events'
MSG_IPNC_CP_ASYNCH	10.2.26, 'IPNC-Events'
MSG_IPNC_INCONSISTENT_STATE	10.2.26, 'IPNC-Events'
MSG_IPNC_INTERNAL_ERROR	10.2.26, 'IPNC-Events'
MSG_IPNC_MESSAGE_DUMP	10.2.26, 'IPNC-Events'
MSG_IPNC_MESSAGE_ERROR	10.2.26, 'IPNC-Events'
MSG_IPNC_PARAM_ERROR	10.2.26, 'IPNC-Events'
MSG_IPNCA_ERROR	10.2.27, 'IPNC- Events'
MSG_IPNCV_INTERNAL_ERROR	10.2.2, 'Status-Events'
MSG_IPNCV_MEMORY_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IPNCV_SIGNALING_ERROR	10.2.46, 'IPNCV-Events'
MSG_IPNCV_STARTUP_ERROR	10.2.2, 'Status-Events'

Event-Code	Abschnitt
MSG_IPNCV_STARTUP_SHUTDOWN	10.2.2, 'Status-Events'
MSG_IPSEC_REBOOT	10.2.3, 'Reboot-Events'
MSG_IPSTACK_INVALID_PARAM	10.2.40, 'IP-Stack-Events'
MSG_IPSTACK_NAT_ERROR	10.2.40, 'IP-Stack-Events'
MSG_IPSTACK_SOH_ERROR	10.2.40, 'IP-Stack-Events'
MSG_ISDN_CMR_ADD_OBJECT_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_DEVICE_PTR_BAD	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_GEN_CALL_REF_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_GENRIC_EVENT	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_INIT_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MAND_FIELDS_MISSING	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MESSAGE_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_DECODE_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_ENCODE_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_SEND_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_UNEXPECTED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_NEW_OBJECT_FAILED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_OBJECT_NOT_FOUND	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_PROTOCOL_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_SEG_MSG_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_SESSION_NOT_FOUND	10.2.7, 'SCN-Protokoll-Events'

Event-Code	Abschnitt
MSG_ISDN_CMR_STATUS_MSG_RECEIVED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_TIMER_EXPIRED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_EVENT	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_VALUE	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNH_STATE_EVENT	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNIMPLEMENTED	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_DEVICE_TYPE	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_INTERFACE	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_PROTVAR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_DEVICE_PTR_NOT_FOUND	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_NO_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_NULL_PTR	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_OVERLOAD_CONDITION	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_IN_USE_BY_O_CALL	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_NOT_AVAILABLE	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_NOT_IN_SERVICE	10.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_START_UP	10.2.7, 'SCN-Protokoll-Events'

Event-Code	Abschnitt
MSG_ISDN_START_UP_ERROR	10.2.7, 'SCN-Protokoll-Events'
MSG_LDAP_ENCODE_DECODE_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_GENERAL_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_IP_LINK_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_MEMORY_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_SOCKET_ERROR	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_SUCCESSFULLY_STARTED	10.2.2, 'Status-Events'
MSG_LLC_EVENT_INVALID_PARAMETER_VALUE	10.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_MISSING_PARAMETER	10.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_MISSING_RESOURCE	10.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE	10.2.50, 'Events für LLC-Operation'
MSG_MAF_ETHERNET_HEADER	10.2.39, 'MAC-Filter-Events'
MSG_MAF_NETBUFFER	10.2.39, 'MAC-Filter-Events'
MSG_MAF_NO_OF_RULES	10.2.39, 'MAC-Filter-Events'
MSG_MAF_ON_OFF	10.2.39, 'MAC-Filter-Events'
MSG_MAF_PARAMETER	10.2.39, 'MAC-Filter-Events'
MSG_MAF_STARTED	10.2.39, 'MAC-Filter-Events'
MSG_MAF_STOPPED	10.2.39, 'MAC-Filter-Events'
MSG_MAND_PARAM_MISSING	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_MIKEY_REBOOT	10.2.3, 'Reboot-Events'
MSG_MPH_INFO	10.2.28, 'MPH-Events'
MSG_MSP_FAX_OVERLONG_PKT	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_MSP_HDLC_ERROR	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'

Event-Code	Abschnitt
MSG_MSP_HDLC_INFO	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_NU_CAR_FAILED	10.2.15, 'NU-Events'
MSG_NU_CAR_RESP_INVALID	10.2.15, 'NU-Events'
MSG_NU_DEV_TAB_NOT_FOUND	10.2.15, 'NU-Events'
MSG_NU_EVENT_EXCEPTION	10.2.15, 'NU-Events'
MSG_NU_FREE_CHN_COMF_TOO_LATE	10.2.15, 'NU-Events'
MSG_NU_FREE_CHN_UNEXPECTED	10.2.15, 'NU-Events'
MSG_NU_GENERAL_ERROR	10.2.15, 'NU-Events'
MSG_NU_INTERNAL_ERROR	10.2.15, 'NU-Events'
MSG_NU_INVALID_CIDL	10.2.15, 'NU-Events'
MSG_NU_IP_ERROR	10.2.15, 'NU-Events'
MSG_NU_NO_FREE_TRANSACTION	10.2.15, 'NU-Events'
MSG_NU_NO_PORT_DATA	10.2.15, 'NU-Events'
MSG_NU_SOH_RESP_INVALID	10.2.15, 'NU-Events'
MSG_NU_SUPERFLUOS_MSG	10.2.15, 'NU-Events'
MSG_NU_TCP_LISTENER_FAILED	10.2.15, 'NU-Events'
MSG_NU_TOO_MUCH_DIGITS	10.2.15, 'NU-Events'
MSG_NU_TRANSPCONT_MISSING	10.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_MSG	10.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_SETUP	10.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_TIMER	10.2.15, 'NU-Events'
MSG_NU_UNKNOWN_MESSAGE	10.2.15, 'NU-Events'
MSG_NU_WRONG_CALL_REF	10.2.15, 'NU-Events'
MSG_NULC_INTERNAL_ERROR	10.2.16, 'NU Leg Control Events'
MSG_NULC_INTERNAL_EVENT	10.2.16, 'NU Leg Control Events'
MSG_NULC_MEMORY_ERROR	10.2.16, 'NU Leg Control Events'
MSG_NULC_MESSAGE_ERROR	10.2.16, 'NU Leg Control Events'

Event-Code	Abschnitt
MSG_NULC_PARAM_ERROR	10.2.16, 'NU Leg Control Events'
MSG_NWRS_DEVICE_NOT_FOUND	10.2.5, 'Routing-Events'
MSG_NWRS_DEVICE_TABLE_NOT_FOUND	10.2.5, 'Routing-Events'
MSG_NWRS_DPLN_ENTRY_INVALID	10.2.5, 'Routing-Events'
MSG_NWRS_DPLN_NOT_FOUND	10.2.5, 'Routing-Events'
MSG_NWRS_EMPTY_FIELD_ECHOED	10.2.5, 'Routing-Events'
MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE	10.2.5, 'Routing-Events'
MSG_NWRS_ODR_COMMAND_UNKNOWN	10.2.5, 'Routing-Events'
MSG_NWRS_ODR_NOT_FOUND	10.2.5, 'Routing-Events'
MSG_NWRS_ROUTE_NOT_FOUND	10.2.5, 'Routing-Events'
MSG_NWRS_UNKNOWN_FIELD_ECHOED	10.2.5, 'Routing-Events'
MSG_NWRS_UNSPEC_ERROR	10.2.5, 'Routing-Events'
MSG_OAM_DMA_RAM_THRESHOLD_REACHED	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_OVERLOAD_REACHED	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_OVERLOAD_CLEARED	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_FAN_OUT_OF_SERVICE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_INTERNAL_EVENT	10.2.29, 'OAM-Events'
MSG_OAM_PRIO_INCREASED	10.2.29, 'OAM-Events'
MSG_OAM_PRIO_SWITCHED_BACK	10.2.29, 'OAM-Events'
MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_PUT_TO_QUEUE_FAILED	10.2.29, 'OAM-Events'
MSG_OAM_QUEUE_BLOCKED	10.2.29, 'OAM-Events'
MSG_OAM_QUEUE_FULL	10.2.29, 'OAM-Events'
MSG_OAM_RAM_THRESHOLD_REACHED	10.2.4, 'Ressourcen-Überwachungs-Events'

Event-Code	Abschnitt
MSG_OAM_THRESHOLD_REACHED	10.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_TIMESYNC	10.2.29, 'OAM-Events'
MSG_OAM_TIMESYNC_FAILED	10.2.29, 'OAM-Events'
MSG_OS_EXCEPTION_ERROR	10.2.3, 'Reboot-Events'
MSG_ERH_NO_LICENSE	10.2.48, 'Fehler-Events'
MSG_OSF_PCS_EXCEPTION	10.2.3, 'Reboot-Events'
MSG_PPP_STACK_PROC	10.2.21, 'PPP-Stack-Events'
MSG_PPP_STACK_REBOOT	10.2.3, 'Reboot-Events'
MSG_PS_INVALID_STREAM_FROM_ADDRESS	10.2.2, 'Status-Events'
MSG_PS_INVALID_STREAM_FROM_PORT	10.2.2, 'Status-Events'
MSG_PPTP_STACK_REBOOT	10.2.3, 'Reboot-Events'
MSG_PPPM_ERR_CONFIG	10.2.20, 'PPP-Manager-Events'
MSG_PPPM_ERR_OPERATION	10.2.20, 'PPP-Manager-Events'
MSG_REG_ERROR_FROM_SOH	10.2.14, 'REG-Events'
MSG_REG_GLOBAL_ERROR	10.2.14, 'REG-Events'
MSG_REG_NIL_PTR_FROM_SOH	10.2.14, 'REG-Events'
MSG_REG_NO_MEMORY	10.2.14, 'REG-Events'
MSG_REG_NO_REGISTRATION_POSSIBLE	10.2.14, 'REG-Events'
MSG_REG_REQUEST_WITHIN_REGISTRATION	10.2.14, 'REG-Events'
MSG_REG_SOH_SEND_DATA_FAILED	10.2.14, 'REG-Events'
MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH	10.2.14, 'REG-Events'
MSG_RESTORE_CFG_REBOOT	10.2.3, 'Reboot-Events'
MSG_SCN_ADD_PARAMETER_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_BIND_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_DEV_NOT_IN_DEVLIST	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_ERROR_12_MSG	10.2.33, 'MAGIC / Device-Manager-Events'

Event-Code	Abschnitt
MSG_SCN_GET_ADMMSG_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_GET_LDAPMSG_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_OPEN_STREAM_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_OPERATION_ON_STREAM_FAILED	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_POLL_FD	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_UNEXPECTED_L2_MSG	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_UNEXPECTED_POLL_EVENT	10.2.33, 'MAGIC / Device-Manager-Events'
MSG_SDR_INIT	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SDR_UNEXPECTED_EVENT	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SI_L2STUB_COUDNT_OPEN_STREAM	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_ERROR_INIT_DRIVER	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_NO_ALLOC	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_NO_CLONE	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_OPEN_OTHER_STREAM-_NOT_POSSIBLE	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_PORT_NOT_OPEN	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_STREAM_ALREADY_OPEN	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_UNEXPECTED_DB_TYPE	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SI_L2STUB_UNKNOWN_SOURCE_PID	10.2.32, 'SI-Events (System-schnittstellen-Events)'
MSG_SIP_FM_INTERNAL_ERROR	10.2.2, 'Status-Events'
MSG_SIP_FM_MSG_INTERNAL_ERROR	10.2.2, 'Status-Events'

Event-Code	Abschnitt
MSG_SIP_FM_MSG_NOT_PROCESSED	10.2.2, 'Status-Events'
MSG_SIP_FM_STARTUP_FAILURE	10.2.2, 'Status-Events'
MSG_SNCP_ADD_OBJECT_FAILED	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_CHANNEL_ID_MISSING	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_CREATE_OBJECT	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_DELETE_OBJECT	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_SET_FORW_ENC	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_SET_REV_ENC	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_DEVICE_ID_MISSING	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_ERROR	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_NEITHER_ENC_COULD_BE_SET	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_NO_RESOURCE_ID	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_UNANTICIPATED_MESSAGE	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNMP_TRAP_COLLECTOR_START_ERROR	10.2.3, 'Reboot-Events'
MSG_SPE_CERT_MISSING	10.2.22, 'SPE-Events'
MSG_SPE_CERT_AVAIL	10.2.22, 'SPE-Events'
MSG_SPE_CERT_UPDATED	10.2.22, 'SPE-Events'
MSG_SPE_CERT_EXPIRED	10.2.22, 'SPE-Events'
MSG_SPE_CERT_TIMEREMAINING	10.2.22, 'SPE-Events'
MSG_SPE_CRL_EXPIRED	10.2.22, 'SPE-Events'
MSG_SPE_CRL_UPDATED	10.2.22, 'SPE-Events'
MSG_SPE_ALL_CRLS_UPTODATE	10.2.22, 'SPE-Events'
MSG_SPL_ADD_OBJECT_FAILED	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'

Event-Code	Abschnitt
MSG_SPL_ERROR	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_FMSEM_ERROR	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_MISSING_CS_ID	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_SESSION_NOT_FOUND	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_UNANTICIPATED_MESSAGE	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_BAD_NWRS_RESULT	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_INVALID_PARAM	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_NO_CSID	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	10.2.3, 'Reboot-Events'
MSG_SSM_SESSION_CREATION_FAILED	10.2.3, 'Reboot-Events'
MSG_SSM_UNSPEC_ERROR	10.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SYSTEM_REBOOT	10.2.3, 'Reboot-Events'
MSG_STRC_STOP	10.2.2, 'Status-Events'
MSG_STRC_START	10.2.2, 'Status-Events'
MSG_T90_ERROR	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_T90_INFO	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_TESTLW_ERROR	10.2.42, 'Test-Loadware-Events'
MSG_TESTLW_INFO	10.2.42, 'Test-Loadware-Events'
MSG_TLS_MUTEX_BLOCKED	10.2.29, 'OAM-Events'
MSG_TLS_POOL_SIZE_EXCEEDED	10.2.3, 'Reboot-Events'
MSG_VCAPI_ACCEPT_ERROR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_ADD_OBJECT_FAILED	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_BUF_NOT_CREATED	10.2.23, 'VCAPI-Events'

Event-Code	Abschnitt
MSG_VCAPI_CONF_ALLOC_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_CONF_WITHOUT_REQ	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_CONV_H2N_ERROR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_CONV_H2N_FAILED	10.2.23, 'VCAPI-Events'
MSG_VCAPI_CONV_N2H_FAILED	10.2.23, 'VCAPI-Events'
MSG_VCAPI_COULD_NOT_CREATE_OBJECT	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_DELETE_OBJECT	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_CSID	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_OBJECT	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_PLCI	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_STORE_REQ	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_CSID_MISSING	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_DATA_B3_ALLOC_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_DATA_NOT_STORED	10.2.23, 'VCAPI-Events'
MSG_VCAPI_DISP_NOT_READY	10.2.23, 'VCAPI-Events'
MSG_VCAPI_ILLEGAL_LINK_NUMBER	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_ILLEGAL_PARTNER_NUMBER	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_IND_ALLOC_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_LINK_TABLE_FULL	10.2.23, 'VCAPI-Events'
MSG_VCAPI_LISTENING_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_MSG_NOT_SEND	10.2.23, 'VCAPI-Events'
MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG	10.2.24, 'VCAPI-Anwendungs-Events'

Event-Code	Abschnitt
MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_NO_ALLOC_EXTENDED	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_ALLOC_MSG	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_ALLOC_SINGLE	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_CAPI_DATA	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_CLIENT	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_LIST_SOCKET	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_LNK_CONN	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_NEW_BUF	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI_AVAILABLE	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_NO_PLCI_DATA_B3	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI_DISCONNECT	10.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_RCV_BUFFER	10.2.23, 'VCAPI-Events'
MSG_VCAPI_PLCI_NOT_FOUND	10.2.23, 'VCAPI-Events'
MSG_VCAPI_RCV_LEN_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_RECEIVE_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_SERVER_ERROR	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_SOCK_NOT_AVAIL	10.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_BIND_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_NOT_OPEN	10.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_RCV_ERR	10.2.23, 'VCAPI-Events'
MSG_VCAPI_TOO_MANY_CLIENTS	10.2.23, 'VCAPI-Events'
MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNANTICIPATED_MESSAGE	10.2.24, 'VCAPI-Anwendungs-Events'

Event-Code	Abschnitt
MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE	10.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNKNOWN_MSG_N2H	10.2.23, 'VCAPI-Events'
MSG_VCAPI_UNKNOWN_NTFY	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_BUF_LEN	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_CONV_H2N	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_CONV_N2H	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_EVENT_CAPI	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_EVENT_SRV	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_LENGTH_MSG	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_LINKNUM	10.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_MSG_LENGTH	10.2.23, 'VCAPI-Events'
MSG_WEBSERVER_INTERNAL_ERROR	10.2.29, 'OAM-Events'
MSG_WEBSERVER_MAJOR_ERROR	10.2.3, 'Reboot-Events'
MSG_X25_ERROR	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X25_INFO	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X75_ERROR	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X75_INFO	10.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_XMLUTILS_ERROR	10.2.47, 'XMLUTILS-Events'
QDC_ERROR_IN_CLIENT	10.2.52, 'QDC-CGWA-Related Events'
QDC_ ERROR_IN_COMMON_CLIENT	10.2.51, 'Client-bezogene Events'
QDC_INVALID_CONFIGURATION	10.2.52, 'QDC-CGWA-Related Events'
QDC_MSG_QUEUE_ERROR	10.2.51, 'Client-bezogene Events'
QDC_PERSYSTENCY_ERROR	10.2.52, 'QDC-CGWA-Related Events'
QDC_SIGNALLING_DATA_ERROR	10.2.51, 'Client-bezogene Events'

Event-Code	Abschnitt
QDC_SYSTEM_ERROR	10.2.51, 'Client-bezogene Events'
QDC_VOIPSD_ERROR	10.2.53, 'QDC VoIPSD Error Report Events'
SENTA_NOK_UPGRADE_REG	10.2.2, 'Status-Events'
SIP_INFORMATION	10.2.54, 'SIP-Events'
SIP_INVALID_PARAMETER_VALUE	10.2.54, 'SIP-Events'
SIP_INVALID_POINTER	10.2.54, 'SIP-Events'
SIP_REBOOT	10.2.3, 'Reboot-Events'
SIP_UNEXPECTED_RETURN_VALUE	10.2.54, 'SIP-Events'

9.2.2 Status-Events

COMGA_NOK_UPGRADE_REG

Laden der COMGA-Firmware via HTTP

FW_NOK_UPGRADE_REG

Laden der Firmware

MSG_DLSC_BOOTSTRAP_OK

Das Bootstrapping des Deployment- und Licensing Server Clients war erfolgreich.

MSG_FIREWALL_ALARM

Alarm an der Firewall.

MSG_GW_SUCCESSFULLY_STARTED

`EventText: 11/21/2001 20:46:52`

Typ: **Information**

Das Gateway wurde zur angegebenen Zeit erfolgreich gestartet. Ein SNMP-Trap wird erzeugt.

MSG_IPNCV_STARTUP_ERROR

`EventText: IPNCV Startup: %s`

Typ: **groß**

IPNCV konnte nicht gestartet werden. Ein SNMP-Trap wird erzeugt. Erstellen Sie einen TR/MR.

MSG_IPNCV_STARTUP_SHUTDOWN

`EventText: IPNCV Start/Stop: %s`

Typ: **Information**

IPNCV wurde erfolgreich gestartet oder angehalten. Ein SNMP-Trap wird erzeugt.

MSG_IPNCV_INTERNAL_ERROR

`EventText: Internal IPNCV error: %s`

Typ: **Warning**

Software-Fehler: ungültige interne Daten entdeckt. Ein SNMP-Trap mit dem Profil IPNCV-Detailed wird erzeugt.

MSG_LDAP_SUCCESSFULLY_STARTED

`EventText: %s`

Typ: **Information**

LDAP wurde erfolgreich gestartet.

FP_EVT_INFORMATION

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Information**

Internes SW-Event – nur zur Information

FP_EVT_TRACE_STOP

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Information**

Trace-Stopp verfügbar

FP_EVT_TRACE_START

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Information**

Trace-Start verfügbar

FP_EVT_SNMP_TRAP

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Warning**

Important events with SNMP Trap Wichtige Events – SNMP-Trap wird erzeugt.

FP_EVT_MINOR

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **klein**

Interner SW-Fehler bei der Remote-Signalisierung

FP_EVT_INDETERMINATE

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Information**

Interner Software-Fehler bei Trace-Stopp und Remote-Signalisierung

MSG_PS_INVALID_STREAM_FROM_ADDRESS

Ungültige Daten von einer bestimmten Adresse.

MSG_PS_INVALID_STREAM_FROM_PORT

Ungültige Daten von einem bestimmten Port.

MSG_SIP_FM_MSG_INTERNAL_ERROR

`EventText: %p`

Typ: **groß**

Softwarefehler innerhalb von SIP_FM_MSG

MSG_SIP_FM_STARTUP_FAILURE

`EventText: SIP_FM startup failed: %s`

Typ: **groß**

Softwarefehler während SIP_FM-Start

MSG_SIP_FM_INTERNAL_ERROR

`EventText: %p`

Typ: **groß**

Softwarefehler innerhalb von SIP_FM

MSG_SIP_FM_MSG_NOT_PROCESSED

`EventText: SIP_FM received an illegal message: %d`

Typ: **groß**

SIP_FM konnte keine Erhalten-Meldung absetzen.

MSG_STRC_STOP

STRC gestoppt.

MSG_STRC_START

STRC gestartet.

MSG_HBR_WARNING

Warnung von HiPath Backup- und Restore.

SENTA_NOK_UPGRADE_REG

Laden der SENTA-Firmware via HTTP

9.2.3 Reboot-Events

MSG_CAT_H323_REBOOT

Der H.323-Stack-Adapter hat keine internen Ressourcen mehr und bewirkt einen Neustart. Der Neustart wird durchgeführt. Ein SNMP-Trap wird erzeugt.

MSG_CAT_HSA_REBOOT

```
EventText: HSA (Reboot) Q931 cmCallNew() failed:reaching
vtNodeCount limit
```

Typ: **Critical**

Der H.323-Stack-Adapter hat keine internen Ressourcen mehr und bewirkt einen Neustart. Der Neustart wird durchgeführt. Ein SNMP-Trap wird erzeugt. Fügen Sie dem Error-Report den Event-Log hinzu!

MSG_OSF_PCS_EXCEPTION

```
EventText: "%p"
```

Typ: **Critical**

Das OSF hat eine kritische Ausnahme registriert. Der Neustart wird jedoch ausgeführt.

MSG_OS_EXCEPTION_ERROR

Das OS hat eine kritische Ausnahme registriert. Der Neustart wird durchgeführt.

MSG_WEBSERVER_MAJOR_ERROR

```
EventText: %p
```

Typ: **groß**

Interner Fehler beim Webserver. Da weitere Aktivitäten des Webservers beeinflusst würden, wird ein Neustart erzwungen. Der Neustart wird durchgeführt.

MSG_ADMIN_REBOOT

Typ: **Information**

```
EventText: Reboot initiated by Admin
```

Ein vom Administrator erzwungener Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

```
EventText: Reboot initiated by Admin (SW Image Activation)
```

Ein vom Administrator durch Aufspielen eines neuen Software-Image erzwungener Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

```
EventText: Reboot initiated by Admin (SW Upgrade)
```

Ein vom Administrator durch Einspielen neuer Daten erzwungener Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_SYSTEM_REBOOT

```
EventText: Reboot initiated by Garbage Collection.
Available memory: xxxx
```

Typ: **Information**

Nach einer internen Speicherbereinigung wird ein notwendiger Neustart ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_EXCEPTION_REBOOT

```
EventText: Reboot initiated by VxWorks Task Exception
```

Typ: **Information**

Nach einem VxWorks-Task wird ein Neustart ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_RESTORE_CFG_REBOOT

```
EventText: Special reboot initiated by Admin (Backup
Service)
```

Typ: **Information**

Nach einer Datenwiederherstellung von HBS wird ein notwendiger Neustart ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_GW_OBJ_MEMORY_EXHAUSTED

```
EventText: Object memory has been exhausted. Last
allocation size: xxxx. Using failsafe areas to attempt a
graceful shutdown
```

Typ: **Critical**

Mögliche Speicherprobleme: es wurde zu viel Speicher reserviert, oder es ist nicht mehr genügend Speicher verfügbar. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_GW_OBJ_ALLOC_FAILED

```
EventText: Memory allocation in partition xxx failed. xxx
Error. Last allocation size: xxxx. Rebooting ...
```

Typ: **Critical**

Mögliche Speicherprobleme: es wurde zu viel Speicher reserviert, oder es ist nicht mehr genügend Speicher verfügbar. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_GW_OBJ_MEMORY_INCONSISTENT

```
EventText: Memory corruption in partition xxx XXX Error.
Invalid block address: xxxx. Rebooting ...
```

Typ: **Critical**

Mögliche Speicherprobleme: es wurde Speicher überschrieben, oder es wurde versucht, bereits freigegebenen Speicher nochmals freizugeben. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

ASSERTION_FAILED_EVENT

```
EventText: Assertion failed ...
```

Typ: **Information**

Internes Software-Kodierungsproblem. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt. Erstellen Sie einen TR/MR.

EXIT_REBOOT_EVENT

Typ: **Information**

```
EventText: Rebooting due to Exit Event ...
```

Internes Software-Kodierungsproblem. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt. Erstellen Sie einen TR/MR.

`EventText: cannot create task tV24CliI. ...`

Die Task-Erzeugung der V.24-CLI-Schnittstelle ist fehl geschlagen. Der erforderliche Neustart wird ausgeführt.

`EventText: internal error: not enough memory ...`

Die Reservierung von Speicher schlug fehl. Der erforderliche Neustart wird ausgeführt.

`EventText: CLI: read operation from STD_IN has failed ...`

Fehlerhafte Ein-/Ausgabe. Der erforderliche Neustart wird ausgeführt.

MSG_TLS_POOL_SIZE_EXCEEDED

`EventText: ?*?maximum number of elements exceeded`

Typ: **groß**

Internes Pool-Größen-Konfigurationsproblem. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt. Erstellen Sie einen TR/MR.

MSG_SSM_NUM_OF_CALL_LEGS_2BIG

`EventText: More than 2 call Legs: not supported! CSID: %x/ %x`

Typ: **groß**

Es sind nicht mehr als zwei Call-Legs pro Session möglich. Die Software ist dadurch in einen instabilen Zustand geraten. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_SSM_SESSION_CREATION_FAILED

`EventText: Session creation failed`

Typ: **groß**

Da keine Session erzeugt werden konnte, ist keine Signalisierung mehr möglich. Der erforderliche Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.

MSG_SNMP_TRAP_COLLECTOR_START_ERROR

`EventText: Trap collector could not be started:%n%s`

Typ: **Information**

Der Thread des Trap Collectors konnte nicht gestartet werden. Überprüfen Sie, ob der Trap-Port 162 bereits anderweitig verwendet wird.

MSG_PPP_STACK_REBOOT

Der Neustart wird durchgeführt.

MSG_PPTP_STACK_REBOOT

Der Neustart wird durchgeführt.

MSG_ASP_REBOOT

Der Neustart wird durchgeführt. Ein SNMP-Trap wird erzeugt.

MSG_DELIC_ERROR

Ein DELIC-Fehler ist aufgetreten. Der Neustart wird durchgeführt. Ein SNMP-Trap wird erzeugt.

MSG_IPSEC_REBOOT

Der Neustart wird durchgeführt.

FP_EVT_CRITICAL

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Critical**

Reboot wird durch einen Softwarefehler ausgelöst.

FP_EVT_MAJOR

`EventText: %x %c #%d/%d %x-%x %s#`

Typ: **groß**

Reboot, weil Resourcen erschöpft sind.

FP_EVT_WARNING

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Warning**

Reboot wurde über das Tool ausgelöst.

SIP_REBOOT

`EventText: InternalSetUserA`

Typ: **csevMajor**

Die Konfiguration des SIP-Stacks war fehlerhaft. Der Neustart wird durchgeführt.

MSG_MIKEY_REBOOT

Der Neustart wird durchgeführt.

9.2.4 Ressourcen-Überwachungs-Events

MSG_IP_LINK2_FAILURE

`EventText: IP Link [still] out of order`

Typ für diesen Log-Eintrag: **Warning**

Eine IP-Netzwerkverbindung ist nicht oder immer noch nicht möglich. Ein SNMP-Trap wird erzeugt. Überprüfen Sie die Steckerverbindungen und Kabel!

`EventText: IP Link no longer out of order`

Typ für diesen Log-Eintrag: **Cleared**

Die IP-Netzwerkverbindung ist wieder verfügbar. Ein SNMP-Trap wird erzeugt.

MSG_IP_LINK2_FAILURE

n/a

MSG_IP_LINK_RESTORE

n/a

MSG_IP_LINK2_RESTORE

n/a

MSG_IP_LINK_SWITCHOVER

n/a

MSG_IP_LINK2_SWITCHOVER

n/a

MSG_OAM_RAM_THRESHOLD_REACHED

```
EventText: High WaterMark "XXX" [still] reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Warning**

Die Systemspeichergrenze ist erreicht. Details sind in der Event-Meldung aufgelistet (Grenzwert, aktueller Wert und Auslastung in Prozent). Hohes Anrufaufkommen kann die mögliche Ursache sein. Ein SNMP-Trap wird erzeugt.

```
EventText: High WaterMark "XXX" no longer reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Cleared**

Das Problem mit der Systemspeichergrenze besteht nicht mehr. Ein niedrigeres Anrufaufkommen kann die Ursache für die geringere Speicherauslastung sein. Ein SNMP-Trap wird erzeugt.

MSG_OAM_DMA_RAM_THRESHOLD_REACHED

```
EventText: High WaterMark "XXX" [still] reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Warning**

Die DMA-Speichergrenze ist erreicht. Details sind in der Event-Meldung aufgelistet (Grenzwert, aktueller Wert und Auslastung in Prozent). Hohes Anrufaufkommen kann die mögliche Ursache sein. Ein SNMP-Trap wird erzeugt.

```
EventText: High WaterMark "XXX" no longer reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Cleared**

Das Problem mit der DMA-Speichergrenze besteht nicht mehr. Ein niedrigeres Anrufaufkommen kann die Ursache für die geringere Speicherauslastung sein. Ein SNMP-Trap wird erzeugt.

MSG_OAM_OVERLOAD_REACHED

n/a

MSG_OAM_OVERLOAD_CLEARED

n/a

MSG_OAM_THRESHOLD_REACHED

```
EventText: High/Low WaterMark "XXX" [still] reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Warning**

Ein Grenzwert (beim Flash-Speicher, bei der Speicherkapazität des Dateisystems oder bei den Netstack IP-Ressourcen) wurde erreicht. Details sind in der Event-Meldung aufgelistet (Grenzwert, aktueller Wert und Auslastung in Prozent). Ein SNMP-Trap wird erzeugt.

```
EventText: High/Low WaterMark "XXX" no longer reached:
           Configured: xxx Current: xxx
```

Typ für diesen Log-Eintrag: **Cleared**

Das Problem mit dem Grenzwert besteht nicht mehr. Ein SNMP-Trap wird erzeugt.

MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE

```
EventText: PSU or RPS [still] out of Service
```

Typ für diesen Log-Eintrag: **Warning**

Bei PSU oder RPS gibt es (immer noch) ein Problem. Ein SNMP-Trap wird erzeugt. Überprüfen Sie die PSU und RPS und tauschen Sie sie gegebenenfalls aus!

```
EventText: PSU or RPS no longer out of Service
```

Typ für diesen Log-Eintrag: **Cleared**

Das Problem mit PSU oder RPS besteht nicht mehr. Ein SNMP-Trap wird erzeugt.

MSG_OAM_FAN_OUT_OF_SERVICE

```
EventText: Fan [still] out of Service
```

Typ für diesen Log-Eintrag: **Warning**

Beim Lüfter gibt es (immer noch) ein Problem. Ein SNMP-Trap wird erzeugt. Überprüfen Sie den Lüfter und tauschen Sie ihn gegebenenfalls aus!

```
EventText: Fan no longer out of Service
```

Typ für diesen Log-Eintrag: **Cleared**

Das Problem mit dem Lüfter besteht nicht mehr. Ein SNMP-Trap wird erzeugt.

MSG_OAM_HIGH_TEMPERATURE_EXCEPTION

```
EventText: High WaterMark 'Temperature' reached:
Configured: xxx Current: xxx . Gateway stopped.
```

Typ: **Warning**

Ein ernsthaftes Temperatur-Problem ist aufgetreten. Das Gateway wurde angehalten. Überprüfen Sie die Umgebung und tauschen Sie gegebenenfalls Boards und/oder Lüfter aus.

MSG_CAR_MALLOC_FAILED

`EventText: Malloc failed`

Typ: **groß**

Die Reservierung von Speicher schlug fehl.

MSG_IPNCV_MEMORY_ERROR

`EventText: IPNCV Memory: %s`

Typ: **groß**

Speicherüberlauf. Ein SNMP-Trap wird erzeugt. Starten Sie das Gateway neu. Erstellen Sie einen TR/MR.

MSG_LDAP_IP_LINK_ERROR

`EventText: IP Link out of order`

Typ: **Warning**

Keine Netzwerk-IP-Verbindung.

MSG_LDAP_MEMORY_ERROR

`EventText: No Materna Buffer Available`

Typ: **groß**

Nicht genügend Speicher zum Senden/Empfangen einer Meldung.

MSG_LDAP_ENCODE_DECODE_ERROR

`EventText: Unable to Encode/Decode LDAP Msg`

Typ: **groß**

Die BER-Kodierung oder -Dekodierung einer LDAP-ASN.1-Meldung schlug fehl.

MSG_LDAP_SOCKET_ERROR

`EventText: LDAP Socket Failure`

Typ: **groß**

Bei den LDAP-Socket-Aufrufen ist ein Fehler aufgetreten.

MSG_LDAP_GENERAL_ERROR

`EventText: LDAP Returns General Error`

Typ: **Warning**

Bei den LDAP-Funktionsaufrufen ist ein Fehler aufgetreten.

MSG_HACKER_ON_SNMP_PORT_TRAP

`EventText: %s has tried to connect with TCP port 7161`

Typ: **Information**

Die angegebene IP-Adresse hat versucht, sich mit dem SNMP TCP-Port 7161 zu verbinden.

9.2.5 Routing-Events

MSG_CAT_NWRS

Typ: **Warning/Major**

Ungültige Daten für NPI- oder TON-Wert in einem ODR-Kommando. Das Kommando wird ignoriert. Diese Meldung kann auch auftreten, wenn ein Administrator ODR während des laufenden Betriebs auswechselt. Überprüfen Sie die ODR-Kommandos NPITYPE, TONTYPE (und CGNPITYPE, CGTONTYPE) auf plausible Werte!

MSG_NWRS_DPLN_ENTRY_INVALID

`EventText: Dial Plan Entry invalid: Dpln=#, DplnEntry=#member`

Typ: **klein**

Syntaxfehler beim Nummernplan: Andere Zeichen als `0123456789*#ANXZ-` sind nicht erlaubt. Verwenden Sie nur erlaubte Zeichen. Notieren Sie nicht mehrere Separatoren hintereinander, und keine Separatoren am Anfang und am Ende!

MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE

`EventText:` Dial Plan not found for Device #port

Typ: **groß**

Der angegebene Port ist keinem Rufnummernplan-Eintrag zugeordnet. Weisen Sie den angegebenen Port im Rufnummernplan zu, und erzeugen Sie wenn erforderlich zuvor einen neuen Rufnummernplan!

MSG_NWRS_EMPTY_FIELD_ECHOED

`EventText:` Empty field # echoed by Out Dial Rule #

Typ: **Warning**

Das Echo-Kommando einer Wahlregel für ausgehende Anrufe resultiert in einem leeren oder unplausiblen Teil-String. Überprüfen Sie den Ziffern-String des Rufnummernplan-Eintrags in Verbindung mit den Echo-Kommandos der Wahlregel für ausgehende Anrufe!

MSG_NWRS_UNKNOWN_FIELD_ECHOED

`EventText:` Unknown field # echoed by Out Dial Rule #

Typ: **klein**

Das Echo-Kommando einer Wahlregel für ausgehende Anrufe resultiert in einem unplausiblen Teil-String. Überprüfen Sie den Ziffern-String des Rufnummernplan-Eintrags in Verbindung mit den Echo-Kommandos der Wahlregel für ausgehende Anrufe!

MSG_NWRS_ODR_COMMAND_UNKNOWN

`EventText:` Unknown Command ...string in Out Dial Rule #

Typ: **klein**

Eine Wahlregel für ausgehende Anrufe enthält ein nicht erkennbares Kommando oder einen ungültigen Wert. Überprüfen Sie die Syntax der

Wahlregel nach Schlüsselwörtern und Separatorzeichen (â:â und â;â) sowie alle Konstanten und Grenzwerte!

MSG_NWRS_ODR_NOT_FOUND

`EventText:` Out Dial Rule # not found"

Typ: **Warning**

Ein Gateway enthält einen nicht auflösbaren Index bei den Wahlregeln für ausgehende Anrufe. Verwenden Sie eine bereits konfigurierte Wahlregel für ausgehende Anrufe oder erstellen Sie eine neue!

MSG_NWRS_DEVICE_NOT_FOUND

`EventText:` Device # port not found

Typ: **groß**

Einem Route-Mitglied ist ein ungültiger Port zugewiesen. Weisen Sie dem Route-Mitglied einen gültigen Ziel-Port zu!

MSG_NWRS_DEVICE_TABLE_NOT_FOUND

`EventText:` Device Table not found

Typ: **groß**

Es ist kein Port verfügbar. Versuchen Sie das Problem durch einen Hardware-Neustart zu beheben!

MSG_NWRS_ROUTE_NOT_FOUND

`EventText:` Route # not found

Typ: **groß**

Ein Mitglied des Rufnummernplans enthält eine nicht auflösbare Route-Nummer. Verwenden Sie eine bereits konfigurierte Route, oder erstellen Sie eine neue!

MSG_NWRS_DPLN_NOT_FOUND

`EventText:` Dial Plan not found: Dpln %I

Typ: **groß**

Ein Rufnummernplan mit der angegebenen ID konnte nicht gefunden werden.

MSG_NWRS_UNSPEC_ERROR

`EventText:` %p

Typ: **groß**

Inkonsistenter Software-Zustand, z. B. durch ungültige Daten.

9.2.6 Anrufkontroll- und Leistungsmerkmal-Events

MSG_SDR_INIT

`EventText:` SDR init %p

Typ: **groß**

SDR konnte nicht gestartet werden (keine Dateien). Während der Initialisierungt von SDR ist ein Fehler aufgetreten.

MSG_SDR_UNEXPECTED_EVENT

`EventText:` SDR: Unexpected event %n%M%n in state %s%n from %s - EXCEP: %n%e

Typ: **Warning**

Unerwartete oder nicht registrierte Meldung.

MSG_SNCP_UNANTICIPATED_MESSAGE

`EventText:` SCN Payload: Unanticipated Message %s in state %s - EXCEP: %n%e

Typ: **Warning**

Eine unbekannte Meldung wurde empfangen.

MSG_SNCP_DEVICE_ID_MISSING

`EventText:` SCN Payload: Mandatory field device ID missing in message 0x %X - EXCEP: %n%e

Typ: **groß**

In der angegebenen Nachricht fehlt das Pflichtfeld für die Device-ID, das zum Erstellen der Ressource-ID erforderlich ist.

MSG_SNCP_CHANNEL_ID_MISSING

`EventText:` SCN Payload: Mandatory field device ID missing in message 0x %X - EXCEP: %n%e

Typ: **groß**

In der angegebenen Nachricht fehlt das Pflichtfeld für die Channel-ID, das zum Erstellen der Resource-ID erforderlich ist.

MSG_SNCP_NO_RESOURCE_ID

`EventText:` SCN Payload: No resource ID available in message 0x%X - EXCEP: %n%e

Typ: **groß**

In der angegebenen Nachricht ist keine Resource-ID vorhanden.

MSG_SNCP_COULD_NOT_DELETE_OBJECT

`EventText:` SCN Payload: Could not delete SCN Payload Object - EXCEP: %n%e

Typ: **groß**

SCN-Payload-Objekt konnte nicht gelöscht werden.

MSG_SNCP_COULD_NOT_CREATE_OBJECT

`EventText:` SCN Payload: Could not delete SCN Payload Object - EXCEP: %n%e

Typ: **groß**

SCN-Payload-Objekt konnte nicht gelöscht werden.

MSG_SNCP_COULD_NOT_SET_FORW_ENC

`EventText:` SCN Payload: Could not set forward encoding to %I for CSID: (%s) and ResID: (%u) - EXCEP: %n%e

Typ: **groß**

Die Weiterleitungs-Kodierung für die war nicht möglich.

MSG_SNCP_COULD_NOT_SET_REV_ENC

`EventText:` SCN Payload: Could not set reverse encoding to %I for CSID: (%s) and ResID: (%u) - EXCEP: %n%e

Typ: **groß**

Die Zurückleitungs-Kodierung war nicht möglich.

MSG_SNCP_NEITHER_ENC_COULD_BE_SET

`EventText:` SCN Payload: Neither encoding could be set for CSID: (%s) and ResID: (%u) - EXCEP: %n%e

Typ: **groß**

Es war keine Kodierung möglich.

MSG_SNCP_ADD_OBJECT_FAILED

`EventText:` SCN Payload: Could not add SCN Payload Object - EXCEP: %n %e

Typ: **groß**

Es konnte kein SCN-Payload-Objekt hinzugefügt werden.

MSG_SNCP_ERROR

`EventText:` SNCP Error: %p

Typ: **Warning/Major**

Inkonsistenter Software-Zustand in der SNCP-Komponente.

MSG_SPL_SESSION_NOT_FOUND

`EventText:` No session for Session Payload Object found using CSID: %u) - EXCEP: %n%e

Typ: **groß**

Es konnte kein Session-Objekt gefunden werden.

MSG_SPL_ADD_OBJECT_FAILED

`EventText:` Session Payload: Object could not be added - EXCEP: %n%e

Typ: **groß**

Es konnte kein Objekt hinzugefügt werden.

MSG_SPL_MISSING_CS_ID

`EventText:` Session Payload: Missing Call and Session ID - EXCEP: %n%e

Typ: **groß**

Anruf- und Session-ID fehlen.

MSG_SPL_UNANTICIPATED_MESSAGE

`EventText:` Session Payload: Unanticipated Message %s in state %s - EXCEP: %n%e

Typ: **Warning**

Unvorhergesehene Meldung.

MSG_SPL_ERROR

`EventText: SPL Error: %p`

Typ: **Warning/Major**

Inkonsistenter Software-Zustand in der SPL-Komponente.

MSG_SPL_FMSEM_ERROR

`EventText: FMSEM Error: %p`

Typ: **Warning/Major**

Inkonsistenter Software-Zustand in der FMSEM-Komponente, die Teil von SPL ist.

MSG_SSM_NO_CSID

`EventText:` Msg doesnât contain a CSID !

Typ: **groß**

Anruf- und Session-ID fehlen.

MSG_SSM_INVALID_PARAM

`EventText:` Invalid parameter %s, value %x

Typ: **groß**

Ein Parameter enthielt einen ungültigen Wert.

MSG_SSM_UNSPEC_ERROR

`EventText:` %p

Typ: **groß**

Inkonsistenter Software-Zustand, z. B. durch ungültige Daten.

MSG_SSM_BAD_NWRS_RESULT

`EventText:` Bad result from NWRS

Typ: **groß**

Vermutliche Ursache ist eine Protokoll-Schleife. Überprüfen Sie die Konfiguration der Route von der Signalquelle zum Ziel!

MSG_MAND_PARAM_MISSING

`EventText:` Mandatory parameter %s for construction of message missing

Typ: **groß**

Eine CCP-Meldung konnte nicht aus der Meldungs-Basis erstellt werden, weil ein Pflichtparameter fehlte.

9.2.7 SCN-Protokoll-Events

MSG_ISDN_CMR_INIT_FAILED

`EventText: Initialization for protocol manager failed. %p`

Typ: **Warning**

Die Initialisierung des Protokoll-Managers schlug fehl.

MSG_ISDN_CMR_MAND_FIELDS_MISSING

`EventText: %pMandatory fields missing (ID %s)`

Typ: **Warning**

In der Meldung fehlen Pflichtfelder.

MSG_ISDN_CMR_OBJECT_NOT_FOUND

`EventText: %pThe object for Call and Session ID %s could not be found`

Typ: **Critical**

Das Session-Objekt eines Verbindungssegments konnte nicht gefunden werden.

MSG_ISDN_CMR_UNIMPLEMENTED

`EventText: %pUnimplemented feature%s`

Typ: **Warning**

Das angeforderte Leistungsmerkmal ist nicht implementiert.

MSG_ISDN_CMR_TIMER_EXPIRED

`EventText: %pTimer %S expired in state %S`

Typ: **Information**

Ein Timer ist abgelaufen.

MSG_ISDN_CMR_WRONG_DEVICE_TYPE

`EventText: %p%Device Id %I is not a valid device type`

Typ: **Warning**

Ein angegebener Device-Typ ist ungültig.

MSG_ISDN_CMR_MSG_DECODE_FAILED

`EventText: %pEvent decoding failed. %s %s %nEvent data: %b`

Typ: **Warning**

Das Dekodieren einer Nachricht schlug fehl.

MSG_ISDN_CMR_NEW_OBJECT_FAILED

`EventText: %pThe object for this Call and Session ID could not be created`

Typ: **Critical**

Das Erzeugen eines Session-Objekts für ein Verbindungssegment schlug fehl.

MSG_ISDN_CMR_ADD_OBJECT_FAILED

`EventText: %pThe object created for this Call and Session ID could not be added to the manager`

Typ: **Critical**

Ein Verbindungssegment-Objekt konnte nicht mit dem Protokoll-Manager verknüpft werden.

MSG_ISDN_CMR_UNEXPECTED_EVENT

`EventText: %pReceived unexpected event Message ID: %s`

Typ: **Information**

Ein unerwarteter Event wurde empfangen.

MSG_ISDN_CMR_SESSION_NOT_FOUND

`EventText: %pThe session object for this Call and Session ID could not be found by the manager`

Typ: **Critical**

Das Session-Objekt zum Verbindungssegment wurde nicht gefunden.

MSG_ISDN_CMR_STATUS_MSG_RECEIVED

`EventText: %pL3 Status message received in state %s`

Typ: **Information**

Eine Statusmeldung wurde empfangen.

MSG_ISDN_CMR_WRONG_PROTVAR

`EventText: %pProtocol Variant %I, Key %x is not valid. Using default Timer Values !`

Typ: **Critical**

Eine Protokollvariante ist ungültig.

MSG_ISDN_CMR_GENRIC_EVENT

`EventText: %p`

Typ: **Information**

Ein allgemeines Ereignis.

MSG_ISDN_RESOURCE_NOT_IN_SERVICE

`EventText: %pResource not in service, Resource State %s`

Typ: **Information**

Falscher Ressourcen-Status: die Ressource gibt es nicht im Dienst.

MSG_ISDN_RESOURCE_NOT_AVAILABLE

`EventText: %pResource not available, Resource State %s`

Typ: **Information**

Die Ressource ist nicht verfügbar.

MSG_ISDN_RESOURCE_IN_USE_BY_O_CALL

`EventText: %pResource in use by other call. Resource not released, Resource State %s`

Typ: **Information**

Die Ressource ist von einem anderen Anruf reserviert (Anruf-Kollision).

MSG_ISDN_DEVICE_PTR_NOT_FOUND

`EventText: %pThe device ID could not be found`

Typ: **Warning**

Das Device-Objekt konnte nicht gefunden werden.

MSG_ISDN_CMR_DEVICE_PTR_BAD

`EventText: %pNull device pointer`

Typ: **Critical**

Der Zeiger auf ein Device-Objekt zeigt auf NULL.

MSG_ISDN_CMR_MSG_ENCODE_FAILED

`EventText: %pEvent encoding failed. %s %s %nEvent data: %b`

Typ: **Warning**

Das Kodieren der Meldung schlug fehl.

MSG_ISDN_CMR_MSG_SEND_FAILED

`EventText: %pL3 Message sending failed`

Typ: **Critical**

Das Kodieren der Meldung schlug fehl.

MSG_ISDN_CMR_SEG_MSG_ERROR

`EventText: %pSegmented message error`

Typ: **klein**

Fehler bei segmentierter Nachricht.

MSG_ISDN_CMR_UNEXPECTED_ERROR

`EventText: %pUnexpected error`

Typ: **klein**

Ein unerwarteter Fehler trat auf.

MSG_ISDN_CMR_UNEXPECTED_VALUE

`EventText: %pUnexpected value for this Device ID`

Typ: **Warning**

Unerwarteter Wert für Device-ID.

MSG_ISDN_CMR_MSG_UNEXPECTED

`EventText: %pUnexpected event`

Typ: **Warning**

Die Meldung war innerhalb des aktuellen Status unterwartet.

MSG_ISDN_CMR_GEN_CALL_REF_FAILED

`EventText: %pCould not generate a Call Reference`

Typ: **Critical**

Das Generieren einer Anruf-Referenz schlug fehl.

MSG_ISDN_CMR_WRONG_INTERFACE

`EventText: %pWrong interface type %s`

Typ: **Critical**

Falscher Schnittstellentyp.

MSG_ISDN_CMR_UNH_STATE_EVENT

`EventText: %pUnhandled event`

Typ: **Warning**

Das Ereignis wurde nicht im passenden Anrufstatus verarbeitet.

MSG_ISDN_NULL_PTR

`EventText: %p%p`

Typ: **Critical**

Es wurde versucht, einen Zeiger auf NULL zu verwenden.

MSG_ISDN_ERROR

`EventText: %pError: %p`

Typ: **klein**

ISDN-Fehler.

MSG_ISDN_NO_ERROR

`EventText: %pNo Error`

Typ: **Information**

Kein ISDN-Fehler.

MSG_ISDN_CMR_PROTOCOL_ERROR

`EventText: Protocol error: Device ID %d`

Typ: **Warning**

Die Meldung entsprach nicht dem gegenwärtigen Protokoll.

MSG_ISDN_CMR_MESSAGE_ERROR

`EventText: Message Error 0x%X`

Typ: **klein**

Die Meldung ist fehlerhaft.

MSG_ISDN_START_UP_ERROR

`EventText: %s: Start up error. %p`

Typ: **Critical**

Beim Startvorgang des ISDN-Protokolls trat ein Fehler auf.

MSG_ISDN_START_UP

`EventText: %s: Start up OK. %p`

Typ: **Information**

Der ISDN-Startvorgang ist abgeschlossen.

MSG_ISDN_OVERLOAD_CONDITION

`EventText: %pOverload Condition. SETUP received, RELEASE COMPLETE sent`

Typ: **Information**

Überlastung erreicht: Anruf gelöscht.

9.2.8 H.323-Events

H323_NO_IP

n/a

H323_SNMP_TRAP

n/a

MSG_H323_MISSING_PARAMETER

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

In einer Meldung, die an eine H.323-Komponente gesendet wurde, fehlt ein Parameter. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_INVALID_PARAMETER_VALUE

`EventText: ...`

Typen: **Major, Minor, Warning**

Ein Parameterwert ist außerhalb des festgelegten Wertebereichs. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_INVALID_CONFIGURATION

`EventText: ...`

Typen: **Major, Warning**

Die H.323-Konfiguration ist fehlerhaft. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log sowie die Konfigurationsdaten des Gateways hinzu!

MSG_H323_UNEXPECTED_RETURN_VALUE

`EventText: ...`

Typen: **Major, Minor, Warning**

Der aktuell aufgerufene Funktion gibt ein unerwartetes Ergebnis zurück. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_INVALID_POINTER

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

Ein Zeiger enthält einen ungültigen Wert. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_INFORMATION

`EventText: ...`

Typ: **Information**

Diese Meldung dient nur zu Ihrer Information.

MSG_H323_UNEXPECTED_MESSAGE

`EventText: ...`

Typen: **Major, Minor, Warning**

Das H.323-Protokoll hat eine unerwartete Meldung erhalten. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_LOGIC_ERROR

`EventText: ...`

Typen: **Major, Warning, Information**

Beim Verarbeiten einer Meldung wurde ein logischer Fehler bemerkt. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_STACK_ERROR

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

Bei einer H.323-Stack-Operation trat ein Fehler auf. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_PROTOCOL_ERROR

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

Eine Protokoll-Information fehlt oder ist fehlerhaft. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_OSCAR_NSD_ERROR

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

Dies ist ein Fehler, der sich auf nicht standard-gerechte Daten bezieht. Aktivieren Sie ein geeignetes H.323-Analyse-Trace-Profil und fügen Sie dem Fehler-Report Trace- und Event-Log hinzu!

MSG_H323_SNMP_TRAP

`EventText: ...`

Typen: **Major, Minor, Warning, Information**

Dieser Event meldet eine Situation, die für den Service-Techniker von Bedeutung ist. Der Service sollte je nach Event-Text entsprechende Maßnahmen ergreifen (z. B. einen Netzwerk-Check durchführen).

9.2.9 H.235-Events

MSG_CAT_H235

`EventText: H.235...`

Typen: **Major, Warning, Information**

Events, die sich auf H.235-Sicherheitsaspekte beziehen. Die H.235-Konfiguration in Gateway, Gatekeeper und bei Clients sollte verifiziert werden.

9.2.10 RTPQM-Events

MSG_IP_RTP_QUALITY_FAILURE

`EventText: ...`

Typ für diesen Log-Eintrag: **groß**

Die LAN-Qualität zur angegebenen Ziel-IP-Adresse wird als 'zu schlecht für Sprachübertragung' eingestuft. Dadurch werden alle weiteren Anrufe zu diesem Tiel über das Leitungsnetz geroutet. Anrufversuche für dieses Ziel werden vom Gateway zurückgewiesen. Überprüfen Sie die 'Packet-Loss'-Einstellung für IP-Verkehr zu dieser IP-Adresse!

`EventText: ...`

Typ für diesen Log-Eintrag: **Cleared**

Die Zeit für die Zurückweisung von LAN-Anrufen für die angegebene IP-Zieladresse ist abgelaufen. LAN-Anrufe zu der Zieladresse sind wieder möglich.

MSG_IP_RTP_QUALITY_WARNING

`EventText: ...`

Typ: **groß**

Dies ist eine Warnung, dass die LAN-Qualität sinkt. Es kann passieren, dass die Route zu der angegebenen Zieladresse in Kürze blockiert wird. Überprüfen Sie die 'Packet-Loss'-Einstellung für IP-Verkehr zu dieser IP-Adresse!

9.2.11 GSA-Events

MSG_GSA_SNMP

`EventText: %p`

Typ: **Critical**

Kritischer Fehler für GSA, der einen SNMP-Trap generiert.

9.2.12 DGW-Events

MSG_BSD44_VCAPI_NO_LIST

`EventText: No listening socket for VCAPI`

Typ: **groß**

Es ist nicht möglich, einen wartenden Socket für VCAPI zu erzeugen. Es ist kein LAN-Verkehr möglich.

MSG_BSD44_DGW_NO_LIST

`EventText: No listening socket for DATA-GW`

Typ: **groß**

Es ist nicht möglich, einen wartenden Socket für DATAGWI zu erzeugen. Es ist kein LAN-Verkehr möglich.

MSG_BSD44_ACCEPT_DGW_ERR

`EventText: accept error for DATAGW Dispatcher`

Typ: **groß**

Es ist nicht möglich, eine neue Verbindung für DATAGW herzustellen.

MSG_BSD44_DGW_SOCKET_FAIL

`EventText: DGW socket() failed`

Typ: **klein**

Ein Client kann keinen Socket empfangen.

MSG_BSD44_DGW_BIND_FAIL

`EventText: DGW bind() failed`

Typ: **klein**

Ein Client kann keinen Socket binden.

MSG_BSD44_DGW_CONNECT_FAIL

`EventText: DGW connect() failed`

Typ: **klein**

Ein Client kann keine Verbindungt zum Server herstellen.

MSG_DGW_CONN_OUT_OF_RANGE

`EventText: dg_capi_HandleCapi20Msg: connection_id=%d out of range!`

Typ: **klein**

Die Verbindungs-ID hat die maximal erlaubte Anzahl von Kanälen überschritten.

MSG_DGW_WRONG_STATE

`EventText: dg_capi_HandleCapi20Msg: id=%d wrong state!`

Typ: **klein**

Falscher Status für den DATAGW-Dispatcher.

MSG_DGW_MSG_IGNORED

`EventText: %s from CAPI_PAYLOAD_IF ignored!`

Typ: **klein**

Meldung ignoriert, da sich der DGW-Dispatcher im falschen Status befindet.

MSG_DGW_CONN_B3_ACT_IND

`EventText: ALLOC error: no more buffers`

Typ: **groß**

Es konnte kein Speicher reserviert werden, um die Meldung CONNECT_B3_ACTIVE_RESPONSE zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_DISC_B3_IND

`EventText: CAPI2_DISCONNECTB3_IND dreadful!: no more buffers`

Typ: **groß**

Es konnte kein Speicher reserviert werden, um die Meldung DGW_CLOSE_REQ zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_ALLOC_DISC_B3

`EventText: CAPI2_DISCONNECTB3_IND(2) dreadful!: no more buffers`

Typ: **groß**

Es konnte kein Speicher reserviert werden, um die Meldung DGW_FREE_REQ zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_UNHANDLED_MSG

`EventText: unhandled %s msg=%d from CAPI_PAYLOAD_IF`

Typ: **groß**

Unbekannte Meldung von CAPI_PAYLOAD_IF an DGW-Dispatcher.

MSG_DGW_DATA_B3_ALLOC_ERR

`EventText: DATAB3_REQ:ALLOC ERROR: returncode %x`

Typ: **groß**

Es konnte kein Speicher reserviert werden, um die Meldung CMT_DATA_REQ an CAPI_PAYLOAD_IF zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_ALLOC_REQ_ERR

`EventText: DDGW_ALLOC_REQ received in wrong state!`

Typ: **klein**

Der DGW-Dispatcher berfindet sich beim Empfang von DGW_ALLOC_REQ im falschen Zustand.

MSG_DGW_ALLOC_CONF_ERR

`EventText: DGW_ALLOC_CONF id=%d received in wrong state!`

Typ: **klein**

Der DGW-Dispatcher befindet sich beim Empfang von DGW_ALLOC_CONF im falschen Zustand.

MSG_DGW_FREE_ALLOC_ERR

`EventText: DGW_FREE_REQ: allocb failed!`

Typ: **groß**

Es konnte kein Speicher reserviert werden, um die Meldung DISCONNECT_B3_REQ zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_UNKNOWN_PRIMITIVE

`EventText: unknown capi primitive: %x`

Typ: **groß**

Unbekannte Meldung von CAPI_PAYLOAD_IF an DGW-Dispatcher.

MSG_DGW_RECEIVE_ERR

`EventText: Error while receiving message for DATAGW Dispatcher:returncode %x`

Typ: **groß**

Empfangsfehler.

MSG_DGW_UNHANDLED_EVENT

`EventText: Unhandled event for DGW-Dispatcher,received event:%D`

Typ: **Warning**

Der DGW-Dispatcher hat einen nicht verarbeiteten Event empfangen.

MSG_DGW_WRONG_EVENT_CAPI20

`EventText: wrong eventcode from CAPI20-Mgr`

Typ: **Warning**

Vom CAPI20-Manager wurde ein fehlerhafter Event-Code empfangen.

MSG_DGW_NO_PLCI

`EventText: Find connection ID by PLCI:PLCI %d not found`

Typ: **Warning**

Wegen fehlerhaftem PLCI ist es nicht möglich, die Verbindungs-ID zu finden.

MSG_DGW_IND_ALLOC_ERR

`EventText: Not possible to allocate a buffer for CMT_DATA_IND`

Typ: **groß**

Es kann kein Speicher für CMT_DATA_IND reserviert werden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_CONF_ALLOC_ERR

`EventText: Not possible to allocate a buffer for CMT_DATA_CONF`

Typ: **groß**

Es kann kein Speicher für CMT_DATA_CONF reserviert werden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_WRONG_EVENT_CAPI

`EventText: wrong eventcode from CAPI_PAYLOAD_INTERFACE`

Typ: **Warning**

Fehlerhafter Event-Code von CAPI_PAYLOAD_INTERFACE.

MSG_DGW_ALLOC_CHN_RUN_OUT

`EventText: ALLOC_CHANNEL_REQ: run out of connection handles`

Typ: **klein**

Zu viele Verbindungen.

MSG_DGW_ALLOC_CHN_CONN_FAIL

`EventText: ALLOC_CHANNEL_REQ:connect failed`

Typ: **groß**

Es konnte keine neue Verbindung zum Server hergestellt werden.

MSG_DGW_OPEN_CHN_UNKNOWN_ID

`EventText: AOPEN_CHANNEL_REQ: unknown id`

Typ: **klein**

Über die Channel-ID konnte die Verbindungs-ID nicht gefunden werden.

MSG_DGW_OPEN_CHN_WRONG

`EventText: OPEN_CHANNEL_REQ:dreadful!: wrong state`

Typ: **klein**

Falscher Zustand für die Meldung OPEN_CHANNEL_REQ.

MSG_DGW_OPEN_CHN_ALLOC_FAIL

`EventText: OPEN_CHANNEL_REQ:Alloc failed`

Typ: **groß**

Für DGW_OPEN_CONFIRM konnte kein Speicher reserviert werden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_FREE_UNKNOWN_ID

`EventText: FREE_CHANNEL_REQ : unknown connection_id`

Typ: **groß**

FREE_CHANNEL_REQ mit falscher ID.

MSG_DGW_FREE_CHN_ALLOC_FAIL

`EventText: FREE_CHANNEL_REQ : Alloc failed`

Typ: **groß**

Für FREE_CHANNEL_REQ konnte kein Speicher reserviert werden. DISCONNECT_B3_REQ konnte nicht gesendet werden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_SEC_ALLOC_FAIL

`EventText: FREE_CHANNEL_REQ : second Alloc failed`

Typ: **groß**

Ein zweiter Versuch, für FREE_CHANNEL_REQ Speicher zu reservieren, schlug fehl. DGW_FREE_REQ konnte nicht gesendet werden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_UNH_MSG_CAPI20_MGR

`EventText: unhandled message %d from CAPI20-Mgr`

Typ: **Warning**

Unbekannte Meldung vom CAPI2.0-Manager.

MSG_DGW_UNKNOWN_ID_CHANNEL

`EventText: find_conn_id_by_chn_id: unknown id %d`

Typ: **klein**

Über die Channel-ID kann die Verbindungs-ID nicht gefunden werden.

MSG_DGW_FREE_NOT_SEND

`EventText: Zuordnungsfehler: DGW_FREE_REQUEST not sent`

Typ: **groß**

Zuordnungsfehler: DGW_FREE_REQUEST nicht gesendet. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_DISC_B3_NOT_SEND

`EventText: Zuordnungsfehler: DISCONNECT_B3_REQUEST not sent`

Typ: **groß**

Zuordnungsfehler: DISCONNECT_B3_REQUEST nicht gesendet. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_SOCKET_UNKNOWN

`EventText: SO_NTFY_CONN_COMPLETE: unknown socket!`

Typ: **klein**

SO_NTFY_CONN_COMPLETE: unbekannter Socket. Die Verbindung wird geschlossen.

MSG_DGW_CONNECT_FAILED

`EventText: SO_NTFY_CONN_COMPLETE: error! ret= %d!`

Typ: **groß**

SO_NTFY_CONN_COMPLETE: Verbindungsfehler.

MSG_DGW_CONN_COMPL_ALLOC

`EventText: SO_NTFY_CONN_COMPLETE: Alloc failed`

Typ: **groß**

Keiner Speicher-Reservierungsanfrage an die entfernte Stelle.

MSG_DGW_CONN_RUN_OUT

`EventText: SO_NTFY_CONNECTION: run out of connection handles:cnt=%d`

Typ: **Warning**

Zu viele Verbindungen.

MSG_DGW_MGR_NOT_READY

`EventText: SO_NTFY_CONNECTION: CAPI20Mgr not ready:DGW_Disp_State=0x%x`

Typ: **Warning**

SO_NTFY_CONNECTION: CAPI2.0-Manager nicht bereit. Start-Operations-Meldung von CAPI2.0-Manager nicht empfangen.

MSG_DGW_BUFAVAIL_SOCK_UNKN

`EventText: SO_NTFY_BUFAVAIL: unknown socket`

Typ: **klein**

Senden nicht möglich wegen unbekanntem Socket.

MSG_DGW_RCV_SOCK_UNKN

`EventText: SO_NTFY_RCV_SDATA: unknown socket`

Typ: **klein**

Daten können nicht empfangen werden wegen unbekanntem Socket.

MSG_DGW_ABORT_SOCK_UNKN

`EventText: SO_NTFY_ABORT: unknown socket`

Typ: **klein**

Verbindung kann nicht geschlossen werden wegen unbekanntem Socket.

MSG_DGW_UNKNOWN_NOTIFIC

`EventText: Unknown notification 0x%x`

Typ: **klein**

Unbekannte Benachrichtigung.

MSG_DGW_RCV_FAILED

`EventText: recv() failed, id=%d`

Typ: **klein**

Daten werden nicht ordnungsgemäß empfangen.

MSG_DGW_INV_MSG_LEN

`EventText: invalid message length: %d`

Typ: **klein**

Meldung mit falscher Länge von entfernter Stelle empfangen.

MSG_DGW_RCV_ALLOC_FAIL

`EventText: FATAL: allocb() failed, id=%d`

Typ: **groß**

Es ist nicht möglich, Speicher für den Empfangspuffer zu reservieren.

MSG_DGW_MSG_RCV_FAIL

`EventText: recv() failed, id=%d`

Typ: **klein**

Es ist nicht möglich, eine Meldung zu empfangen.

MSG_DGW_INVALID_LENGTH

`EventText: invalid lenght:%d %s`

Typ: **klein**

Falsche Länge von entfernter Stelle empfangen.

MSG_DGW_INV_DATA_LEN

`EventText: invalid data lenght:%d`

Typ: **klein**

Falsche Datenlänge von entfernter Stelle empfangen.

MSG_DGW_SEND_FAILED

`EventText: send() failed, id=%d`

Typ: **klein**

Es ist nicht möglich, eine Meldung an die entfernte Stelle zu senden.

MSG_DGW_SEND_DATA_ERR

`EventText: send() data failed, id=%d`

Typ: **klein**

Es ist nicht möglich, Daten an die entfernte Stelle zu senden.

MSG_DGW_SOCKET_NOT_OPEN

`EventText: DGW socket not opened`

Typ: **groß**

DGW-Socket wurde nicht geöffnet. Es sind keine Verbindungen möglich.

MSG_DGW_SOCKET_BIND_ERR

`EventText: bind error for DGW socket %d`

Typ: **groß**

Bindungs-Fehler bei DGW-Socket. Es sind keine Verbindungen möglich.

MSG_DGW_LISTENING_ERR

`EventText: listening error for DGW socket %d`

Typ: **groß**

Listening-Fehler bei DGW-Socket. Es sind keine Verbindungen möglich.

MSG_DGW_ACCEPT_FAILED

`EventText: so_accept() failed`

Typ: **klein**

Es werden keine neuen Verbindungen akzeptiert.

9.2.13 CAR-Events

MSG_CAR_GENERAL_ERROR

`EventText: CAR : General error : %s`

Typ: **klein**

Im Subsystem CAR trat ein allgemeiner Fehler auf.

MSG_CAR_NO_MEMORY

`EventText: CAR : no more memory available`

Typ: **klein**

`EventText:` CAR: there is no more memory available.

MSG_CAR_FKT_GET_IPADR_FAILED

`EventText: CAR : car_fkt_get_ipadr result unsuccessful due to lack of memory (mat_allocb)`

Typ: **klein**

Die Funktion `Car_fkt_get_ipadr` gibt ein erfolgloses Ergebnis zurück, was dazu führt, dass `mat_allocb` keinen Speicher mehr reservieren kann.

MSG_CAR_START_TCP_LISTENER_FAILED

`EventText: CAR : SOH : start of TCP listener failed : returncode soh_api_start_tcp_listener = %d`

Typ: **Critical**

Die Funktion `soh_api_send_tcp_listener` gibt einen ungültigen Wert zurück. Der TCP-Listener konnte nicht gestartet werden.

MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_SOH_ERROR

`EventText: CAR : SOH : sending update request failed : returncode soh_api_send_tcp_data = %d`

Typ: **Critical**

Die Funktion `soh_api_send_tcp_listener` gibt einen ungültigen Wert zurück. Das Senden des Update-Requests schlug fehl.

MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_NO_MEMORY

`EventText: CAR : SOH : Start update failed due to lack of memory`

Typ: **klein**

CAR: SOH: Das Senden des Update-Requests schlug aufgrund von Speichermangel fehl.

MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CALLADDRTAB_TOO_BIG

`EventText: CAR : SOH : update data : number of CallAddressEntries = %d too big`

Typ: **klein**

CAR: SOH: Die Anzahl der Einträge, die vom Update empfangen wurde, ist zu groß. Möglicherweise ein SOH-Fehler.

MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS

`EventText: CAR : SOH : received message is not from the Venus server. Received IP address = 0x%x`

Typ: **groß**

CAR: SOH: Die empfangene Meldung stammt nicht vom Venus-Server.

MSG_CAR_DB_READ_NODE_TABLE_ERROR

`EventText: CAR : DB : Read of Node Table failed : table index = %d`

Typ: **groß**

CAR: DB: Das Lesen der Knoten-Tabelle schlug fehl.

MSG_CAR_ALIVE_IP_CONNECTION_LOST

`EventText: CAR : Alive : ip connection %d.%d.%d.%d lost`

Typ: **groß**

`EventText:` CAR: Aktiv: IP-Verbindung verloren.

MSG_CAR_ALIVE_IP_CONNECTION_LOST

`EventText: CAR : Alive : ip connection %d.%d.%d.%d lost`

Typ: **groß**

CAR: Aktiv: IP-Verbindung verloren.

MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN

`EventText: CAR: Alive : ip connection %d.%d.%d.%d ok again`

Typ: **Information**

CAR: Aktiv: IP-Verbindung wieder in Ordnung.

MSG_CAR_ERROR_WITH_OAM_INTERFACE

`EventText: CAR : An error occurred with the OAM interface RC = %d`

Typ: **klein**

CAR: Bei der OAM-Schnittstelle trat ein Fehler auf.

MSG_CAR_NO_FREE_CODEC_TAB_ELE

`EventText: No free table element for CODECs found`

Typ: **klein**

Kein freies Tabellenelement für CODECs gefunden.

MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB

`EventText: Cannot arrange node table %d`

Typ: **groß**

Knotentabelle kann nicht angeordnet werden.

MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS

`EventText: Cannot sort MAC addresses %s`

Typ: **klein**

MAC-Adressen können nicht sortiert werden.

MSG_CAR_CODECS_INCONSISTENT

`EventText: HSA CODEC tables inconsistent %s`

Typ: **groß**

Die HSA-CODEC-Tabellen sind inkonsistent.

MSG_CAR_WRONG_NODE_ID

`EventText: Wrong node id %d`

Typ: **groß**

Falsche Knotenidentifikation.

MSG_CAR_WRONG_SERVICE

`EventText: Wrong service %d`

Typ: **klein**

Falscher Service.

MSG_CAR_NODE_INFO_ALREADY_AVAILABLE

`EventText: Node info already available for %d`

Typ: **klein**

Die Knoteninformationen für den angegebenen Knoten sind bereits verfügbar.

MSG_CAR_DBF_SERVER_INCONSISTENT

`EventText: DB feature server inconsistent %s`

Typ: **groß**

Der DB-Feature-Server befindet sich in einem inkonsistenten Zustand.

MSG_CAR_UNEXPECTED_MSG_RECV

`EventText: Unexpected message received %s`

Typ: **klein**

Eine unerwartete Meldung wurde empfangen.

MSG_CAR_UNEXPECTED_DATA_RECV

`EventText: Unexpected data received %s`

Typ: **klein**

Es wurden unerwartete Daten empfangen.

MSG_CAR_PARAM_NOT_FOUND

`EventText: Parameter not found %s`

Typ: **groß**

Ein Parameter wurde nicht gefunden.

MSG_CAR_WRONG_EVENT

`EventText: Wrong event received %x`

Typ: **groß**

Ein falsches Ereignis wurde empfangen.

MSG_CAR_WRONG_LENGTH

`EventText: Wrong length %d`

Typ: **klein**

Falsche Länge.

MSG_CAR_WRONG_IP_ADDRESS

`EventText: Wrong IP address %d.%d.%d.%d`

Typ: **groß**

Falsche IP-Adresse.

MSG_CAR_UNAUTHORIZED_IP_ACCESS

`EventText: Unauthorized access from %d.%d.%d.%d`

Typ: **klein**

Nicht authorisierter Zugriff von der angegebenen IP-Adresse aus.

MSG_CAR_NO_MAC_ADDRESS

`EventText: No MAC address found`

Typ: **groß**

Keine MAC-Adresse gefunden.

MSG_CAR_DBFS_POSS_CONFLICT

`EventText: %s`

Typ: **Warning**

Möglicher Konfikt.

MSG_CAR_CODEC_ENTRY_DELETED

`EventText: CODEC deleted for TableId %d, NodeId %d`

Typ: **groß**

HSA CODEC Zugang gelöscht.

9.2.14 REG-Events

MSG_REG_GLOBAL_ERROR

`EventText: REG : Global error : %s`

Typ: **klein**

REG: Allgemeiner Fehler.

MSG_REG_NO_MEMORY

`EventText: REG : No more memory available`

Typ: **klein**

REG: kein Speicher mehr verfügbar.

MSG_REG_SOH_SEND_DATA_FAILED

`EventText: REG : SOH : send data failed : returncode soh_api_send_tcp_data = %d`

Typ: **Critical**

REG: SOH : Senden der Daten fehlgeschlagen: `soh_api_send_tcp_data` gab einen falschen Rückgabecode zurück.

MSG_REG_REQUEST_WITHIN_REGISTRATION

`EventText: REG : REG request within registration`

Typ: **klein**

REG: REG-Anforderung während Registrierung.

MSG_REG_NIL_PTR_FROM_SOH

`EventText: REG : NIL pointer received from SOH : Pointer = 0x%x`

Typ: **Critical**

REG: NIL-Zeiger (Zeiger ohne Adress-Inhalt) von SOH empfangen.

MSG_REG_ERROR_FROM_SOH

`EventText: REG : SOH : error from SOH : errorcode = 0x%x`

Typ: **Critical**

REG: SOH; Fehler von SOH.

MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH

`EventText: REG : SOH : unknown event from SOH 0x%x`

Typ: **klein**

REG: SOH: Unbekanntes Ereignis von SOH.

MSG_REG_NO_REGISTRATION_POSSIBLE

`EventText: REG : No registration possible (no response)`

Typ: **groß**

REG: Keine Registrierung möglich (keine Antwort).

9.2.15 NU-Events

MSG_NU_GENERAL_ERROR

`EventText: General error %s`

Typ: **Warning**

Nur als ein temporärer Dummy.

MSG_NU_TRANSPCONT_MISSING

`EventText: Transport container missing`

Typ: **groß**

Der Transport-Container fehlt.

MSG_NU_NO_FREE_TRANSACTION

`EventText: No free transaction store found in %s`

Typ: **Warning**

In einer Funktion wurde kein freier Transaktionsspeicher gefunden.

MSG_NU_INVALID_CIDL

`EventText: NCIDL invalid`

Typ: **groß**

Die in der Meldung gesendete CIDL ist ungültig.

MSG_NU_CAR_FAILED

`EventText: Call to CAR function failed`

Typ: **groß**

Der Aufruf einer CAR-Funktion schlug fehl. Es wurde ein fehlerhafter Return-Code zurück gegeben.

MSG_NU_CAR_RESP_INVALID

`EventText: Invalid Response from CAR: 0x%x`

Typ: **groß**

Ungültige Antwort von CAR.

MSG_NU_UNEXPECTED_MSG

`EventText: Unexpected message: State:%d, Event:0x%x, Msgtype:0x%x`

Typ: **groß**

Unerwartete Meldung in einem bestimmten NU-Status.

MSG_NU_UNEXPECTED_TIMER

`EventText: Timer unexpected: State: %d, Subind:0x%x`

Typ: **klein**

Unerwartetes Timer-Ereignis in einem bestimmten NU-Status.

MSG_NU_FREE_CHN_UNEXPECTED

`EventText: Free channel unexpected: State: %d`

Typ: **groß**

Unerwartet freier Kanal in einem bestimmten NU-Status.

MSG_NU_FREE_CHN_COMF_TOO_LATE

`EventText: Free channel confirmation too late State: %d`

Typ: **groß**

Bestätigung für freien Kanal von NU-Leg-Kontrolle kam in einem bestimmten NU-Status zu spät.

MSG_NU_EVENT_EXCEPTION

`EventText: Event exception: State: %d, Event:0x%x, Data:0x %x`

Typ: **klein**

In einem bestimmten NU-Zustand ist eine Ereignisausnahme aufgetreten.

MSG_NU_WRONG_CALL_REF

`EventText: Wrong Call Reference. Event: 0x%x`

Typ: **groß**

Falsche Aufrufreferenz vom System oder vom LAN.

MSG_NU_UNEXPECTED_SETUP

`EventText: Unexpected SETUP: State:%d, Lwport/IPAddr:0x%x, CR:%d, Direction:%d`

Typ: **Warning**

Unerwartetes SETUP bei aktiver Transaktion in einem bestimmten NU-Status. Dies könnte durch eine Blendsituation hervorgerufen worden sein.

MSG_NU_NO_PORT_DATA

`EventText: No data for port_%d found in %s`

Typ: **groß**

In einer bestimmten Funktion wurden keine Port-Daten vorgefunden.

MSG_NU_SUPERFLUOS_MSG

`EventText: Superfluous message: Event:0x%x, Lwport:%d, Channel:%d, Data:0x%x`

Typ: **klein**

An NU gesendete Superfluous-Meldung. Dies könnte durch ein asynchrones Verhalten der beiden Knoten hervorgerufen worden sein.

MSG_NU_IP_ERROR

`EventText: IP Error: IPAddress:0x%x, Error: 0x%x`

Typ: **klein**

IP-Fehler.

MSG_NU_UNKNOWN_MESSAGE

`EventText: Unknown message: Event:0x%x, Channel:%d`

Typ: **klein**

An NU gesendete unbekannte Meldung.

MSG_NU_INTERNAL_ERROR

```
EventText: NU internal error: %s
```

Typ: **klein**

Interner NU-Software-Fehler.

MSG_NU_TOO_MUCH_DIGITS

```
EventText: ?*?Too many digits sent at a time
```

Typ: **klein**

Es wurden zu viele Ziffern gleichzeitig gesendet.

MSG_NU_TCP_LISTENER_FAILED

```
EventText: Start_tcp_listener failed
```

Typ: **Critical**

Der Socket-Handler konnte eine Listener-Funktion nicht starten.

MSG_NU_SOH_RESP_INVALID

```
EventText: SOH call back response invalid. Event:0x%x,
Reason:%s
```

Typ: **klein**

Parameter, die von einer Callback-Funktion im Socket-Handler zurück gegeben wurden, sind ungültig, oder es liegt ein SOH-Fehler vor.

MSG_NU_DEV_TAB_NOT_FOUND

```
EventText: Device table not found
```

Typ: **groß**

Der Zugriff auf die Gerätetabelle ist nicht in Ordnung.

9.2.16 NU Leg Control Events

MSG_NULC_MESSAGE_ERROR

```
EventText: Unexpected message ID or eventcode (%x)
            %x = message type
```

Typ: **Warning**

Unerwartete oder unbekannte Meldung erhalten.

MSG_NULC_PARAM_ERROR

```
EventText: Missing/not valid parameter %s in message %s
            %s = name of either parameter or message
```

Typ: **groß**

Ein Pflicht-Parameter fehlt oder enthält einen ungültigen Wert.

MSG_NULC_MEMORY_ERROR

`EventText: EventText: ?*?Canâ##t access/allocate memory`

Typ: **groß**

Die Anwendung erhielt den angeforderten Speicher nicht, oder irgendeine andere Operation gab einen Nullzeiger zurück.

MSG_NULC_INTERNAL_ERROR

`EventText: %s`

Typ: **groß**

Interner Fehler bei NU-Leg-Kontrolle.

MSG_NULC_INTERNAL_EVENT

`EventText: %s`

Typ: **Information**

Die Anwendung wurde erfolgreich gestartet oder beendet.

9.2.17 HFA-Manager-Events

MSG_HFAM_HAH_ALLOC_CHAN_ERR

`EventText: tried to allocate channel for client that is not in idle state`

Typ: **groß**

Es wurde versucht, einen Kanal für einen Client zu belegen, der sich nicht im Ruhezustand befindet. Interner Fehler im HFA-Manager.

MSG_HFAM_HAH_ALLOC_CONF_ERR

`EventText: HFAM_ALLOCATE_CHANNEL_CONF received from client that is not in allocating or opening state`

Typ: **groß**

Von einem Client, der sich nicht im öffnenden Status befindet, wurde die Meldung `HFAM_OPEN_CHANNEL_CONF` empfangen. HFAA-Fehler.

MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR

`EventText: unknown/unexpected event code received: lw_event`

Typ: **groß**

Unbekannten/unerwarteten Event-Code empfangen: `lw_event`. Systemseitiger Fehler DH/CP.

MSG_HFAM_MAIN_ILLEG_PORTNO_ERR

`EventText: Illegal port no with event code`

Typ: **groß**

Ungültige Portnummer mit Event-Code. Überprüfen Sie das System!

MSG_HFAM_MAIN_NO_LOGONTIMER_ERR

`EventText: No logon timer started for that client`

Typ: **groß**

Für den Client wurde kein Logon-Timer gestartet. Interner Fehler des HFA-Managers.

MSG_HFAM_LIH_CREATE_REGISOCK_ERR

`EventText: Could not create registration socket`

Typ: **Critical**

Es konnte kein Registrierungs-Socket erzeugt werden. LAN-seitiger Fehler.

MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR

`EventText: Could not set socket option â##reuse address`

Typ: **Critical**

Die Socket-Option 'reuse address' konnte nicht gesetzt werden. LAN-seitiger Fehler.

MSG_HFAM_LIH_BIND_REGISOCK_ERR

`EventText: Could not bind registration socket`

Typ: **Critical**

Der Registrierungs-Socket konnte nicht gebunden werden. LAN-seitiger Fehler.

MSG_HFAM_LIH_LISTEN_REGISOCK_ERR

`EventText: Could not listen at registration socket`

Typ: **Critical**

Am Registrierungs-Socket war keine Überwachung möglich. LAN-seitiger Fehler.

MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR

`EventText: Could not accept TCP/IP connection from client`

Typ: **Critical**

Die TCP/IP-Verbindung des Clients konnte nicht akzeptiert werden. LAN-seitiger Fehler. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR

`EventText: Could not accept TCP/IP connection from client`

Typ: **groß**

Die Verbindung vom Client wurde nicht akzeptiert. LAN-seitiger Fehler. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_MAX_CON_EXCEED_ERR

`EventText: max no.(HFAM_MAX_CONNECTIONS) of TCP/IP connections exceeded`

Typ: **groß**

Die maximale Anzahl (HFAM_MAX_CONNECTIONS) von TCP/IP-Verbindungen wurde überschritten. Interner Fehler des HFA-Managers.

MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR

```
EventText: Cannot accept connection from client
```

Typ: **groß**

Die Verbindung vom Client konnte nicht akzeptiert werden. LAN-seitiger Fehler. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR

```
EventText: CSocket would block: no data -> ignore
```

Typ: **klein**

Der Socket würde blockieren: keine Daten. Ignorieren. LAN-seitiger Fehler.

MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR

```
EventText: TC_DATAGRAM received from client->subscriber_no
while not in logged_in state, discarded
```

Typ: **klein**

Vom Client->Kundennummer wurde die Meldung TC_DATAGRAM empfangen, obwohl nicht eingeloggt. Daher ausgesondert. LAN-seitiger Fehler. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_UNEXP_CORNET_ERR

```
EventText: unknown/unexpected Cornet-TS message received
from client
```

Typ: **klein**

Unbekannte/unerwartete Cornet-TS-Meldung vom Client empfangen. Überprüfen Sie den Client!

MSG_HFAM_LIH_IPADR_TOO_LONG_ERR

```
EventText: IP-address too long, cut !
```

Typ: **groß**

IP-Adresse war zu lang und wurde abgeschnitten. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR

```
EventText: SubNo too long, cut !
```

Typ: **groß**

Kundennummer war zu lang und wurde abgeschnitten. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_ALGORITM_OBJID_ERR

```
EventText: SubNo too long, cut !
```

Typ: **groß**

Die Algorithmus Objekt-ID war zu lang und wurde abgeschnitten. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_PROTOCOL_LIST_ERR

`EventText: too many elements in protocol list`

Typ: **groß**

Die Protokoll-Liste enthält zu viele Elemente. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_RETURNED_SOCKET_ERR

`EventText: returned socket error`

Typ: **groß**

Zurück gegebener Socket-Fehler. LAN-seitiger Fehler.

MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR

`EventText: timeslot is valid`

Typ: **groß**

Der Login-Timer für einen Client konnte nicht gestartet werden. HFA-Manager Start.

MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR

`EventText: Input Parameter for hfam_sih_send_ts invalid`

Typ: **groß**

Ein Input-Parameter für die Funktion `hfam_sih_send_ts` war ungültig. System-seitiger Fehler.

MSG_HFAM_SIH_CORNET_LONGER_28_ERR

`EventText: cannot synthesize CorNet-TS message longer than 28 bytes`

Typ: **groß**

CorNet-TS-Meldungen mit mehr als 28 Bytes können nicht synthetisiert werden. System-seitiger Fehler.

MSG_HFAM_MON_NO_MON_TIMER_ERR

`EventText: No monitor timer !`

Typ: **klein**

Kein Monitor-Timer. HFA-Manager Start.

MSG_HFAM_REG_LOGIN_NOTREG_ERR

`EventText: DL_LOGON_IN received for client not in not_registered state, subno`

Typ: **klein**

Die Meldung `DL_LOGON_IN`, die für den Client empfangen wurde, ist nicht im registrierten Zustand. HFA-Manager intern.

MSG_HFAM_REG_SUBNO_TOO_LONG_ERR

`EventText: DL_LOGON_IN received for client not in not_registered state`

Typ: **groß**

Die Unternummer in der Meldung `DL_LOGON_IN` ist zu lang und wurde abgeschnitten. Überprüfen Sie das Client-Setup im System!

MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR

`EventText: SubNo from System I/F not found in config data`

Typ: **klein**

Die Unternummer der Systemschnittstelle wurde in den Konfigurationsdaten nicht gefunden. Überprüfen Sie das Client-Setup im System!

MSG_HFAM_REG_ESTAB_NOTREG_ERR

`EventText: DL_EST_IN arrived for client not in registered state`

Typ: **klein**

Die Meldung `DL_EST_IN`, die für den Client empfangen wurde, ist nicht im registrierten Zustand. Überprüfen Sie das System-Setup oder WBM!

MSG_HFAM_REG_RELIN_NOTREG_ERR

`EventText: DL_REL_IN arrived for client not in registered state`

Typ: **klein**

Die Meldung `DL_REL_IN`, die für den Client empfangen wurde, ist nicht im registrierten Zustand. Überprüfen Sie das System-Setup oder WBM!

MSG_HFAM_REG_MISSING_L2INFO_ERR

`EventText: missing L2addr-InfoElem, no IP address`

Typ: **klein**

`L2addr-InfoElem` fehlt, keine IP-Adresse. Überprüfen Sie das System-Setup oder WBM!

MSG_HFAM_REG_LOGON_REJECT_ERR

`EventText: logon of client->subscriber_no rejected`

Typ: **Information**

Das Logon der Client-Kundennummer wurde zurück gewiesen. Überprüfen Sie das System-Setup!

MSG_HFAM_REG_INVAL_PWD_LEN_ERR

`EventText: invalid password length of <sub_number>, no hash`

Typ: **klein**

Ungültige Passwortlänge zu <Unternummer>, kein Hash. Überprüfen Sie das Client-Setup oder WBM!

9.2.18 HFA-Adapter-Events

MSG_HFAA_MESSAGE_ERROR

`EventText: Unexpected message ID or eventcode (%x)`

Typ: **Warning**

Unerwartete oder unbekannte Meldung erhalten.

MSG_HFAA_PARAM_ERROR

`EventText: Missing/not valid parameter %s in message %s`

Typ: **groß**

Ein Pflicht-Parameter fehlt oder enthält einen ungültigen Wert.

MSG_HFAA_MEMORY_ERROR

`EventText: ?*?Canâ##t access/allocate memory`

Typ: **groß**

Die Anwendung erhält nicht den angeforderten Speicher, oder ein Konstruktor gibt einen Nullzeiger zurück.

MSG_HFAA_INTERNAL_ERROR

`EventText: %s`

Typ: **groß**

Ein interner Fehler im HFA-Adapter.

MSG_HFAA_INTERNAL_EVENT

`EventText: %s`

Typ: **Information**

Die Anwendung wurde erfolgreich gestartet oder beendet.

9.2.19 PPP-Anruf-Kontroll-Events

Derzeit keine implementiert.

9.2.20 PPP-Manager-Events

MSG_PPPM_ERR_CONFIG

`EventText: %p`

Typen: **Critical, Major, Minor**

Inkonsistenz bei den Konfigurationsdaten. Fehler beim Admin-Empfänger. Gehen Sie die Konfigurationsdaten für PPP systematisch durch. Informieren Sie die Software-Entwicklung, stellen Sie Trace-Dateien (PPPM_TBAS, PPPM_TSTD, PPPM_TEXT Level 9) zur Verfügung, die dieses fehlerhafte Verhalten dokumentieren!

MSG_PPPM_ERR_OPERATION

`EventText: %p`

Typen: **Critical, Major, Minor**

Unerwartete Bedingung während einer Operation. Informieren Sie die Software-Entwicklung, stellen Sie Trace-Dateien (PPPM_TBAS, PPPM_TSTD, PPPM_TEXT Level 9) zur Verfügung, die dieses fehlerhafte Verhalten dokumentieren!

9.2.21 PPP-Stack-Events

MSG_PPP_STACK_PROC

`EventText: %p`

Typen: **Major, Minor, Warning**

Interner Fehler bei der PPP-Stack-Verarbeitung. Informieren Sie die Software-Entwicklung, stellen Sie Trace-Dateien (PPP_STACK_PROC Level 6 und PPP_STACK_DBG_IF Level 9) zur Verfügung, die dieses fehlerhafte Verhalten dokumentieren!

9.2.22 SPE-Events

MSG_SPE_CERT_MISSING

Zertifikat für Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) ist nicht verfügbar.

MSG_SPE_CERT_AVAIL

Zertifikat für Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) ist verfügbar.

MSG_SPE_CERT_UPDATED

Zertifikat für Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) wurde aktualisiert.

MSG_SPE_CERT_EXPIRED

Zertifikat für Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE)) ist abgelaufen.

MSG_SPE_CERT_TIMEREMAINING

Zertifikat für Signaling- und Payload-Encryption, verbleibende Zeit

MSG_SPE_CRL_EXPIRED

Zertifikatssperrliste für SPE ist abgelaufen.

MSG_SPE_CRL_UPDATED

Zertifikatssperrliste für SPE wurde aktualisiert.

MSG_SPE_ALL_CRLS_UPTODATE

Alle Zertifikatssperrlisten für SPE sind aktuell.

9.2.23 VCAPI-Events

MSG_BSD44_SELECT_ERROR

`EventText: Select error for VCAPI & DATAGW Dispatcher`

Typ: **groß**

Sockets für VCAPI- und DATAGW-Clients arbeiten nicht mehr.

MSG_BSD44_ACCEPT_ERROR

`EventText: Accept error for VCAPI Dispatcher`

Typ: **groß**

Es ist nicht möglich, eine neue Verbindung für VCAPI zu errichten.

MSG_VCAPI_NO_CAPI_DATA

`EventText: No CAPI data in message with event 0x%x`

Typ: **klein**

In der Meldung, die vom VCAPI-Server oder von `CAPI_PAYLOAD_INT` empfangen wurde, sind keine Daten verfügbar.

MSG_VCAPI_WRONG_LINKNUM

`EventText: Wrong link number %d in message %s`

Typ: **klein**

In der Meldung, die vom VCAPI-Server oder von `CAPI_PAYLOAD_INT` empfangen wurde, ist eine falsche Linknummer.

MSG_VCAPI_LINK_TABLE_FULL

`EventText: No free element found in VS_Plci_Link table`

Typ: **groß**

Zu viele physikalische Link-Verbindungen werden nicht ordnungsgemäß freigegeben.

MSG_VCAPI_NO_PLCI

`EventText: PLCI not found in VS_Plci_Link table (to find message_nbr)`

Typ: **groß**

PLCI in `VS_Plci_Link` Tabelle nicht gefunden (benötigt, um `message_nbr` zu finden).

MSG_VCAPI_CONV_H2N_ERROR

`EventText: Conversion error:%d`

Typ: **klein**

Die Meldung zum Client wurde nicht korrekt konvertiert.

MSG_VCAPI_CONV_H2N_FAILED

`EventText: Conversion for %s returns %d,expected %d`

Typ: **klein**

Die Konvertierung gibt einen falschen Wert zurück.

MSG_VCAPI_WRONG_CONV_H2N

`EventText: Wrong conversion for %s`

Typ: **klein**

Die Nachricht wurde nicht konvertiert (falsche Nachricht).

MSG_VCAPI_WRONG_MSG_LENGTH

`EventText: Wrong message length %d`

Typ: **klein**

Die Gesamtlänge der CAPI-Nachricht stimmt nicht.

MSG_VCAPI_CONV_N2H_FAILED

`EventText: Conversion for %s returns %d,expected %d)`

Typ: **klein**

Die Konvertierung gibt einen falschen Wert zurück.

MSG_VCAPI_WRONG_CONV_N2H

`EventText: Wrong conversion for %s`

Typ: **klein**

Die Nachricht wurde nicht konvertiert (falsche Nachricht).

MSG_VCAPI_UNKNOWN_MSG_N2H

`EventText: unknown msg %s`

Typ: **klein**

Falsches Sub-Kommando in der Nachricht.

MSG_VCAPI_TOO_MANY_CLIENTS

`EventText: Too many clients connected`

Typ: **Warning**

Kein freies Element in der Verbindungstabelle gefunden. Die Verbindung wird geschlossen.

MSG_VCAPI_ACCEPT_ERROR

`EventText: Accept error for VCAPI Dispatcher`

Typ: **groß**

Es ist nicht möglich, eine neue Verbindung für VCAPI zu errichten.

MSG_VCAPI_DISP_NOT_READY

`EventText: VCAPI Dispatcher not ready`

Typ: **groß**

Der VCAPI-Server hat keine `VCAPI_EVENT_START_OPERATION_REQ`-Meldung an den Dispatcher gesendet.

MSG_VCAPI_NO_CLIENT

`EventText: no client address`

Typ: **klein**

Keine Client-Adresse.

MSG_VCAPI_WRONG_BUF_LEN

`EventText: Wrong buffer length %d`

Typ: **klein**

Die Puffergröße befindet sich nicht innerhalb der Grenzen der Meldung.

MSG_VCAPI_NO_RCV_BUFFER

`EventText: rcvBufPP=0x%x null`

Typ: **klein**

Der Empfangspuffer ist entweder schon wieder freigegeben, oder es ist nicht möglich, entsprechenden Speicher zu reservieren.

MSG_VCAPI_NO_ALLOC_SINGLE

`EventText: Not possible to allocate a single buffer`

Typ: **klein**

Es ist nicht möglich, einen einzelnen Empfangspuffer zu erhalten (Speicher-Reservierungsfehler).

MSG_VCAPI_NO_ALLOC_EXTENDED

`EventText: Not possible to allocate an extended buffer`

Typ: **groß**

Es ist nicht möglich, einen erweiterten Empfangspuffer zu erhalten (Speicher-Reservierungsfehler). Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_BUF_NOT_CREATED

`EventText: Not possible to create buffer with size:%d`

Typ: **groß**

Es ist nicht möglich, so viel Speicher wie erforderlich zu reservieren.

MSG_VCAPI_NO_NEW_BUF

`EventText: No new buffer created by vs_bputd`

Typ: **groß**

Es ist nicht möglich, einen neuen Puffer zum Speichern der empfangenen Daten zu erzeugen (Speicher-Reservierungsfehler). Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_DATA_NOT_STORED

`EventText: Not possible to get a receive buffer,data not stored`

Typ: **groß**

Die empfangenen Daten wurden nicht gespeichert, weil kein neuer Puffer erzeugt werden konnte (Speicher-Reservierungsfehler). Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_SOCKET_NOT_OPEN

`EventText: VCAPI-Socket not opened`

Typ: **groß**

Der Socket konnte nicht geöffnet werden (Verbindungen mit Clients sind nicht möglich).

MSG_VCAPI_SOCKET_BIND_ERR

`EventText: bind error for socket %d`

Typ: **groß**

Bindungs-Fehler beim VCAPI-Socket (Verbindungen mit Clients sind nicht möglich).

MSG_VCAPI_LISTENING_ERR

`EventText: listening error for socket %d`

Typ: **groß**

Es ist nicht möglich, einen Listening-VCAPI-Socket zu erzeugen (Verbindungen mit Clients sind nicht möglich).

MSG_VCAPI_RECEIVE_ERR

`EventText: Error while receiving message for VCAPI Dispatcher:Returncode %x`

Typ: **klein**

Fehler beim Empfangen einer Meldung für den VCAPI-Dispatcher.

MSG_VCAPI_NO_ALLOC_MSG

`EventText: Not possible to allocate a buffer`

Typ: **groß**

Es ist nicht möglich, eine Meldung an den VCAPI-Dispatcher zu senden, weil kein Puffer reserviert werden konnte (Speicher-Reservierungsfehler). Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_WRONG_EVENT_SRV

`EventText: wrong eventcode from VCAPI_SERVER`

Typ: **Warning**

Der VCAPI-Dispatcher hat vom VCAPI-Server einen falschen Event empfangen.

MSG_VCAPI_PLCI_NOT_FOUND

`EventText: PLCI not found in VS_Plci_Link table`

Typ: **klein**

Beim Empfangen einer Meldung von `VS_Plci_Link` wurde PLCI in der Tabelle `CAPI_PAYLOAD_IF` nicht gefunden.

MSG_VCAPI_IND_ALLOC_ERR

`EventText: Not possible to allocate a buffer for CMT_DATA_IND`

Typ: **groß**

Es ist nicht möglich, einen Puffer für `CMT_DATA_IND` zu reservieren. Die Meldung an den Client kann nicht gesendet werden. Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_CONF_ALLOC_ERR

`EventText: Not possible to allocate a buffer for CMT_DATA_CONF`

Typ: **groß**

Es ist nicht möglich, einen Puffer für `CMT_DATA_CONF` zu reservieren. Die Meldung an den Client kann nicht gesendet werden. Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_WRONG_EVENT_CAPI

`EventText: Nwrong eventcode from CAPI_PAYLOAD_INTERFACE`

Typ: **Warning**

Der VCAPI-Dispatcher hat einen falschen Event von `CAPI_PAYLOAD_IF` empfangen.

MSG_VCAPI_WRONG_LENGTH_MSG

`EventText: Wrong message length %d`

Typ: **Warning**

Die Meldung vom Client an den VCAPI-Server/`CAPI_PAYLOAD_IF` hat eine fehlerhafte Länge.

MSG_VCAPI_NO_PLCI_DATA_B3

`EventText: PLCI not found in VS_Plci_Link table (for DATA_B3_REQ)`

Typ: **klein**

PLCI wurde in der Tabelle `VS_Plci_Link` nicht gefunden (für `DATA_B3_REQ`). Die Meldung an `CAPI_PAYLOAD_IF` kann nicht gesendet werden.

MSG_VCAPI_DATA_B3_ALLOC_ERR

`EventText: ALLOC ERROR: returncode %x`

Typ: **groß**

Es ist nicht möglich, einen Puffer zum Senden der DATA_B3_REQ-Meldung an CAPI_PAYLOAD_IF zu erhalten (Speicher-Reservierungsfehler). Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_NO_PLCI_DISCONNECT

EventText: PLCI Element not found in VS_Plci_Link table for DISCONNECT_RESPONSE

Typ: **klein**

Für die DISCONNECT_RESPONSE-Meldung wurde das PLCI-Element in der Tabelle VS_Plci_Link nicht gefunden.

MSG_VCAPI_MSG_NOT_SEND

EventText: Not possible to send message

Typ: **Warning**

Es ist nicht möglich, eine Meldung zu senden. Die Schnittstelle zu CAPI_PAYLOAD gibt -1 zurück.

MSG_VCAPI_NO_LIST_SOCKET

EventText: no listening socket stored in connection table

Typ: **groß**

In der Verbindungstabelle kann kein Listening-Socket gespeichert werden. Es können keine neuen Verbindungen geöffnet werden.

MSG_VCAPI_RCV_LEN_ERR

EventText: Wrong message length at receive data from client

Typ: **Warning**

Beim Empfang von Daten vom Client hat eine Meldung eine falsche Länge. Die Verbindung wird geschlossen. Die Meldung wird nicht an den VCAPI-Server gesendet.

MSG_VCAPI_SOCKET_RCV_ERR

EventText: Error on receiving data from the Socket (connection interrupted)

Typ: **Warning**

Die Verbindung wurde unterbrochen, was einen Fehler beim Empfangen von Daten verursacht.

MSG_VCAPI_SOCK_NOT_AVAIL

EventText: connected socket not stored in connection table

Typ: **klein**

Der verbundene Socket wurde nicht in der Verbindungstabelle gespeichert. Es können keine Daten empfangen werden.

MSG_VCAPI_UNKNOWN_NTFY

EventText: Unbekannte Benachrichtigung. Used value:%d

Typ: **Warning**

Unbekannte Benachrichtigung.

MSG_VCAPI_NO_LNK_CONN

`EventText: Link number not found in connection table`

Typ: **klein**

Die Linknummer wurde in der Verbindungstabelle nicht gefunden.

9.2.24 VCAPI-Anwendungs-Events

MSG_VCAPI_SERVER_ERROR

`EventText: VCAPI Server error: %p`

Typ: **Warning**

Verschiedene VCAPI-Server-Fehler vom HXG2-Code.

MSG_VCAPI_UNANTICIPATED_MESSAGE

`EventText: Unanticipated Message %s for CSID %s in state %s`

Typ: **Warning**

Der CAPI-Manager hat eine unvorhergesehene Meldung für den aktuellen Zustand des entsprechenden CAPI-Objekts empfangen.

MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE

`EventText: Unanticipated CAPI message %s`

Typ: **Warning**

Der CAPI-Manager hat eine unvorhergesehene CAPI-Meldung mit einem unbekannten Kommando und Subkommando empfangen.

MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE

`EventText: Unanticipated VCAPI Dispatcher message %d`

Typ: **Warning**

Der VCAPI-Server hat eine VCAPI-Dispatcher-Meldung mit einem unbekannten Event empfangen.

MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE

`EventText: Unanticipated Message Base %m`

Typ: **Warning**

Der VCAPI-Server, die VCAPI-Schnittstelle oder der CAPI-Manager haben eine Meldungsbasis mit unvorhergesehener ID empfangen.

MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT

`EventText: Part of the CAPI Message is missing (%d > %d)`

Typ: **Warning**

Die Länge der CAPI-Meldung ist größer als die Größe des VBStrings, der diese CAPI-Meldung enthält.

MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG

`EventText: Message Base without CAPI message`

Typ: **Warning**

Der VCAPI-Server, die VCAPI-Schnittstelle oder der CAPI-Manager hat `CapiInd` oder `CapiReq` erhalten, jedoch ohne die erforderliche CAPI-Meldung.

MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG

`EventText: MMessage Base without Data GW message`

Typ: **Warning**

Der CAPI-Manager hat von NU oder vom Data GW Dispatcher eine Meldungsbasis empfangen, jedoch ohne die erforderliche VCAPI-Dispatcher-Meldung.

MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG

`EventText: Message Base without VCAPI Dispatcher message`

Typ: **Warning**

Der VCAPI-Server jat vom VCAPI Dispatcher eine Meldungsbasis empfangen, jedoch ohne die erforderliche VCAPI-Dispatcher-Meldung.

MSG_VCAPI_ILLEGAL_LINK_NUMBER

`EventText: Illegal link number: %d`

Typ: **Warning**

Es wurde der Versuch unternommen, ein Element der Dynamischen Linktabelle mit einem ungültigen Index zu adressieren.

MSG_VCAPI_ILLEGAL_PARTNER_NUMBER

`EventText: Illegal partner number: %d`

Typ: **Warning**

Es wurde der Versuch unternommen, auf die Informationen zu einem nicht angeforderten VCAPI-Partner zuzugreifen.

MSG_VCAPI_ADD_OBJECT_FAILED

`EventText: Could not add a CAPI object to the managed object list`

Typ: **groß**

Ein neu erzeugtes CAPI-Objekt konnte nicht zur verwalteten Objektliste hinzugefügt werden. Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_COULD_NOT_CREATE_OBJECT

`EventText: Could not create a CAPI object`

Typ: **Warning**

Es konnte kein neues CAPI-Objekt erzeugt werden.

MSG_VCAPI_COULD_NOT_DELETE_OBJECT

`EventText: Could not delete a CAPI object`

Typ: **groß**

Das angegebene CAPI-Objekt konnte nicht gelöscht werden. Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_NO_PLCI_AVAILABLE

`EventText: No PLCI available`

Typ: **Warning**

Alle verfügbaren PLCIs sind belegt.

MSG_VCAPI_CSID_MISSING

`EventText: CSID is missing`

Typ: **Warning**

Der CAPI-Manager hat eine Meldung von NU oder von CCP empfangen, die keine Anruf- und Session-ID enthält.

MSG_VCAPI_COULD_NOT_FIND_PLCI

`EventText: Could not find the corresponding PLCI`

Typ: **Warning**

Das PLCI, das zu einer gegebenen Anruf- und Session-ID oder zu einer gegebenen Kanal-ID gehört, konnte nicht gefunden werden.

MSG_VCAPI_COULD_NOT_FIND_OBJECT

`EventText: Could not find the corresponding CAPI Object`

Typ: **Warning**

Das CAPI-Objekt, das zu einer gegebenen Anruf- und Session-ID gehört, konnte nicht gefunden werden.

MSG_VCAPI_COULD_NOT_FIND_CSID

`EventText: Could not find the corresponding CSID`

Typ: **Warning**

Die Anruf- und Session-ID, die zu einem gegebenen PLCI gehört, konnte nicht gefunden werden.

MSG_VCAPI_COULD_NOT_STORE_REQ

`EventText: Could not store the request %x %x for PLCI %d`

Typ: **groß**

An der CAPI-Schnittstelle ist kein Speicher mehr verfügbar, um den Request zu speichern. Das Gateway führt einen automatischen Neustart durch.

MSG_VCAPI_CONF_WITHOUT_REQ

`EventText: Confirmation %x %x for PLCI %d without stored Request`

Typ: **Warning**

Die CAPI-Schnittstelle hat eine Bestätigung ohne entsprechenden gespeicherten Request empfangen.

9.2.25 H.323-Client-Events

MSG_H323CLIENT_INVALID_CLIENTID

`EventText: invalid Peer ID: %d`

Typ: **groß**

Software-Fehler: der Index der Client-Tabelle ist nicht korrekt. Das Trace-Profil H323Client-Internal wird gestoppt.

MSG_H323CLIENT_INVALID_ADMIN_MSG

`EventText: invalid admin message for file %s received`

Typ: **klein**

Beim Lesen/Schreiben von Konfigurationsdateien wurde ein Fehler empfangen. Das Trace-Profil H323Client-Internal wird gestoppt.

MSG_H323CLIENT_NWRS_ENTRY_FAILED

`EventText: create %s entry failed for client (%i, %i)`

Typ: **groß**

Das Erzeugen eines NWRS-Eintrags schlug fehl. Das Trace-Profil H323Client-Internal wird gestoppt.

MSG_H323CLIENT_INVALID_PARAM

`EventText: invalid parameter %s, value %x`

Typ: **groß**

Software-Fehler: ungültiger Parameter. Das Trace-Profil H323Client-Internal wird gestoppt.

MSG_H323CLIENT_MAPS_DIFFER

`EventText: size of maps differ (call no: %I, IP: %I)`

Typ: **groß**

Software-Fehler: ungültiger Parameter. Das Trace-Profil H323Client-Internal wird gestoppt.

9.2.26 IPNC-Events

MSG_IPNC_MESSAGE_ERROR

`EventText: message error: %s`

Typ: **groß**

Eine unerwartete Meldung wurde empfangen und ignoriert. Das Trace-Profil IPNC-Std wird gestoppt.

MSG_IPNC_MESSAGE_DUMP

```
EventText: message error: %s% M
```

Typ: **groß**

Eine unerwartete Meldung wurde empfangen und ignoriert. Das Trace-Profil IPNC-Std wird gestoppt.

MSG_IPNC_PARAM_ERROR

```
EventText: message parameter error: %s %x
```

Typ: **groß**

Eine Meldung mit ungülgigem Parameter wurde empfangen und ignoriert. Das Trace-Profil IPNC-Std wird gestoppt.

MSG_IPNC_INTERNAL_ERROR

```
EventText: internal error: %I
```

Typ: **groß**

Software-Fehler: ungültige interne Daten wurden entdeckt. Das Trace-Profil IPNC-Detailed wird gestoppt.

MSG_IPNC_INCONSISTENT_STATE

```
EventText: inconsistent internal state: %s %x
```

Typ: **groß**

Software-Fehler: Daten wurden während der Verarbeitung inkonsistent. Das Trace-Profil IPNC-Std wird gestoppt.

MSG_IPNC_CP_ASYNCH

```
EventText: CP and IPNC asynchronous: %s %s
```

Typ: **groß**

Asynchronie zwischen den Zuständen von CP und IPNC entdeckt. Das Trace-Profil IPNC-Std wird gestoppt.

9.2.27 IPNC- Events

MSG_IPNCA_ERROR

```
EventText: IPNC Adapter: (some) Error description ("IPNC
Adapter: %s")
```

Typ: **klein**

Ein kleinerer Fehler ist aufgetreten.

9.2.28 MPH-Events

MSG_MPH_INFO

```
EventText: %p            SGP Message not sent
```

Typ: **Information**

Event-Log-Eintrag für alle MPH-Events. SGP-Meldung kann nicht an IPNC gesendet werden.

9.2.29 OAM-Events

MSG_TLS_MUTEX_BLOCKED

`EventText: Mutex blocked`

Typ: **groß**

Software-Fehler mit Stillstand. Starten Sie das Gateway neu und erstellen Sie einen Fehler-Report!

MSG_DISP_SENDER_NOT_SET

`EventText: Sender not set in message: %n%M`

Typ: **Critical**

Interner Software-Fehler. Der Meldungskopf ist nicht gesetzt. Diesem Event folgt stets ein ASSERT-Event, der einen automatischen Neustart bewirkt.

MSG_OAM_TIMESYNC

`EventText: Time Synchronization from %s to %s`

Typ: **Information**

Die Zeitsynchronisierung wurde durchgeführt.

MSG_OAM_TIMESYNC_FAILED

`EventText: Time Synchronization failed`

Typ: **Warning**

Die Zeitsynchronisierung wurde nicht durchgeführt.

MSG_OAM_PRIO_INCREASED

`EventText: Priority of %s increased`

Typ: **Warning**

Die Priorität eines OAM-Tasks (Trace, Event, OAM) wurde wegen hohem Load erhöht. Dies ist jedoch ein gültiges Verhalten.

MSG_OAM_PRIO_SWITCHED_BACK

`EventText: Priority of %s switched back. OAM Msg Queue OK`

Typ: **Cleared**

Die Priorität eines OAM-Tasks (Trace, Event, OAM) wurde wieder zurück gesetzt, da der hohe Load nicht mehr besteht. Dies ist jedoch ein gültiges Verhalten.

MSG_OAM_QUEUE_FULL

`EventText: POAM Msg Queue (%s) full. Remove Messages`

Typ: **groß**

Die Warteschlange von OAM-Tasks (Trace, Event, OAM) ist voll. Alle Meldungen werden gelöscht. Siehe Section 8.4.1.4, "Überlastung der Baugruppe durch Trace-Informationen".

MSG_OAM_PUT_TO_QUEUE_FAILED

`EventText: Put to OAM Msg Queue (%s) failed. Remove Message`

Typ: **groß**

Das Hinzufügen zur Meldungswarteschlange von OAM-Tasks (Trace, Event, OAM) schlug ohne erkennbaren Grund fehl. Alle Meldungen werden gelöscht.

MSG_OAM_QUEUE_BLOCKED

`EventText: Put to OAM Msg Queue (%s) failed. Queue blocked. Remove Message`

Typ: **groß**

Das Hinzufügen zur Meldungswarteschlange von OAM-Tasks (Trace, Event, OAM) schlug fehl, weil die Warteschlange blockiert ist. Alle Meldungen werden gelöscht.

MSG_OAM_INTERNAL_EVENT

`EventText: %p`

Typ: **Warning**

Das Ausführen einer automatischen Aktion schlug fehl.

MSG_ADMIN_LOGGED_IN

`EventText: %s user \"%s\" (session id = %d) logged in`

Typ: **Information**

Information zu einem erfolgreichen Login eines Administrators.

MSG_ADMIN_SESSION_CREATED

`EventText: %s session created for user \"%s\" (session id = %d)`

Typ: **Information**

Eine Session für einen Administrator oder eine automatische Login-Prozedur (z. B. AutoDiscovery oder Datentransfer von OpenScape 4000 V10 zu HG 3500/3575) wurde erzeugt.

MSG_ADMIN_LOGGED_OUT

`EventText: %s user \"%s\" (session id = %d) logged out`

Typ: **Information**

Information zu einem erfolgreichen Login eines Administrators.

MSG_ADMIN_INVALID_LOGIN

`EventText: Invalid login from %s (user \"%s\")`

Typ: **Information**

Ungültiger Login-Versuch.

MSG_ADMIN_SESSION_EXPIRED

```
EventText: Session id = %d of user \"%s\" expired
```

Typ: **Information**

Die Session ist abgelaufen (Session-Timeout erreicht). Loggen Sie sich gegebenenfalls neu ein!

MSG_ADMIN_GOT_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) got write
access
```

Typ: **Information**

Ein Administrator hat Schreibberechtigung erhalten. Damit kann er die Gateway-Konfiguration ändern.

MSG_ADMIN_DIDNâT_GET_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) didnâ##t get
write access
```

Typ: **Information**

Ein Administrator hat keine Schreibberechtigung erhalten. Ein anderer Administrator hat bereits Schreibberechtigung. Warten Sie oder erzwingen Sie die Schreibberechtigung (z. B. via WBM).

MSG_ADMIN_RELEASED_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) released write
access
```

Typ: **Information**

Ein Administrator hat die Schreibberechtigung beendet und kann keine Änderungen mehr an der Gateway-Konfiguration durchführen. Andere Administratoren können nun Schreibberechtigung erhalten.

MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) released write
access
```

Typ: **Information**

Der aktuelle Administrator hat die Schreibberechtigung zwangsweise verloren, weil ein anderer Administrator die Schreibberechtigung übernommen hat. Nur der andere Administrator kann nun die Gateway-Konfiguration ändern.

MSG_CAR_CALL_ADDR_REJECTED

```
EventText: Call address rejected %s
```

Typ: **klein**

Die angegebene Rufadresse wurde zurückgewiesen.

MSG_WEBSERVER_INTERNAL_ERROR

```
EventText: %p
```

Typ: **Warning**

Interner Fehler beim Webserver, interne Ausnahmesituation, die jedoch keinen Einfluss auf weitere Aktivitäten des Webservers hat.

9.2.30 CLI-Events

MSG_CLI_TELNET_ABORTED

`EventText: Telnet client \"%s\" aborted`

Typ: **Warning**

Ein Telnet-Client hat vor dem Einloggen die Verbindung getrennt.

MSG_CLI_LOGGED_IN_FROM_TELNET

`EventText: User \"%s\" logged in (session id = %d) from telnet CLI with IP address %s`

Typ: **Information**

Ein Telnet-Client hat sich erfolgreich eingeloggt.

MSG_CLI_LOGGED_IN_FROM_V24

`EventText: User \"%s\" logged in (session id = %d) from V24 CLI`

Typ: **Information**

Ein Benutzer hat sich über die V.24-Schnittstelle erfolgreich eingeloggt.

9.2.31 HIP-Events

MSG_HIP_ALLOC_DEV_OBJ

`EventText: hi_main: Device allocation memory not possible`

Typ: **Warning**

Kein Heap-Speicher für Device-Daten. Überprüfen Sie den verfügbaren Speicher!

MSG_HIP_NO_MEM_CLBLK

`EventText: hi_main: No memory for Cluster block available`

Typ: **Warning**

Kein Speicher für ein Cluster-Block verfügbar. Überprüfen Sie, warum kein reservierbarer Speicher im Gateway verfügbar ist!

MSG_HIP_NO_MEM_CL

`EventText: hi_main: No memory for Cluster %d available`

Typ: **Warning**

Kein Speicher für ein Cluster verfügbar. Überprüfen Sie, warum kein reservierbarer Speicher im Gateway verfügbar ist!

MSG_HIP_NO_NETPOOL_INIT

`EventText: NETPOOL INIT not possible: Return value %d`

Typ: **Warning**

Die Initialisierung des Netpools für HIP ist nicht möglich. Überprüfen Sie den Rückgabewert %d und ergreifen Sie geeignete Maßnahmen!

MSG_HIP_NO_OBJ_INIT

`EventText: No initialization of END_OBJ Structure possible`

Typ: **Warning**

Die Initialisierung von `END_OBJ` für HIP ist nicht möglich. Überprüfen Sie den `END_OBJ`-Zeiger und den Speicher!

MSG_HIP_NO_DEVLOAD

`EventText: hi_main:Loading device into MUX not possible, unit = %d, pendLoad = %X,Pinitstring = %X, Loaning = %d,pBSP = %X`

Typ: **Warning**

Das Laden des HIP-Device in MUX ist nicht möglich. Überprüfen Sie die Parameter, die an `muxDevLoad` übergeben werden!

MSG_HIP_NO_DEVSTART

`EventText: I_main: Start HIP device not Possible, return value = %X`

Typ: **Warning**

Das Starten des HIP Device in MUX ist nicht möglich. Werten Sie den Rückgabewert %X aus und ergreifen Sie geeignete Maßnahmen.

MSG_HIP_NO_MEM_TO_SI

`EventText: SI_main: allocating of memory for message to SI not possible`

Typ: **Warning**

Das Anfordern von Speicher für eine Meldung an die Systemschnittstelle ist nicht möglich. Überprüfen Sie, warum kein Speicher am Gateway angefordert werden kann.

MSG_HIP_NO_CLPOOL_ID

`EventText: hi_main: No clusterpool ID available`

Typ: **Warning**

Es ist keine Cluster-Pool-ID zum Senden eines Pakets zu einer IP über MUX verfügbar. Überprüfen Sie das Problem!

MSG_HIP_NO_CLUSTER

`EventText: I_main:No cluster available to make packet,packet_len = %d`

Typ: **Warning**

Es ist kein Cluster der nachgefragten Länge verfügbar. Das Problem kann darin bestehen, dass nicht genügend Cluster einer bestimmten Länge frei sind, oder dass die Cluster nicht freigegeben worden sind.

MSG_HIP_NO_CLBLK

`EventText: No clusterblock for netpool available`

Typ: **Warning**

Es gibt keine Cluster-Blocks mehr. Die Anzahl der definierten Cluster-Blocks ist nicht groß genug.

MSG_HIP_NO_PMBLK

`EventText: No memory block for incoming messages from MUX`

Typ: **Warning**

MUX ruft HIP ohne einen Zeiter auf einen Speicherblock auf. Überprüfen Sie die Schnittstelle IP > MUX -> HIP!

MSG_HIP_PKTLEN_ZERO

`EventText: Packet length from MUX = zero`

Typ: **Warning**

Länge des Pakets von MUX ist 0. Informieren Sie die für IP zuständige Person über diese Nachricht.

MSG_HIP_ALLOC_MES_SI

`EventText: No allocation for message SI possible`

Typ: **Warning**

Das Senden einer Meldung von HIP an die Systemschnittstelle ist nicht möglich. Überprüfen Sie den verfügbaren Speicher!

MSG_HIP_PMBLK_ZERO

`EventText: Length of packet from Mux is zero`

Typ: **Warning**

Länge des Pakets von MUX ist 0. Informieren Sie die für IP/MUX zuständige Person über diese Nachricht.

9.2.32 SI-Events (Systemschnittstellen-Events)

MSG_SI_L2STUB_STREAM_ALREADY_OPEN

`EventText: Stream already open for device %X`

Typ: **Warning**

Das Device ist durch die `SI_open`-Prozedur bereits geöffnet worden. Überprüfen Sie MAL, um herauszufinden, warum es `SI_open` zweimal aufruft!

MSG_SI_L2STUB_COUDNT_OPEN_STREAM

`EventText: Stream couldnâ##t be opened for device %X`

Typ: **Warning**

Fehler beim Vxworks-Costream zum Öffnen eines Datenkanals für ein Device. Überprüfen Sie die maximale Anzahl von Devices und interpretieren Sie den Fehler-Code!

MSG_SI_L2STUB_ERROR_INIT_DRIVER

`EventText: Critical Error in Initializing L2 driver`

Typ: **Critical**

Die Initialisierung von L2 ist nicht möglich. Überprüfen Sie den Fehlercode in Vxworks!

MSG_SI_L2STUB_NO_CLONE

`EventText: Unsupported non-Clone open!`

Typ: **Warning**

Eine nicht unterstützte Nicht-Clone-Instanz ist geöffnet.

MSG_SI_L2STUB_OPEN_OTHER_STREAM_NOT_POSSIBLE

`EventText: Unable to open another L2 stream`

Typ: **Warning**

Überprüfen Sie den Fehlercode von Vxworks!

MSG_SI_L2STUB_UNEXPECTED_DB_TYPE

`EventText: Unexpected db_type (0x%x)"`

Typ: **Warning**

Der Meldungstyp ist für DLPI nicht erlaubt.

MSG_SI_L2STUB_NO_ALLOC

`EventText: Unable to allocb(%d)`

Typ: **Critical**

Es ist kein Speicher mehr verfügbar. Das Gateway führt einen automatischen Neustart durch. Ein SNMP-Trap wird erzeugt. Weitere Maßnahmen sind nicht erforderlich.

MSG_SI_L2STUB_PORT_NOT_OPEN

`EventText: Port has not been opened`

Typ: **Warning**

Ein Port muss geöffnet sein bevor der Transfer durchgeführt werden kann. Überprüfen Sie, warum der Port geschlossen ist!

MSG_SI_L2STUB_UNKNOWN_SOURCE_PID

`EventText: PSource PID not known (0x%x)`

Typ: **Warning**

Meldung von einer unbekannten PID. Überprüfen Sie, wer diese Meldung gesendet hat!

MSG_SI_L2STUB_UNEXPECTED_EVENT_CODE

```
EventText: Unexpected event code (%d) from SWU
```

Typ: **Warning**

Von HiPath 3000 gesendeter Event-Code ist nicht bekannt. DH in HiPath 3000 überprüfen.

9.2.33 MAGIC / Device-Manager-Events

9.2.33.1 Startup- und interne Meldungen

MSG_DEVM_NO_PROTOCOL_FOR_DEVICE

```
EventText: Device %u could not be bound to protocol %d.
Device has been taken out of service
```

Typ: **groß**

Das angegebene Device konnte keinem Protokoll zugeordnet werden und befindet sich daher 'out-of-Service'. Überprüfen und korrigieren Sie den Inhalt der Datei devmgr.txt.

MSG_DEVM_NO_PROTOCOL_FOR_DEVICE

```
EventText: Device %u could not be bound to protocol %d.
Device has been taken out of service
```

Typ: **groß**

Das angegebene Device konnte keinem Protokoll zugeordnet werden und befindet sich daher 'out-of-Service'. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

MSG_DEVM_BINDING_FAILED

```
EventText: Protocol rejected. Device '%u' will be taken out
of service
```

Typ: **groß**

Ein ungültiges Protokoll ist in der persistenten Datei angegeben. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

MSG_DEVMGR_DEVICEID_OUT_OF_RANGE

```
EventText: The current DeviceId: %d is out of range
```

Typ: **groß**

Die angegebene Device-ID befindet sich außerhalb des gültigen Bereichs. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE

```
EventText: No Device Type for %s Device available in
persistency
```

Typ: **groß**

Ungültiger Device-Typ in der persistenten Datei. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE

`EventText: No Device Type for %s Device available in persistency`

Typ: **groß**

In der persistenten Datei wurde kein Eintrag für den angegebenen Device-Typ gefunden. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

MSG_DEVMGR_CREATE_FAILED

`EventText: %s create failed`

Typ: **groß**

Eine Device-Objketinstanz der angegebenen Klasse konnte nicht erzeugt werden. Zu wenig Speicher! Starten Sie das System neu!

MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY

`EventText: Can not read %s persistency file`

Typ: **groß**

Die angegebene persistente Datei kann nicht gelesen werden. Überprüfen Sie die persistenten Dateien! Starten Sie das System neu!

MSG_DEVMGR_SCN_TASK_FAILED

`EventText: SCN Task create failed`

Typ: **groß**

Es kann keine Klasseninstanz von `SCN_TASK` erzeugt werden; der Startvorgang wurde unterbrochen. Starten Sie das System neu!

MSG_DEVMGR_INTERROR_DEVID

Typ bei den nachfolgenden Event-Texten: **groß**

`EventText: SCN Task create failed`

In der globalen Device-Tabelle konnte kein gültiger Device-Zeiger gefunden werden.

`EventText: DeviceId (%x): Got NULL pointer instead of Resource!`

Ein Null-Zeiger auf eine Ressource ist aufgetreten.

`EventText: DeviceId (%x): No container object found!`

In der globalen Tabelle wurde kein gültiger Objekt-Zeiger gefunden.

`EventText: DeviceId (%x): No protocol manager found!`

Es wurde kein gültiger Protokoll-Manager gefunden.

`EventText: DeviceId (%x): No protocolId in message!`

Aus der persistenten Datei konnte keine Protokoll-ID gelesen werden. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

`EventText: DeviceId (%x): If Table init failed, DVMGR not initialized!`

Fehler beim Systemstart. Es konnten keine If-Tabellen erzeugt werden. Starten Sie das System neu! Wenn das Problem anhält, ist ein neues APS erforderlich.

`EventText: DeviceId (%x): Startup failed, DVMGR not initialized!`

Fehler beim Systemstart. Der Device-Manager konnte nicht gestartet werden. Starten Sie das System neu! Wenn das Problem anhält, ist ein neues APS erforderlich.

`EventText: DeviceId (%x): is not a fax deviceId. Could not set fax status.`

Eine falsche Device-ID wurde erhalten.

`EventText: DeviceId (%x): Got NULL pointer !!!`

Null-Zeiger erhalten.

`EventText: DeviceId (%x): No free channel found!`

Keinen freiden Kanal gefunden.

`EventText: DeviceId (%x): Unknown Device Type!`

Unbekannten Device-Typ erhalten. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei devmgr.txt!

`EventText: DeviceId (%x): Device %d canâ##t be created!`

Device konnte nicht erzeugt werden. Für dieses Device sind keine Verbindungen möglich.

`EventText: DeviceId (%x): Insert in global Device Table failed!`

Das Einfügen in die globale Device-Tabelle schlug fehl. Dieses Device wird dem System nicht bekannt sein.

Typ bei den nachfolgendem Event-Texten: **klein**

`EventText:` DeviceId (%x): Not enough memory to create Resource object!!

Nicht genügend Speicher, um eine Ressource zu erstellen.

Typ bei den nachfolgenden Event-Texten: **Warning**

`EventText: DeviceId (%x): Amount of configured resources exceeds overall limit.`

Die Anzahl der Gesamt-Ressourcen ist kleiner als die Anzahl der Ressourcen, die diesem Device zugeordnet sind. Überprüfen Sie die Konfiguration der Ressourcen in devmgr.txt!

`EventText: DeviceId (%x): Unexpected SUSY id !!!`

Unerwartete SUSY-ID erhalten.

`EventText: DeviceId (%x): iAdmCommand: Unexpected value received`

Unerwartetes Kommando erhalten.

`EventText: DeviceId (%x): id >= MAX_RESOURCE_NUMBER!`

Falsche Ressource erhalten.

`EventText: DeviceId (%x): Wrong param from persistency file gwglobal.txt!`

Parameter der persistenten Datei konnten nicht gelesen werden. Überprüfen und korrigieren Sie den Inhalt der persistenten Datei gwglobal.txt!

`EventText: DeviceId (%x): BChannel not found in resources!`

B-Kanal konnte in den Ressourcen nicht gefunden werden.

`EventText: DeviceId (%x): Got a LOGON_TRK_IND msg for wrong device!`

Meldung für falsches Device erhalten.

`EventText: DeviceId (%x): Unknown resource state!`

Ressource befindet sich in unbekanntem Zustand.

`EventText: DeviceId (%x): Configured Trunk Channels exceed physical Limit!`

Die konfigurierten Leitungskanäle (Manager E) überschreiten die Anzahl der physikalischen B-Kanäle.

Typ bei den nachfolgenden Event-Texten: **Information**

`EventText: DeviceId (%x): Unknown AdminState! AdminState set to AStateDown`

Unbekannter Admin-Status.

`EventText: DeviceId (%x): Shutdown of SCN_Task failed! Continue with Shutdown.`

Das Beenden von `SCN_TASK` schlug fehl. Das Beenden wird jedoch fortgesetzt.

MSG_DEVMGR_INTERROR_RESID

Typ bei den nachfolgenden Event-Texten: **Warning**

`EventText: ResourceId (%x): Fax Indication received from wrong device`

Falscher Device-Typ.

`EventText: ResourceId (%x): No ASCII character defined for digit %d`

Falsche Ziffer.

`EventText: ResourceId (%x): G711TransparentChannel Indication not from SCN-side`

Falsche Anzeige.

`EventText: ResourceId (%x): State RESOURCE_IN_USE not set!`

Status lässt sich nicht ändern.

`EventText: ResourceId (%x): State RESOURCE_IDLE not set!`

Status lässt sich nicht ändern.

`EventText: ResourceId (%x): DecreaseResourceCounter() failed`

Herunterzählen des Ressourcen-Zählers schlug fehl.

`EventText: ResourceId (%x): Leg not opened`

Leg ist noch nicht geöffnet.

`EventText: ResourceId (%x): No Codecs available!`

Keinen Codec gefunden. Anrufe sind nicht möglich.

`EventText: ResourceId (%x): Codec value out of range!`

Unbekannter Codec.

`EventText: ResourceId (%x): Number of licenses out of range!`

Unbekannte Codec-Menge.

`EventText: ResourceId (%x): new state not expected!`

Unerwarteten Status erhalten.

`EventText: ResourceId (%x): Leg already in a connection`

Der eigene Leg oder der des Partners ist bereits verbunden. Der Befehl wird abgewiesen.

`EventText: ResourceId (%x): ChangeState(%d): N/A in state %s`

Der Status kann nicht geändert werden in Folge eines falschen Status.

`EventText: ResourceId (%x): Resource not in state RESOURCE_IN_USE`

Falscher Status.

`EventText: ResourceId (%x): No Dtmf tone defined for character %c`

Falsches Zeichen.

Typ bei den nachfolgenden Event-Texten: **groß**

`EventText: ResourceId (%x): GOT NULL POINTER !!!`

Null-Zeiger erhalten.

MSG_DEVMGR_INTERROR_CHNID

`EventText: ChannelId (%x): Channel out of range!`

Typ: **Warning**

Falsche Kanalnummer.

MSG_DEVMGR_MSCERROR_RESID

Typ bei den nachfolgenden Event-Texten: **Warning**

`EventText: Could not connect Legs. TIMEOUT, Faxstatus not changed from MSC`

Legs konnten wegen Timeout nicht verbunden werden.

`EventText: DCould not connect Legs; FAX_STATUS_ERROR from MSC`

Legs konnten wegen `FAX_STATUS_ERROR` von MSC nicht verbunden werden.

9.2.33.2 LEG-Management-Meldungen

MSG_DEVMGR_OPEN_LEG_FAILED

`EventText: Open of %s Leg failed; MSC Error Code %d`

Typ: **Warning**

Payload-Leg konnte nicht geöffnet werden; MSC antwortet mit angegebenem Fehler-Code.

MSG_DEVMGR_OPEN_WRONG_RES_STATE

`EventText: Open of %s Leg failed; Resource State %d`

Typ: **Warning**

Der Status der Ressource ist unerwartet. Der Status wird nicht geändert, aber gibt `false` an den Aufrufer zurück.

MSG_DEVMGR_UPDATE_LEG_FAILED

`EventText: Update of %s Leg failed; MSC Error Code %d`

Typ: **Warning**

Daten vom Payload Leg konnten nicht geändert werden; MSC antwortet mit dem angegebenen Fehler-Code.

MSG_DEVMGR_CONNECT_WRONG_LEGS

`EventText: Connect of %s Leg failed; Partner not a %s Leg`

Typ: **Warning**

Der Partner-Leg hat einen falschen Leg-Typ, weshalb die Verbindung nicht hergestellt wird.

MSG_DEVMGR_CONNECT_LEGS_FAILED

`EventText: Connect of %s Leg failed; MSC Error Code %d`

Typ: **Warning**

Die Verbindung zum angegebenen Leg schlug fehl; MSC erzeugte den angegebenen Fehler-Code.

MSG_DEVMGR_LISTEN_WRONG_RES_STATE

`EventText: ListenForConnect on %s Leg failed; State %d Mode %d`

Typ: **Warning**

Das Listening am Fax-Kanal schlug fehl, entweder wegen eines falschen Status oder eines falschen Modus.

MSG_DEVMGR_CONNECT_WRONG_RES_STATE

`EventText: Connect on %s Leg failed; State %d Mode %d`

Typ: **Warning**

Das Verbinden am Fax-Kanal schlug fehl, entweder wegen eines falschen Status oder eines falschen Modus.

MSG_DEVMGR_DISCONNECT_LEGS_FAILED

`EventText: Disconnect of %S Leg failed; MSC Error Code %d`

Typ: **Warning**

Das Trennen von Payload-Legs schlug fehl; MSC antwortet mit dem angegebenen Fehler-Code.

MSG_DEVMGR_CLOSE_LEG_FAILED

`EventText: Close of %s Leg failed; MSC Error Code %d`

Typ: **Warning**

Das ordnungsgemäße Schließen des Payload-Legs schlug fehl; es wurde aber dennoch geschlossen.

9.2.33.3 Layer2-Kommunications-Meldungen

MSG_SCN_ERROR_12_MSG

`EventText: L2 Error: %d Primitive: %d received on Device: %d`

Typ: **groß**

Layer2 hat eine Fehlermeldung gesendet; es wird lediglich geloggt.

MSG_SCN_ADD_PARAMETER_FAILED

`EventText: L2 Error: %d Primitive: %d received on Device: %d`

Typ: **groß**

Das Hinzufügen eines Parameters schlug fehl.

MSG_SCN_DEV_NOT_IN_DEVLIST

`EventText: Device %d not in devicelist of SCN_TASK`

Typ: **groß**

Das angegebene Device wurde in der Device-Liste nicht gefunden.

MSG_SCN_GET_ADMMSG_FAILED

`EventText: Reading message from admin stream failed`

Typ: **groß**

Vom Admin-Stream kann eine Meldung nicht gelesen werden.

MSG_SCN_GET_LDAPMSG_FAILED

`EventText: Reading message for device %d failed`

Typ: **groß**

Vom Admin-Stream kann eine Meldung nicht gelesen werden.

MSG_SCN_UNEXPECTED_L2_MSG

`EventText: Unexpected layer2 message on device %d`

Typ: **groß**

Layer2 hat eine unerwartete DLPI-Meldung gesendet; es wird nur geloggt.

MSG_SCN_OPERATION_ON_STREAM_FAILED

`EventText:` Operation on stream failed for device %u

Typ: **groß**

Eine Operation am angegebenen Stream schlug fehl.

MSG_SCN_POLL_FD

`EventText: Poll returned unexpected value -1`

Typ: **groß**

Das Polling schlug fehl.

MSG_SCN_OPEN_STREAM_FAILED

`EventText: Open stream failed on device %d`

Typ: **groß**

Das Öffnen eines Kommunikationspfads zu Layer2 schlug fehl. Starten Sie das System neu!

MSG_SCN_UNEXPECTED_POLL_EVENT

`EventText: Unexpected poll event on device %u`

Typ: **groß**

Für das angegebene Device wurde unerwarteter Event erhalten.

MSG_SCN_BIND_FAILED

`EventText: Bind for device: %d failed`

Typ: **groß**

Das Binden des Layer2-Kommunikationspfads schlug fehl. Starten Sie das System neu!

MSG_DEVMGR_LAYER2_SERVICE_TRAP

Typ bei den nachfolgenden Event-Texten: **Critical**

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Waiting for DL_CONNECT_IND`

Eine Meldung von der Systemschnittstelle fehlt, weshalb Layer2 nicht bereit ist. Ein SNMP-Trap wird erzeugt.

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Initiated by Layer2`

Die Systemschnittstelle nimmt Layer2 außer Betrieb. Für dieses Device sind keine Anrufe mehr möglich. Ein SNMP-Trap wird erzeugt.

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Initiated by Application/Operator`

Der Administrator nimmt Layer2 außer Betrieb. Für dieses Device sind keine Anrufe mehr möglich. Ein SNMP-Trap wird erzeugt.

Typ bei den nachfolgendem Event-Texten: **Information**

`EventText: DEVMGR DevId: %d Layer2 In-Service`

Layer2 ist bereit. Verbindungen zu diesem Device sind möglich. Ein SNMP-Trap wird erzeugt.

9.2.34 Wichtige Plattform-Software-Status-Events

MSG_ASP_INFO

Typ bei den nachfolgenden Event-Texten: **Information**

`EventText: Booting DSP module #<nr> with <DSP SW Version > from < date>`

Diese Meldung erscheint beim Starten und markiert den Beginn des Boot-Vorgangs des DSP-Moduls.

`EventText: Loading ...`

Diese Meldung erscheint beim Starten und markiert den Beginn des DSP-Software-Downloads.

`EventText: Booting DSP Modules #<nr> done`

Diese Meldung erscheint beim Starten und markiert den erfolgreichen Abschluss des Boot-Vorgangs des DSP-Moduls.

9.2.35 Major ASC-Events

MSG_ASC_ERROR

`EventText: DSP channel not initialized`

Typ: **Indeterminate**

Möglicherweise ein Konfigurationsproblem. Verifizieren Sie die ASC-Konfiguration im Gateway.

9.2.36 Major ASP-Events

MSG_ASP_ERROR

Typ bei den nachfolgenden Event-Texten: **Critical**

`EventText: Hardware-Konfiguration invalid: <error string>`

Unterschiedliche DSP-Module (DDM1, DDM2) eingesteckt. Überprüfen Sie die DSP-Module auf dem Main-Board.

`EventText: DSP Error 7,<nr>,0,0,0,0...`

Möglicherweise wurde vom LAN ein RTP-Paket mit ungültiger Länge empfangen. Erscheint nur an der Konsole.

`EventText: DSP Error 9,<nr>,0,0,0,0...`

Speicherproblem: DSP-seitig blockiert irgendetwas. Erscheint nur an der Konsole.

9.2.37 Minor ASP Events

MSG_ASP_INFO

`EventText: fec restarts because of high traffic on LAN - Restart counter <nr>`

Typ: **Information**

Diese Meldung erscheint jedes zehnte mal, wenn der FEC-Sender durch eine Kollision oder hohen Traffic blockiert ist. Einige Pakete gehen während des automatischen Neustarts von FEC verloren. Behalten Sie den LAN-Traffic im Auge!

9.2.38 IP-Filter-Events

MSG_IPF_STARTED

`EventText: IP Filter started`

Typ: **Information**

Ein IP-Filterobjekt wurde erzeugt.

MSG_IPF_STOPPED

`EventText: IP Filter stopped`

Typ: **Information**

Ein IP-Filterobjekt wurde zerstört.

MSG_IPF_ON_OFF

`EventText: IP Filter is switched %s`

Typ: **Information**

Der IP-Filter wurde aktiviert/deaktiviert.

MSG_IPF_PARAMETER

`EventText: Rule number %d: missing parameter %s`

Typ: **Critical**

Beim Lesen der angegebenen Filterregel war es nicht möglich, den angegebenen Parameter zu lesen.

9.2.39 MAC-Filter-Events

MSG_MAF_STARTED

`EventText: MAC Address Filter started`

Typ: **Information**

Ein MAC-Adress-Filterobjekt wurde erzeugt.

MSG_MAF_STOPPED

`EventText: MAC Address Filter stopped`

Typ: **Information**

Ein MAC-Adress-Filterobjekt wurde zerstört.

MSG_MAF_ON_OFF

`EventText: MAC Address Filter is switched %s`

Typ: **Information**

Der MAC-Adress-Filter wurde aktiviert/deaktiviert.

MSG_MAF_PARAMETER

`EventText: Rule number %d: missing parameter %s`

Typ: **Critical**

Beim Lesen der angegebenen Filterregel war es nicht möglich, den angegebenen Parameter zu lesen.

MSG_MAF_NO_OF_RULES

`EventText: Number of rules is bigger than the maximum of %d`

Typ: **Critical**

Die Anzahl der eingegebenen Regeln ist größer als das vordefinierte Maximum.

MSG_MAF_NETBUFFER

`EventText: IP packet seems to be corrupt`

Typ: **Critical**

Ein Fehler trat auf beim Versuch, auf einen Speicherbereich zuzugreifen, wo sich IP-Pakete befinden sollen.

MSG_MAF_ETHERNET_HEADER

`EventText: Cannot find ethernet header of IP packet`

Typ: **Critical**

Ein Fehler trat auf beim Versuch, auf den Ethernet-Header eines IP-Pakets zuzugreifen.

9.2.40 IP-Stack-Events

MSG_IPSTACK_NAT_ERROR

`EventText: CNAT Error: %s`

Typ: **Critical**

Ein kritischer Fehler trat auf bei der Netzwerk-Adressübersetzung (NAT).

MSG_IPSTACK_SOH_ERROR

`EventText: Error occurred in Socket Handler`

Typ: **Critical**

Beim Socket-Handler trat ein Fehler auf.

MSG_IPSTACK_INVALID_PARAM

`EventText: IP Stack invalid parameter %s, value %s`

Typ: **klein**

Der IP-Stack hat einen ungültigen Parameter empfangen.

9.2.41 DELIC-Events

MSG_DELIC_ERROR

`EventText: delic mailbox fatal error; reboot delic`

Typ: **Critical**

Ein Neustart ist erforderlich nach einem schweren DELIC-Mailbox-Fehler. Der Neustart wird automatisch durchgeführt. Das OpenScape 4000-System wird nicht benachrichtigt.

9.2.42 Test-Loadware-Events

MSG_TESTLW_INFO

`EventText: Info: %p`

Typ: **Information**

Information über TESTLW-Funktionen (erfolgreiche Initialisierung usw.).

MSG_TESTLW_ERROR

`EventText: Fehler (error): %p`

Typ: **groß**

Fehler bei Initialisierung, wegen Empfang einer unbekannten Meldung, bei Speicher- und Timer-Fehlern.

9.2.43 Fax-Konverter-, HDLC- und X.25-Events

MSG_FAXCONV_INFO

`EventText: Info: %p`

Typ: **Information**

Informationen zum Faxkonverter-Modul (erfolgreiche Initialisierung, Operationen usw.).

MSG_FAXCONV_ERROR

`EventText: Fehler (error): %p`

Typ bei den nachfolgendem Fehlern: **Warning**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern.

Typ bei den nachfolgendem Fehlern: **groß**

Fehler beim Öffnen des Faxkonverter-Moduls.

MSG_MSP_FAX_OVERLONG_PKT

n/a

MSG_T90_INFO

`EventText: Info: %p`

Typ: **Information**

Informationen zum T.90-Protokoll-Modul (erfolgreiche Initialisierung, Operationen usw.).

MSG_T90_ERROR

`EventText: Fehler (error): %p`

Typ: **Warning/Major**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern.

MSG_X25_INFO

`EventText: Info: %p`

Typ: **Information**

Informationen zum X.25-Protokoll-Modul (erfolgreiche Initialisierung, Operationen usw.).

MSG_X25_ERROR

`EventText: Fehler (error): %p`

Typ: **Warning/Major**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern.

MSG_X75_INFO

`EventText: Info: %p`

Typ: **Information**

Informationen zum X.75-Protokoll-Modul (erfolgreiche Initialisierung, Operationen usw.).

MSG_X75_ERROR

`EventText: Fehler (error): %p`

Typ: **Warning/Major**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern.

MSG_MSP_HDLC_INFO

`EventText: Info: %p`

Typ: **Information**

Informationen zum HDLC-Treiber (erfolgreiche Initialisierung, Operationen usw.).

MSG_MSP_HDLC_ERROR

`EventText: Fehler (error): %p`

Typ: **Warning/Major**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern und Fehlern beim Öffnen des HDLC-Treibers.

9.2.44 IP-Accounting-Events

MSG_IPACCSRV_SOCKET_ERROR

`EventText: Socket Error: %d (%s)`

Typ: **groß**

Ein schwerer Fehler trat auf an der Socket-Schnittstelle. Das Gateway führt einen automatischen Neustart durch.

MSG_IPACCSRV_MEMORY_ERROR

`EventText: Memory allocation failed`

Typ: **groß**

Die Anwendung kann nicht den erforderlichen Speicher reservieren. Das Gateway führt einen automatischen Neustart durch.

MSG_IPACCSRV_INTERNAL_ERROR

`EventText: Internal Error in IP Accounting (code: %d %s)`

Typ: **groß**

Verschiedene Fehler, z. B. wenn OAM einen Fehler-Code zurück liefert. Die Meldung wird angezeigt.

MSG_IPACCSRV_MESSAGE_ERROR

`EventText: Wrong internal message (origin: %s, code %d)`

Typ: **Warning**

Vom IP-Counting- oder IP-Accounting-Client wurde eine unbekannte Meldung erhalten. Die Meldung wird angezeigt.

MSG_IPACCSRV_MARK_REACHED

`EventText: WIP Accounting data reached upper mark, it shall be read`

Typ: **Warning**

Die obere Marke der IP-Counting-Tabelle wurde erreicht. Ein SNMP-Trap wird erzeugt. Wenn die IP-Accounting-Informationen verarbeitet werden sollen, melden Sie sich mit dem IP-Accounting-Client an.

MSG_IPACCSRV_OVERFLOW

`EventText: IP Accounting data has overflown`

Typ: **Warning**

Die obere Marke der IP-Counting-Tabelle wurde erreicht. Daten gehen verloren. Ein SNMP-Trap wird erzeugt. Wenn die IP-Accounting-Informationen verarbeitet werden sollen, melden Sie sich mit dem IP-Accounting-Client an.

MSG_IPACCSRV_LOGON

`EventText: Login of IP Accounting client: %s`

Typ: **Information**

Je nach Platzhalter %s Information darüber, ob das Logon erfolgreich war oder nicht. Die Meldung wird angezeigt. Wenn das Logon erfolglos war, überprüfen Sie die Ursache!

9.2.45 Endpunkt-Registrierungs-Handler-Events

MSG_ERH_INFORMATION

`EventText: %p`

Typ: **Information**

Wichtige ERH-Informationen. Überprüfen Sie diesen Event gegebenenfalls in Verbindung mit anderen ERH-Events.

MSG_ERH_ERROR

`EventText: %p`

Typ: **Warning**

Fehler, die während einer ERH-Operation bemerkt wurden (falls nicht von anderen Event-Klassen eingestuft). Erstellen Sie einen Trace mit ERH_REGISTRATION, ERH_ADMISSION und ERH_CONFIGURATION und Trace-Level 6, um weitere Informationen zu gewinnen.

MSG_ERH_REGISTRATION_ERROR

`EventText: %p`

Typ: **Warning**

Fehler, die während der ERH-Registrierung bemerkt wurden. Erstellen Sie einen Trace mit ERH_REGISTRATION, ERH_CONFIGURATION und Trace-Level 6, um weitere Informationen zu gewinnen. Sehr oft wird dieser Fehler durch eine fehlerhafte Konfiguration verursacht. Lesen Sie außerdem die Meldungen des Typs MSG_ERH_INFORMATION.

MSG_ERH_ADMISSION_ERROR

`EventText: %p`

Typ: **Warning**

Fehler, die während dem Aufnehmen/Lösen von Endpunkten bemerkt wurden. Erstellen Sie einen Trace mit ERH_ADMISSION und Trace-Level 6, um weitere Informationen zu gewinnen. Überprüfen Sie die Endpunkte, die nicht funktionieren.

MSG_ERH_SECURITY_DENIAL

`EventText: %p`

Typ: **Critical**

Hinweis darauf, dass der ERH eine Anforderung auf Registrierung, Ent-Registrierung, Aufnehmen oder Lösen von Endpunkten aus Sicherheitsgründen verweigert hat. Überprüfen Sie sorgfältig, ob diese Meldung durch eine fehlerhafte Konfiguration im Netzwerk hervorgerufen wurde, oder ob es sich um die Attacke eines Netzwerks-Eindringlings handelt.

MSG_ERH_SUB_OUT_OF_SERVICE

n/a

MSG_ERH_NO_LICENSE

`EventText: %p`

Typ: **Warning**

Hinweis darauf, dass keine ComScendo-Lizenzen für die Registrierung eines H.323-Endpunkts verfügbar sind. Im Lizenz-Management (Manager E) müssen mehr Lizenzen konfiguriert werden.

9.2.46 IPNCV-Events

MSG_IPNCV_SIGNALING_ERROR

`EventText: IPNCV Signaling Error: %s`

Typ: **Warning**

Software-Fehler: ungültige interne Daten entdeckt.

9.2.47 XMLUTILS-Events

MSG_XMLUTILS_ERROR

`EventText: %d`

Typ: **groß**

In der XMLUTILS-Komponente ist ein Fehler aufgetreten.

9.2.48 Fehler-Events

MSG_OSF_PCS_ERROR

`EventText: %p`

Typ: **groß**

OSF hat einen bedeutenden Fehler entdeckt.

9.2.49 LAN-Signalisierung bezogene Events - CCE

CCE_GENERAL_ERROR

`EventText: ...`

Typ: **Major, Minor, Warning, Information**

CCE-Fehler der nicht von einer Interaktion mit PSS-Speicherung ausgelöst wurde (z. B. Interaktion mit einem QDC-Client).

CCE_PSS_STORE_ERROR

`EventText: ...`

Typ: **Major, Minor, Warning, Information**

CCE-Fehler der von einer Interaktion mit PSS-Speicherung ausgelöst wurde (z. B. Interaktion mit einem QDC-Client).

9.2.50 Events für LLC-Operation

MSG_LLC_EVENT_MISSING_RESOURCE

`EventText: %p`

Typ: **Information**

Wichtige Informationen über eine LLC-Operation.

MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE

`EventText: %p`

Typ: **Critical**

Bei Fehler, die während einer LLC-Operation auftauchen (sofern sie nicht schon von anderen Event-Klassen klassifiziert wurden).

MSG_LLC_EVENT_MISSING_PARAMETER

`EventText: %p`

Typ: **Critical**

Verbindliches Element fehlt in der Meldung.

MSG_LLC_EVENT_INVALID_PARAMETER_VALUE

`EventText: %p`

Typ: **Warning**

Ungültige Meldung.

9.2.51 Client-bezogene Events

(Events der Kategorie QoS Data Collection)

QDC_SIGNALLING_DATA_ERROR

`EventText: Signaling data could not be completely retrieved for the QDC report`

Typ: **Information**

Die Signalisierungsdaten für den QDC-Report sind nicht vollständig.

QDC_MSG_QUEUE_ERROR

`EventText: QDC message queue is full.`

Typ: **groß**

QDC-Meldungsspeicher ist voll. Meldungen können verloren gehen.

QDC_SYSTEM_ERROR

`EventText: QDC software failure`

Typ: **groß**

QDC läuft nicht korrekt.

QDC_ ERROR_IN_COMMON_CLIENT

`EventText: Error in QDC Common Client: %s`

Typ: **Warning**

Allgemeine Fehlermeldung; Reason described in specific text represented instead of %s.

9.2.52 QDC-CGWA-Related Events

(Events der Kategorie QoS Data Collection)

QDC_INVALID_CONFIGURATION

`EventText: Invalid QDC configuration`

Typ: **Warning**

Der Administrator versucht eine ungültige QDC-Konfiguration zu verwenden.

QDC_PERSYSTENCY_ERROR

`EventText: QDC default configuration could not be read from the persistency`

Typ: **Warning**

Die Standard-QDC-Konfiguration konnte nicht aus dem Persistenz-Speicher ausgelesen werden.

QDC_ERROR_IN_CLIENT

`EventText: Error in QDC Client: %s`

Typ: **Warning**

Allgemeine Fehlermeldung; Fehlerursache in Klartext statt %s.

9.2.53 QDC VoIPSD Error Report Events

QDC_VOIPSD_ERROR

`EventText: Error in secure data handling: %s`

Typ: **Information**

Eine der Komponenten meldet einen Fehler bei der 'sicheren' Datenübertragung: %s

9.2.54 SIP-Events

SIP_INFORMATION

`EventText: ...`

Typ: **Major, Minor, Warning, Information**

Just informationSHT: startup/shutdown.

SIP_INVALID_PARAMETER_VALUE

`EventText: ...`

Typ: **Major, Minor, Warning**

Ein Parameterwert ist außerhalb des festgelegten Wertebereichs.

SIP_UNEXPECTED_RETURN_VALUE

`EventText: ...`

Typ: **Major, Minor, Warning**

Die aktuell aufgerufene Funktion gibt ein unerwartetes Ergebnis zurück.

SIP_INVALID_POINTER

`EventText: ...`

Typ: **Major, Minor, Warning, Information**

Ein Zeiger hat einen ungültigen Wert.

10 Anhang: WAN/LAN-Management

Die Administrierung gekoppelter Netze im WAN/LAN-Bereich ist eine technisch anspruchsvolle Aufgabe. Im Rahmen dieser Tätigkeit tauchen früher oder später Konfigurationsprobleme auf, die es schnell und effizient zu beseitigen gilt. Das in diesem Anhang vermittelte Wissen soll Ihnen dabei helfen.

10.1 Dienstprogramme zur Diagnose von TCP/IP

Um Fehler in einer TCP/IP Umgebung zu finden, die sich nicht auf eine einfache Ursache zurückführen lassen, stellt jedes Betriebsystem geeignete Werkzeuge zur Verfügung. Da jedes Betriebssystem seine eigenen Tools mit entsprechenden Parametern für die Befehle besitzt, sollen hier nur die wichtigsten Funktionen der Microsoft Betriebssysteme erläutert werden. Weitere Tools für UNIX-basierte Betriebssysteme werden in RFC 1147 ausführlich beschrieben. Spezielle Parameter sind in der Hilfe für das entsprechende Betriebssystem enthalten und können in der Regel durch Eingabe von `<Command> -?` abgefragt werden.

10.1.1 ping

Das wohl am meisten benötigte Tool ist der `ping`-Befehl. Mit diesem Befehl kann überprüft werden, ob ein Rechner im Netzwerk erreichbar ist und somit mit ihm kommuniziert werden kann. Dabei wird dem Ziel-Rechner eine ICMP-ECHO-Meldung gesendet, die an den Absender zurückgeschickt wird. Gelangt die Antwort zum sendenden Rechner zurück, so ist eine Kommunikation mit dem angegebenen Rechner möglich. Die meisten Varianten des PING-Befehls geben Statistiken über die Verbindung aus.

Syntax für Windows-Betriebssysteme:

:

`ping <Host> [<Parameter>]`

Für `<Parameter>` sind folgende Angaben möglich:

`<Host>`	Enthält die Zieladresse oder den Host-Namen des Zielrechners
`-t`	Sendet ununterbrochen Testpakete zum Rechner. Normalerweise werden nur 4 Testpakete gesendet.
`-a`	IP-Adressen werden zu Host-Namen aufgelöst.
`-n <Anzahl>`	Sendet <Anzahl> Testpakete zum Rechner.
`-l <Größe>`	Sendet Testpakete mit <Größe> Bytes
`-i <TTL>`	Anzahl Router-HOPs die für ein Paket erlaubt sind. Der Zähler wird beim Sender auf einen Startwert gesetzt und von jedem Router der das Paket weiterreicht dekrementiert.

`-w <Timeout>`	Zeit in Millisekunden, in der auf eine Antwort gewartet wird. Läuft diese Zeit ab, so erscheint eine Timeout-Meldung. Standardmäßig steht dieser Wert auf 1000 (1s). Bei langsamen Verbindungen z. B. über Modem oder GSM ist es ratsam, diesen Wert auf 5000 (5s) bzw. 10000 (10s) zu setzen. Beträgt die Antwortzeit mehr als 1s erhält man Timeout-Meldungen, obwohl eine Verbindung möglich ist.

Beispiel:

Verbindung zum lokalen Rechner überprüfen. Der eigene Rechner ist normalerweise unter der Loopback-Adresse `127.0.0.1` und dem Namen `localhost` zu erreichen.

```
C:\>ping localhost

PING wird ausgeführt für localhost [127.0.0.1] mit 32 Bytes Daten:

Antwort von 127.0.0.1: Bytes=32 Zeit<10ms TTL=128

Antwort von 127.0.0.1: Bytes=32 Zeit<10ms TTL=128

Antwort von 127.0.0.1: Bytes=32 Zeit<10ms TTL=128

Antwort von 127.0.0.1: Bytes=32 Zeit<10ms TTL=128
```

Meldungen:

Sollte der entfernte Rechner nicht antworten, so kann man anhand der Meldungen auf den Fehler schließen.

- Ungültige IP-Adresse (unknown host): Der Host-Name konnte nicht in eine gültige IP-Adresse umgewandelt werden. Diese Meldung entsteht, wenn der DNS-Server nicht erreicht werden kann oder ausgefallen ist. Diese Fehlermeldung tritt nur auf, wenn der Host mit einem Namen angesprochen wird.
- Ziel-Host nicht erreichbar (network unreachable): Es existiert keine gültige Route zum Zielsystem. Die Ziel-Adresse konnte nicht erreicht werden, da ein Gateway ausgefallen ist oder auf dem lokalen Rechner nicht richtig angegeben ist.
- Zeitüberschreitung der Anforderung (Timeout): Der Rechner verfügt über eine Route zum Zielrechner, aber bekommt keine Antwort. Die Meldung gelangt zwar zum Ziel-Host, kann aber nicht zurückgeschickt werden. Dieser Fehler ist auf ein fehlerhaftes Routing des Zielrechners zurückzuführen.

10.1.2 ipconfig

Einen schnellen Weg, die TCP/IP-Netzwerkkonfiguration abzufragen, bietet das Programm `ipconfig`. Damit lassen sich die IP-Adressen, Subnet-Masks, Gateways und Statistiken der Netzwerkkarten anzeigen. Weiterhin lassen sich über DHCP zugewiesene IP-Adressen freigeben bzw. erneuern.

Syntax für Windows-Betriebssysteme:

```
ipconfig [<Parameter>]
```

Für `<Parameter>` sind folgende Angaben möglich:

`/all`	Zeigt ausführliche Informationen der Netzwerkkonfiguration an. Diese enthalten Host-Name, verwendete DNS-Server, MAC-Adressen der jeweiligen Netzwerkadapter und DHCP Informationen.
`/release [Adapter]`	Gibt die über DHCP zugewiesene IP-Adresse am Adapter frei.
`/renew [Adapter]`	Weist dem Adapter über DHCP eine neue IP-Adresse zu.

Wird der Adapter bei den Parametern `release` und `renew` nicht angegeben, so werden alle IP-Adressen an allen über DHCP zugewiesenen Adaptern freigegeben oder neu zugewiesen.

Beispiel:

Abfrage der aktuellen Konfiguration in ausführlicher Form:

```
C:\>ipconfig /all

Windows NT IP-Konfiguration

   Host-Name ..............:  myhost.unify.de

   DNS-Server..............:  192.168.50.23

                              192.168.50.160

   Knotentyp ..............:  Broadcast

   NetBIOS-Bereichs-ID .....:

   IP-Routing aktiviert.....:  Nein

   WINS-Proxy aktiviert.....:  Nein

   NetBIOS-Auswertung mit DNS: Ja
```

```
Ethernet-Adapter El90x2:

   Beschreibung......... ...:  3Com 3C90x Ethernet
                               Adapter

   Physische Adresse........:  00-10-5A-DD-56-55,

   DHCP aktiviert...........:  Nein

   IP-Adresse..............:  192.168.129.1

   Subnet Mask.............:  255.255.255.0

   Standard-Gateway.........:
```

```
Ethernet-Adapter El90x1:
```

```
Beschreibung......... ...:  3Com 3C90x Ethernet
                            Adapter

Physische Adresse.....:  00-10-5A-37-26-B1,

DHCP aktiviert..........:  Ja

IP-Adresse.............:  192.168.14.6

Subnet Mask............:  255.255.255.0

Standard-Gateway.....:  192.168.14.1

DHCP-Server............:  192.168.11.103

Lease                       Di., 17.08.1999 08:43:30
erhalten....... ...: ...:

Lease läuft ab....... ...:  Di., 19.01.2038 04:14:07
```

10.1.3 nslookup

Eine IP-Adresse kann durch einen Host-Namen zugeordnet werden. Diese Zuweisung von Namen und IP-Adresse wird im DNS-Server (DNS = Domain Name Server) hinterlegt. Mit dem Befehl `nslookup` lassen sich die Daten abfragen, die für einen bestimmten Host im DNS-Server gespeichert sind. Durch Eingabe des Befehls `nslookup` in der MSDOS-Eingabeaufforderung versucht sich das Programm mit dem im Netzwerk hinterlegten DNS-Server zu verbinden. Wird ein Name erfragt, so liefert dieser die zugehörige IP-Adresse zurück. Wird hingegen eine IP-Adresse erfragt, so wird der Host-Name zurückgeliefert. Ist die IP-Adresse oder der Host-Name nicht im DNS-Server hinterlegt, so gibt dieser eine dementsprechende Fehlermeldung aus.

Die Meldung `Ungültige IP-Adresse` des `nslookup`-Befehls sagt aus, dass der angegebene Host-Name nicht in eine IP-Adresse umgewandelt werden konnte. Dies geschieht, wenn der DNS-Server ausgefallen ist oder der Eintrag nicht existiert. Voraussetzung dabei ist, dass die DNS-Server in der Netzwerkkonfiguration eingetragen und über das Netzwerk ansprechbar sind.

Mit `nslookup` können verschiedene Einträge (Records) des DNS-Servers abgefragt werden. Nachdem man das Programm gestartet hat, lassen sich durch folgende Einträge die dementsprechenden Daten abfragen.

`set type=<Typ>`

Für `<Typ>` sind folgende Angaben möglich:

`a`	Adressen Einträge
`any`	Alle Einträge
`mx`	Mail Exchanger Einträge
`ns`	Name Server Einträge
`soa`	Start of Authority Einträge
`hinfo`	Host Info Einträge

`axfr`	Alle Einträge einer Zone
`txt`	Text Einträge

Syntax für Windows-Betriebssysteme:

`nslookup <Host>`

`<Host>`	Enthält die Zieladresse oder den Host-Namen des Zielrechners

Beispiel:

```
C:\>nslookup localhost
Server: ns.domain.com
Adresse: 192.168.0.1
Name: localhost
Adresse: 127.0.0.1
```

Der Host 'localhost' besitzt die IP-Adresse 127.0.0.1.

10.1.4 hostname

Der Befehl `hostname` gibt den Namen des lokalen Rechners zurück. Im Gegensatz zu anderen Betriebssystemen lässt sich bei Microsoft Betriebssystemen über diesen Befehl der Host-Name nicht verändern.

Beispiel:

```
C:\>hostname
localhost
```

10.1.5 netstat

Der Befehl `netstat` dient zum Überprüfen bestehender Verbindungen, eingerichteter Routen und liefert detaillierte Statistiken und Informationen der einzelnen Netzwerkschnittstellen zurück. Die neben der Routingtabelle am meisten benötigte Funktion von `netstat` ist die Abfrage, welche Verbindungen auf dem lokalen Rechner existieren und in welchem Zustand sie sich befinden.

Syntax für Windows-Betriebssysteme:

netstat [<Parameter>] [<Intervall>]

Für `<Parameter>` sind folgende Angaben möglich:

`-a`	Zeigt alle Verbindungen an, d. h. Anwendungen, die auf eine Verbindung warten, werden ebenfalls angezeigt, z. B. ein Telnet Server.
`-e`	Zeigt die Ethernet-Statistik an
`-n`	Zeigt IP-Adressen anstatt Host-Namen an

`-p <Proto>`	Zeigt Verbindungen an, die über das Protokoll `<Proto>` laufen
`-r`	Zeigt die Routingtabelle an, die aber auch durch `route print` angezeigt wird.
`-s`	Zeigt Statistik nach Protokoll an
`<Intervall>`	Wiederholt die Anzeige nach <Intervall> Sekunden

Beispiel:

Abfrage aller Verbindungen im IP-Adressen Format (verkürzt)

```
C:\>netstat -a -n

Aktive Verbindungen

Proto  Lokale Adresse          Remote Adresse        Status
....
....
TCP    0.0.0.0:25             0.0.0.0:0             LISTENING
TCP    0.0.0.0:80             0.0.0.0:0             LISTENING
....
....
TCP    192.168.129.3:110      192.168.129.1:1037    ESTABLISHED
TCP    192.168.129.3:23       192.168.129.2:1038    ESTABLISHED
TCP    192.168.129.3:1031     192.168.129.1:80      ESTABLISHED
....
....
UDP    0.0.0.0:25             *:*
UDP    0.0.0.0:80             *:*
....
```

Mit Hilfe dieser Tabelle ist es möglich, IP-Verbindungen und deren Zustand anzuzeigen. Bevor auf dieses Beispiel näher eingegangen wird, sollen zunächst die Variablen kurz erläutert werden.

`<Proto>`	Gibt an, über welches Protokoll die Kommunikation abgewickelt wird. Dabei unterscheidet Windows nur zwischen den Protokollen TCP und UDP. Leider werden einige Server, die nur über ein einziges Protokoll laufen, sowohl als TCP- als auch als UDP-Server dargestellt. Aus diesem Grund lässt sich nicht eindeutig darauf schließen, welches Protokoll verwendet wird.
`<lokale Adresse>`	Gibt die eigene Adresse an, die eine Verbindung aufgebaut hat oder auf eine Verbindung wartet. Die lokale Adresse und die Remote-Adresse werden im Format <IP-Adresse>:<Port-Nummer> dargestellt.
`<Remote Adresse>`	Gibt die entfernte Adresse an, die eine Verbindung aufgebaut hat oder mit der man sich verbunden hat.
`<Zustand>`	

Zeigt den momentanen Zustand der Verbindungen an:

`ESTABLISHED`	Der lokale Rechner hat eine Verbindung mit einem Server aufgebaut. In diesem Fall ist der lokale Rechner ein Client.
`LISTENING`	Der lokale Rechner ist bereit eine Verbindung anzunehmen. In diesem Fall ist der lokale Rechner ein Server.
`SYN_SENT`	Der lokale Rechner signalisiert einem Server, dass er eine Verbindung aufbauen möchte.
`SYN_RECEIVED`	Der lokale Rechner, auf dem ein Server läuft, hat ein SYN_SENT Signal erhalten, d. h. ein Client möchte mit ihm eine Verbindung aufbauen.
`FIN_WAIT_1,`	Der lokale Rechner möchte die Verbindung mit einem Server beenden.
`TIME_WAIT`	Der lokale Rechner wartet auf die Bestätigung des Servers, die Verbindung zu beenden.
`CLOSE_WAIT`	Der lokale Rechner, auf dem ein Server läuft, hat ein FIN_WAIT_1 von einem Client erhalten, d. h. der Client möchte die Verbindung beenden.
`FIN_WAIT_2,`	Der lokale Rechner hat die Bestätigung vom Server erhalten die Verbindung zu beenden.
`LAST_ACK`	Der Server hat die Bestätigung gesendet, dass die Verbindung beendet wird.
`CLOSED`	Der Server hat die Bestätigung des Clients erhalten, dass die Verbindung beendet wurde.

Ein Rechner kann gleichzeitig sowohl Server als auch Client sein. Dies ist z. B. der Fall, wenn sich der lokale Rechner mit seinem eigenen Server verbindet. Dies ist durch das Loopback-Interface 127.0.0.1 möglich. Läuft z. B. ein Telnet Server auf dem lokalen Rechner, so kann durch den Befehl `telnet localhost` eine Telnet Sitzung auf dem eigenen Rechner geöffnet werden.

Um festzustellen, welche Daten aus dem obigen Beispiel gewonnen werden können, soll dies nun schrittweise erklärt werden.

Proto	Lokale Adresse	Remote Adresse	Status
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING

Die ersten beiden Einträge befinden sich im Zustand LISTENING, d. h. auf dem lokalen Rechner sind zwei Programme (Server) gestartet, die darauf warten, dass sich ein Client mit ihnen verbindet. Beide sind an die IP-Adresse 0.0.0.0 gebunden. Diese IP-Adresse sagt aus, dass der Server an alle verfügbaren Netzwerkschnittstellen gebunden ist. Ist eine einzige Netzwerkkarte installiert, hat dieser schon zwei Schnittstellen, nämlich die lokale Netzwerkkarte (192.168.129.3) und die Loopbackschnittstelle 127.0.0.1, die von Windows standardmäßig installiert wird. In diesem Beispiel laufen auf dem lokalen Rechner jeweils ein HTTP-Server (Port 80) und ein SMTP-Server (Port 25). Um festzustellen, ob die Netzwerkkarte richtig funktioniert, sollte man diese durch 'anpingen' vom lokalen Rechner aus testen, z. B. `ping 192.168.129.3`. Jede Fehlermeldung bei diesem Test stellt eine falsch konfigurierte Netzwerkschnittstelle dar. Möchte man z. B. die Verbindung zum lokalen HTTP-Server testen, so kann man dies einfach mit einem Web-Browser durch Eingabe der URL `https://127.0.0.1` oder `https://192.168.129.3` testen. Durch Eingabe von 'telnet localhost 25' oder 'telnet 192.168.129.3 25' ist es möglich, eine Verbindung zum lokalen SMTP-Server herzustellen. Dabei wird durch 25 der Port, d. h. die Anwendung angegeben.

Die nächsten drei Einträge sind aktive Verbindungen. Diese können entweder vom lokalen Rechner zu einem Remote Rechner, oder von einem Remote Rechner zum lokalen Rechner aufgebaut worden sein.

Proto	Lokale Adresse	Remote Adresse	Status
TCP	192.168.129.3:1037	192.168.129.1:110	ESTABLISHED
TCP	192.168.129.3:1038	192.168.129.2:23	ESTABLISHED
TCP	192.168.129.3:80	192.168.129.1:1039	ESTABLISHED

Damit man eine Unterscheidung zwischen ein- und ausgehenden Verbindungen treffen kann, benötigt man die Einträge, die sich im LISTENING-Zustand (Server) befinden. Dazu schaut man, ob der Port, der unter dem lokalen Rechner angegeben ist, selbst auf dem lokalen Rechner läuft. Die erste Zeile gibt den Port 1037 aus. Dieser Port läuft nicht als Server (LISTENING) auf dem lokalen Rechner (192.168.129.3). Somit muss diese Verbindung vom lokalen Rechner an einen Remote Rechner (192.168.129.1) mit dem Port 110 (POP3) angebunden sein. Mit anderen Worten holt sich der lokale Rechner gerade seine E-Mails bei einem POP3-Server ab.

Der zweite Eintrag muss auch eine ausgehende Verbindung sein, da sich dieser Port ebenfalls nicht im LISTENING-Zustand auf dem lokalen Rechner finden lässt. Der lokale Rechner hat also eine Verbindung mit dem Rechner 192.168.129.2 und dem Port 23 (Telnet) aufgebaut. Dies besagt, dass der lokale Rechner eine Telnet Sitzung auf dem Remote PC geöffnet hat.

Im dritten Eintrag passt der lokale Port 80 (HTTP) mit dem eines Servers zusammen. Der Remote Rechner 192.168.129.1 öffnet also gerade Web-Seiten auf dem lokalen Rechner.

10.1.6 nbtstat

Mit Hilfe dieses Dienstprogrammes ist es möglich, die Verbindungen, die das 'NetBIOS over TCP/IP-Protokoll' (WINS-Client(TCP/IP)) benutzen, zu überprüfen. Bei dem 'NetBIOS over TCP/IP Protokoll' wird ein NetBIOS-Paket in ein TCP/IP-Paket verpackt und auf der Gegenseite wieder ausgepackt. Dies wird benötigt, da NetBIOS nicht geroutet werden kann, so wie dies mit TCP/IP möglich ist. Da z. B. die Windows Laufwerksfreigaben nur über NetBIOS laufen, müssen diese in TCP/IP verpackt werden, um in andere physikalische Netze transportiert zu werden. Dazu legt sich Windows einen NetBIOS-Name-Cache an, der auch manuell angelegt werden kann. Dabei werden die IP-Adressen zum Rechnernamen in einer Tabelle aufgelöst. Diese Datei nennt sich `lmhosts` und steht je nach Betriebssystem im System- oder in einem darunterliegenden Verzeichnis.

Win95/98/ME:	*%systemroot%*
WinNT/2000/XP:	*%systemroot%\system32\drivers\etc*

Windows stellt in diesen Verzeichnissen diverse Beispieldateien bereit, die als Vorlage dienen und in denen der Aufbau der jeweiligen Beispieldatei erklärt ist. Diese Dateien haben die Endung *sam*. In diesem Fall heißt die Datei *lmhosts.sam*. Sollte die Datei *lmhosts* noch nicht existieren, so kann sie einfach nach *lmhosts* kopiert und editiert werden.

Syntax für Windows-Betriebssysteme:

`nbtstat [<Parameter>]`

Für `<Parameter>` sind folgende Angaben möglich:

`-a <Host-Name>`	Liefert die Namenstabelle des unter <Host-Name> angegebenen Rechners zurück
`-A<IP-Adresse>`	Liefert die Namenstabelle des unter <IP-Adresse> angegebenen Rechners zurück
`-c`	Der NetBIOS-Name-Cache wird mit NetBIOS-Namen und zugehörigen IP-Adressen aufgelistet
`-n`	Alle verwendeten lokalen NetBIOS-Namen werden aufgelistet
`-R`	Löscht den NetBIOS-Name-Cache und lädt die Datei `LMHOST` neu
`-r`	Listet die Namensauswertung der Windows Netzwerke auf
`-S`	Zeigt die Verbindungen von Client- und Server-Verbindungen in Form von IP-Adressen an.

`-s`	Zeigt die Verbindungen von Client- und Server-Verbindungen an und löst die IP-Adressen in Namen auf.

10.1.7 pathping

Dieser Befehl, der ab Windows 2000 verfügbar ist, dient zum Verfolgen von Routen und bietet neben den Features der Befehle `ping` und `tracert` weitere Informationen. Der Befehl `pathping` sendet über einen gewissen Zeitraum Datenpakete an jeden Router auf dem Pfad zu einem Ziel. Anhand der von jedem Abschnitt zurückübermittelten Datenpakete werden dann bestimmte Statistiken berechnet. Da der `pathping` den Paketverlust bei jedem Router und jeder Verbindung anzeigt, können Sie feststellen, welche Router oder Verbindungen Netzwerkprobleme verursachen..

Win 2000:	*%systemroot%\system32*

Syntax für Windows-Betriebssysteme:

`pathping [<Parameter>] Zielname`

Für `<Parameter>` sind folgende Angaben möglich:

`-n`	Legt fest, dass Adressen nicht zu Hostnamen aufgelöst werden.
`-h <Abschnitte>`	Gibt an, wie viele Abschnitte bei der Zielsuche höchstens durchlaufen werden sollen. Default-Wert ist 30.
`-c <Hostliste>`	Ermöglicht das Trennen von aufeinander folgenden Computern durch dazwischenliegende Gateways (Loose Source Route) anhand der Hostliste.
`-p <Zeitraum>`	Gibt (in Millisekunden) die Pause zwischen aufeinander folgenden ping-Befehlen an. Der Standardwert ist 250 Millisekunden (1/4 Sekunde).
`-q <Anzahl>`	Gibt die Anzahl der Abfragen an jeden PC auf dem Pfad an. Default-Wert ist 100.
`-w <Timeout>`	Gibt (in Millisekunden) an, wie lange auf die einzelnen Antworten gewartet werden muss. Der Standardwert ist 3000 Millisekunden (3 Sekunden).
`-T`	Fügt den Ping-Paketen eine Layer-2-Prioritätskennung hinzu (beispielsweise für 802.1) und sendet diese Kennung an sämtliche Netzwerkgeräte auf der Route. Auf diese Weise können Sie schnell und einfach feststellen, welche Netzwerkgeräten nicht ordnungsgemäß für die Layer-2-Priorität konfiguriert wurden. Dieser Parameter muss in Großbuchstaben angegeben werden.

`-R`	Überprüft, ob die einzelnen Netzwerkgeräte auf der Route das Resource Reservation Setup-Protokoll (RSVP) unterstützen. Mit diesem Protokoll kann der Hostcomputer eine bestimmte Bandbreite für einen Datenstrom reservieren. Dieser Parameter muss in Großbuchstaben angegeben werden.
`Zielname`	Gibt den Zielcomputer (Endpunkt) an, der entweder durch eine IP-Adresse oder einen Hostnamen gekennzeichnet ist.

10.1.8 route

Möchte man mehrere TCP/IP-Netzwerke miteinander verbinden, so muss man das Routing konfigurieren. Ohne das Routing-Verfahren käme man nicht über das lokale Netz hinaus. Beim Routing ist zu beachten, dass das Gateway, das das lokale Netzwerk mit anderen Netzwerken verbindet, nur im gleichen TCP/IP-Netzwerk liegen kann, in dem man sich selbst befindet.

Syntax für Windows-Betriebssysteme:

route <Befehl> <Ziel> <Subnetzmaske> <Gateway> [metric <Hops>] [<Parameter>]

Für `<Befehl>` sind folgende Angaben möglich:

`print`	Zeigt die aktuelle Routing-Tabelle an
`add`	Fügt eine neue Route hinzu
`löschen`	Löscht eine bestehende Route
`change`	Ändert eine bestehende Route
`<Ziel>`	Gibt den Ziel-Host oder das Ziel-Netzwerk an, welches über das <Gateway> erreichbar ist.
`<Subnet>`	Gibt die Subnet-Mask an.
`<Gateway>`	Gibt die IP-Adresse des Gateways an, über das die unter <Ziel> angegebene IP-Adresse erreicht werden kann.
`<Hops>`	Gibt die Anzahl von Gateways an, die zwischen Absender und Ziel der Daten liegen. Dieser Parameter ist nur relevant, wenn mehrere Routen zu einem Ziel existieren. Durch diesen Parameter können bestimmte Routen bevorzugt werden. Da in den meisten Fällen aber nur ein Gateway existiert, kann man hier den Wert '1' setzen.

Für `<Parameter>` sind folgende Angaben möglich:

`-f`	Löscht alle Routing-Einträge in der Routing-Tabelle

`-p`	Erstellt einen permanenten Eintrag. Dieser Parameter kann nur mit dem Befehl `add`. angegeben werden. Normalerweise werden Routen nur statisch mit dem Befehl `route` gesetzt. d. h. nach einem Neustart sind die gesetzten Routen nicht mehr vorhanden. Der Parameter `-p` macht den Eintrag permanent und ist somit auch nach einem Neustart des Betriebssystems noch vorhanden.

Beispiel 1:

Permanentes Einfügen einer Default Route

```
C:\cmd>route add 0.0.0.0 mask 0.0.0.0 192.168.0.199 -p
```

Beispiel 2:

Abfrage der Routingtabelle

```
C:\>route print

Aktive Routen:
```

Netzwerkadresse	Netzmaske	Gateway-Adresse	Schnittstelle	Nummer
0.0.0.0	0.0.0.0	192.168.128.1	192.168.128.14	
10.2.0.0	255.255.0.0	192.168.128.1	192.168.128.14	
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.128.14	255.255.255.255	127.0.0.1	127.0.0.1	1
192168128255	255.255.255.255	192.168.128.14	192.168.128.14	
224.0.0.0	224.0.0.0	192.168.128.14	192.168.128.14	
255.255.255.255	255.255.255.255	192.168.128.14	192.168.128.14	

Bei den letzten beiden Einträgen handelt es sich um Multicast- bzw. Broadcast-Einträge, die hier aber nicht näher erläutert werden sollen.

10.1.9 tracert

Der Befehl `tracert` (trace route) wird dazu benutzt, den Weg vom lokalen Rechner zum Ziel-Host zu verfolgen. Dabei gibt es alle Gateways aus, die auf dem Weg zum Ziel-Host passiert wurden.

Syntax für Windows-Betriebssysteme:

```
tracert <Host> [<Parameter>]
```

`<Host>`	Enthält die Zieladresse oder den Host-Namen des Zielrechners

Für `<Parameter>` sind folgende Angaben möglich:

`-d`	IP-Adressen werden nicht nach Namen aufgelöst

`-h <Anzahl>`	Gibt die höchstmögliche Anzahl der Gateways bis zum Ziel-Host an
`-j <Liste>`	Schlägt eine Route von zu passierenden Gateways vor
`-w <Timeout>`	Wartet <Timeout> Millisekunden auf einen Antwort

Beispiel:

```
C:\cmd>tracert localhost

Verfolgung der Route zu localhost [127.0.0.1] über maximal
30 Abschnitte:

1 <10 ms <10 ms <10 ms localhost [127.0.0.1]

Route-Verfolgung beendet.
```

10.1.10 arp

Bevor ein Paket von einem Host zu einem anderen Host geschickt werden kann, muss erst die Hardware-Adresse (MAC-Adresse) der Netzwerkkarte des Ziel-Hosts bekannt sein. Zu diesem Zweck hält sich jeder Rechner, der über das TCP/IP-Protokoll kommuniziert, eine sog. ARP-Tabelle. 'ARP' (Address Resolution Protocol) dient zum Auflösen der IP-Adresse zur Hardware-Adresse (MAC-Adresse). Vor jedem Verbindungsaufbau wird die ARP-Tabelle durchsucht, ob sich der Ziel-Host darin befindet. Ist der Rechner nicht in der Tabelle zu finden, so wird ein ARP-Request mit der IP-Adresse des Ziel-Hosts über das Netzwerk geschickt. Empfängt der Ziel-Host diese Anforderung, schickt dieser seine Hardware-Adresse an den anfordernden Rechner zurück, der diese Hardware-Adresse wiederum in seine ARP-Tabelle einträgt. Bei der nächsten Verbindung ist die Hardware-Adresse des Ziel-Hosts bekannt und kann direkt übernommen werden. Wird eine Hardware-Adresse benötigt, die außerhalb des log. TCP/IP-Netzes liegt, so wird nur die Hardware-Adresse des Routers benötigt, über den der Ziel-Host erreicht werden kann.

Syntax für Windows-Betriebssysteme:

arp <Parameter>

Für `<Parameter>` sind folgende Angaben möglich:	
a	Zeigt die ARP-Tabelle an
`-d`	Löscht einen Eintrag in der ARP-Tabelle
`-s`	Fügt einen Host-Eintrag der ARP-Tabelle hinzu

Beispiel 1:

Eintrag einer neuen MAC-Adresse in die ARP-Tabelle

```
C:\>arp -s 192.168.0.199 02-60-8c-f1-3e-6b
```

Beispiel 2:

Abfrage der ARP-Tabelle

```
C:\>arp -a
Schnittstelle: 192.168.0.1 on Interface 1
```

Internet-Adresse	Physische Adresse	Typ
192.168.0.1	00-00-5a-42-66-60	dynamisch
192.168.0.10	00-60-70-cd-59-22	dynamisch
192.168.0.199	02-60-8c-f1-3e-6b	statisch

10.1.11 Telnet

Telnet ermöglicht dem Benutzer, sich auf einem fremden Rechner einzuloggen. Dabei benutzt das Programm standardmäßig den Port 23. Möchte man sich zu einem Rechner mit einem anderen Port einloggen, so muss man zusätzlich die Portnummer angeben.

Syntax für Windows-Betriebssysteme:

telnet [<Host> [<Port>]]

<Host>	Enthält die Zieladresse oder den Host-Namen des Zielrechners
<Port>	Portnummer, die die Anwendung auf dem Zielrechner identifiziert

Beispiel:

```
C:\>telnet localhost 110
```

10.2 IP-Adressierung: Subnetze

Um der Verknappung von offiziellen IP-Adressen entgegenzuwirken und um ein IP-Netzwerk in voneinander getrennte Teilnetze zu splitten, bietet sich das Verfahren des 'Subnetting' an.

Bezogen auf die Zuteilung von offiziellen IP-Adressen bietet das Subnetting beispielsweise die Möglichkeit, mit einer vorhandenen Class A, B, C-Netzwerkadresse weitere eigenständige IP-Netzwerke zu generieren.

Bei den Netzwerken hat man sich auf verschiedene Klassen und Standardnetzwerkmasken geeinigt:

Table 27: Netzwerkklassen und Standardnetzwerkmasken

Klasse	Subnetzmaske
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Das Aufsplitten in eigenständige Subnetze bietet zudem den entscheidenden Vorteil, dass der lokale Verkehr eines Netzes in den jeweiligen Subnetzen verbleibt. Der Zugriff auf fremde Netze muss über einen Router erfolgen.

Die grundlegende Funktionsweise des Subnetting ist denkbar einfach und basiert auf der sogenannten 'Subnet-Mask'. Über diese Maske werden die Bits definiert, die innerhalb einer IP-Adresse den Netzwerk- bzw. Hostteil repräsentieren. Gesetzte Bits (1) geben den Netzwerkanteil an, während gelöschte Bits (0) den Hostanteil angeben.

Um eine Subnet-Mask besser analysieren zu können, betrachtet man diese besser im Binärformat. Als Beispiel soll die Class C Standardnetzwerkmaske 255.255.255.0 dienen.

Table 28: Beispiel einer Class C Standardnetzwerkmaske

	Netzwerk			Host
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Netzmaske	255	255	255	0
Binärformat	1111 1111	1111 1111	1111 1111	0000 0000

Bei der Subnetmask 255.255.255.0 geben die ersten 3 Bytes den Netzwerkanteil (alle Bits 1) und das letzte Byte den Hostanteil (alle Bits 0) an.

Anhand dieser Subnet-Mask entscheidet ein Host (Router, Workstation o. ä.), ob eine angesprochene IP-Adresse im eigenen Netz liegt oder nicht. Liegt der Ziel-Host nicht im gleichen Netzwerk, so werden Pakete an diese Adresse über entsprechend hinterlegte Routing-Mechanismen weitergeleitet.

Um Subnetze zu erstellen, die auf die jeweiligen Bedürfnisse zugeschnitten sind, muss vorher abgeklärt werden, wie viele Subnetze in einem klassenbasierten Netzwerk (Class A, B, C) gebildet werden sollen. Wird ein Netz aufgeteilt, entstehen immer 2n Subnetze. Dieses soll anhand eines Beispiels näher erläutert werden.

Das Class C Netzwerk 192.168.1.0 soll in 4 Subnetze geteilt werden. Standardmäßig hat ein Class C Netzwerk die Subnet-Mask 255.255.255.0. Um im binären System 4 verschiedene Kombinationen zu erhalten, benötigt man 2 Bits. Nachfolgende Tabelle zeigt die Abhängigkeit der Bitanzahl zur Anzahl der Netze.

Table 29: Bit-Anzahl in Abhängigkeit der Netzanzahl

Bits	Kombinationen	Bits	Kombinationen
1	21 = 2	17	217 = 131072
2	22 = 4	18	218 = 262144
3	23 = 8	19	219 = 524288
4	24 = 16	20	220 = 1048576
5	25 = 32	21	221 = 2097152
6	26 = 64	22	222 = 4194304

Bits	Kombinationen	Bits	Kombinationen
7	27 = 128	23	223 = 8388608
8.	28 = 256	24	224 = 16777216
9	29 = 512	25	225 = 33554432
10	210 = 1024	26	226 = 67108864
11	211 = 2048	27	227 = 134217728
12	212 = 4096	28	228 = 268435456
13	213 = 8192	29	229 = 536870912
14	214 = 16384	30	228 = 1073741824
15	215 = 32768	31	231 = 2147483648
16	216 = 65536	32	232 = 4294967296

Damit keine Lücken in den Adressbereichen entstehen, fügt man den bereits existierenden Einsen der Subnetmaske von links nach rechts weitere Einsen hinzu.

Table 30: Beispiel des Binärformats einer Subnetzmaske

Class C	**Netzwerk**			**Host**
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Netzmaske	255	255	255	0
Binärformat	1111 1111	1111 1111	1111 1111	0000 0000
Neu	**Netzwerk**			**Host**
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Binärformat	1111 1111	1111 1111	1111 1111	**11** 00 0000
Netzmaske	255	255	255	192

Rechnet man das neu entstandene Subnetz vom Binärsystem in das Dezimalsystem um, so erhält man die Subnet-Mask 255.255.255.192. Für den Netzwerkanteil stehen jetzt 26 Bits und für den Hostanteil 6 Bits zur Verfügung. Rechner, deren Netzwerkanteil gleiche Bitmuster aufweisen, können in einem physikalischen Netzwerk direkt miteinander kommunizieren. Jedes andere Netzwerk kann nur über ein Gateway erreicht werden. Betrachtet man das veränderte 4. Byte mit den beiden neuen Netzwerkbits 25 und 26, so kann man jetzt die neu entstandenen Subnetze berechnen.

Table 31: Berechnung neu entstandener Subnetze

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
0000 0000	0	192.168.1.0	192.168.1.63	1-62

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
0100 0000	64	192.168.1.64	192.168.1.127	65-126
1000 0000	128	192.168.1.128	192.168.1.191	129-190
1100 0000	192	192.168.1.192	192.168.1.255	193-254

Das eigentliche Subnetting besteht also darin, dass eine Erweiterung des Netzwerkteils einer IP-Adresse erfolgt, indem der Hostanteil entsprechend verkürzt wird. Die Anzahl der zur Verfügung stehenden Subnetze und Hosts ergeben sich durch folgende Bedingungen:

Die Anzahl der verfügbaren Host-Adressen ist weitgehend von der Länge des Hostteils der IP-Adresse abhängig. Ein 6 Bit-Hostanteil stellt – rein rechnerisch – 64 Adressen zur Verfügung. Da aber zu jedem IP-Netzwerk, also auch für ein einzelnes Subnetz, zwei reservierte Adressen gehören, verringert sich die max. Anzahl um 2 Adressen. Es handelt sich dabei um die Host-Adressen, die nur Nullen oder nur Einsen enthalten. Erstere wird für die Adressierung eines Netzwerkes verwendet, während letztere für Broadcasts im jeweiligen Netz genutzt wird.

Wie oben erwähnt werden die neuen Bits des Netzwerkanteils von links nach rechts an die bereits vorhandenen Bits angefügt. Nachfolgend soll gezeigt werden, warum dies so ist. Benutzt man z. B. die Subnet-Mask 255.255.255.3 für das Netzwerk 192.168.1.0, so liegt der Hostanteil inmitten des Netzwerkanteils.

Table 32: Hostanteil in einem Netzwerkanteil

	Netzwerk			Host	Netzwerk
Bytes	1. Byte	2. Byte	3. Byte	4. Byte	
Netzmaske	255	255	255	3	
Binärformat	1111 1111	1111 1111	1111 1111	0000 00	**11**

Mit diesem Subnet erhält man keine zusammenhängenden IP-Adressbereiche, da sich nur die Hosts in einem Netzwerk befinden, die die letzten beiden Bits gesetzt haben. Die sich daraus ergebenden Adressen sind in der nachfolgenden Tabelle aufgeführt.

Table 33: Netzwerkadressen in Abhängigkeit der letzten beiden Bit-Stellen

4. Byte	Dezima	Neue Netzwerke	Broadcast Adresse	Hostadressen
0000 00**00**	0	192.168.1.0	192.168.1.252	4,8,12,16,20,...,248
0000 00**01**	1	192.168.1.1	192.168.1.253	5,9,13,17,21,...,249
0000 00**10**	2	192.168.1.2	192.168.1.254	6,10,14,18,22,...,250
0000 00**11**	3	192.168.1.3	192.168.1.255	7,11,12,19,23,...,251

Aus den Hostadressen kann man ersehen, dass die einzelnen Hosts nicht in zusammenhängenden Bereichen liegen. Diese Art von Subnetting macht die Administration sehr unübersichtlich! Aus diesem Grund sollte diese Art von Subnetting nicht verwendet werden.

Bisher wurde gezeigt, wie man Subnetze bildet. Nachfolgend wird erläutert, wie man die IP-Adressen von Rechnern den jeweiligen Subnetzen zuordnet.

Die folgende Tabelle zeigt 4 IP-Adressen eines Netzwerkes (Class C) und ihre Verbindung zur verwendeten Subnet-Mask 255.255.255.224.

Table 34: Zuordnung von IP-Adressen zu Netzwerken der Klasse C

	Netzwerk	Host
255.255.255.224	11111111.11111111.11111111,111	00000
193.98.44.33	11000001.01100010.00101100,001	00001
193.98.44.101	11000001.01100010.00101100,011	00101
193.98.44.129	11000001.01100010.00101100,100	00001
193.98.44.61	11000001.01100010.00101100,001	11101

Die binäre Darstellung der Maske und Adressen zeigt recht deutlich, welchem Subnetz die jeweiligen IP-Adressen angehören: Adresse 1 und 4 sind im Subnetz '.32' (00100000), Adresse 2 gehört dem Subnetz '.96' (01100000) an und Adresse 3 befindet sich in Subnetz '.128' (10000000).

Legt man für das Beispiel die übliche Standard-Maske 255.255.255.0 eines Class C-Netzwerkes zugrunde, so würde die Länge des Netzwerkteils 24 Bit betragen, der Hostteil hätte eine Länge von 8 Bit. Durch die Subnet-Mask 255.255.255.224 ist der Netzwerkteil einer IP-Adresse im Netz genau 27 Bit lang, der Hostteil umfasst dementsprechend nur noch 5 Bit.

Als Referenz sind in der nachfolgenden Übersicht die meistgenutzten Masken der Class C mit den zugehörigen Netz- und Hostverteilungen aufgeführt.

Table 35: Übersicht der meistgenutzten Masken der Klasse C

Subnetzmaske	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
255.255.255.0	1	253	0	255	1 – 254
255.255.255.128	2	126	0	127	1 – 126
			128	255	129 – 254
255.255.255.192	4	62	0	63	1 – 62
			64	127	65 – 126
			128	191	129 – 190
			192	255	193 – 254

Subnetzmaske	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
255.255.255.224	8.	30	0	31	1 – 30
			32	63	33 – 62
			64	95	65 – 94
			96	127	97 – 126
			128	159	129 – 158
			160	191	161 – 190
			192	223	193 – 222
			224	255	225 – 254
255.255.255.240	16	16	0	15	1 – 14
			16	31	17 – 30
			32	47	33 – 46
			48	63	47 – 62
			64	79	65 – 78
			80	95	81 – 94
			96	111	97 – 110
			112	127	113 – 126
			128	143	129 – 142
			144	159	145 – 158
			160	175	161 – 174
			176	191	177 – 190
			192	207	193 – 206
			208	223	209 – 222
			224	239	225 – 238

Subnetzmaske	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
			240	255	241 – 254

Beispiel:

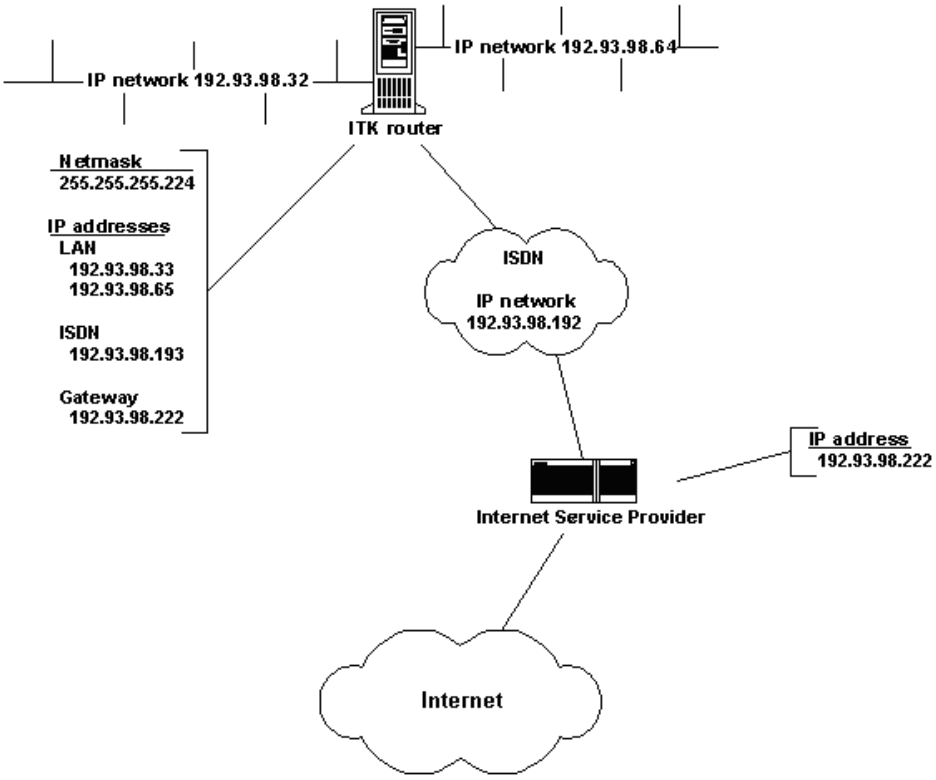
Ein LAN mit zwei Ethernet-Netzwerken soll über einen ISDN-Zugang an das Internet angeschlossen werden. Alle Stationen im lokalen Ethernet sollen Zugriff auf das Internet haben und auch aus dem Internet heraus direkt erreichbar sein. Legt man entsprechende Strukturen einer Class C-Adresse zugrunde, so müsste normalerweise für beide Ethernet-Netzwerke und für das ISDN-Netzwerk je ein komplettes Class C-Netzwerk zur Verfügung gestellt werden. Da in einem Thin Ethernet-Segment die maximale Anzahl der Stationen allerdings auf 30 begrenzt ist, wären schon dort allein 223 Host-Adressen pro Netzwerk verloren.

Genau hier setzt das Subnetting an: Durch die Verwendung einer entsprechenden Subnet-Mask kann mit nur einem Class C-Netzwerk eine vollständige Anbindung des LANs erreicht werden, und zwar ohne die erwähnte Verschwendung von Host-Adressen.

Zu diesem Zweck stellt ein Internet Service Provider ein Class C-Netzwerk mit folgenden Grunddaten zur Verfügung:

IP-Adresse Provider:	192.93.98.222
IP-Adresse Gateway:	192.93.98.222
IP-Adresse Netzwerke:	192.93.98.0
Subnetz-Maske:	255.255.255.0

Die nachfolgende Zeichnung gibt eine entsprechende Konfiguration wieder:



Anbindung des BNC-Netz an Twisted Pair zur HG 3500/3575

Als Subnetz-Maske bietet sich 255.255.255.224 an, da diese Maske 8 Subnetze mit je 30 Hosts bereitstellt. Die Anzahl der Hosts in jedem Subnetz deckt sich also mit der maximalen Anzahl von Stationen in einem Ethernet-Segment.

Aus der Darstellung ist ersichtlich, dass zwei Subnetze, hier 192.93.98.32 und 192.93.98.64, den beiden LAN-Baugruppen des ITK Router zugewiesen wurden. Eine der beiden LAN-Baugruppen erhält die IP-Adresse 192.93.98.33 und die andere 192.93.98.65. Somit können über jede Baugruppe jeweils 29 weitere Stationen mit IP-Adressen versorgt werden.

10.3 Portnummern

10.3.1 Portnummern auf OpenScape 4000 V10

Table 36: Portnummern auf OpenScape 4000 V10

Client/ Server	Protokoll	Server	Client	Anwendung
H.323 (H.225/ Q931)	TCP	1720	ephermeral	Voice over IP für Systemclients, H.323 Clients, All-Serve-und IP-Net-working
RTP/RTCP	UDP	1.500	ephermeral	

Client/ Server	Protokoll	Server	Client	Anwendung
H.245,	TCP	ephermeral	ephermeral	
Accounting Server	TCP	13042		
SNMP (Get/Set)	UDP	161		SNMP-Browser, OpenScape FM
RTCP/MSC	UDP	162		

10.4 PC- Soundeinstellungen für Voice over IP

Mit der Möglichkeit, mit Voice over IP über Netzwerke und PC zu telefonieren, sind eine Vielzahl von Konfigurationen speziell bei den Soundkarten der PCs zu beachten. Fehler, wie schlechte Sprachqualität und einseitige oder fehlende Gesprächsverbindungen, sind oft mit Veränderung von Einstellungen zu beheben. In dem folgenden Kapitel sind einige Lösungsvorschläge beschrieben, die bei der Einrichtung eines Voice-Clients helfen sollen. Diese Hilfe ist allgemein gehalten, da diese Einstellungen von der Hard- und Software und von der Umgebung, in der sich der PC befindet, abhängig sind. Eine detaillierte Beschreibung ist zu umfangreich, und deshalb unübersichtlich.

Desweiteren sind verminderte Sprachqualität nicht immer ein Zeichen von Konfigurationsfehlern oder Hard- und Software-fehlern. z. B. Knackgeräusche, d. h. kurze Unterbrechungen (verloren gegangene Sprachpakete), können auch ein Zeichen zu hoher LAN-Last sein. Durch Umstrukturierung des LAN, Umstellung auf 100BaseT oder der Einsatz von Switches kann die Qualität der Voice over IP- Verbindung verbessert werden. Wird der Audiostandard G.711 (64 kbit/s) anstelle von G.723 (5 kbit/s) verwendet, erzeugt das eine weitaus höhere LAN- Last. Bei wenigen aktiven Voice-Applikationen wird G.711 keine spürbaren LAN-Lasten verursachen. Wird aber Voice over IP intensiv genutzt, kann das bei schon ausgelasteten LANs zur Verschlechterung der Sprachqualität führen.

Konfigurationsmöglichkeiten

1) Gleichzeitiges Sprechen und Hören nicht möglich

2)
- Soundkartentreiber ist nicht vollduplexfähig, es muss ein Update installiert werden, damit die Karte vollduplexfähig wird
- Falsche Konfiguration der Voice- Applikation, vollduplex in der Software aktivieren

3) Vollduplexfähigkeit des Soundkartentreibers kann mit Netmeeting getestet werden. Unter **Optionen** #→ **Audio** besteht die Möglichkeit, vollduplex zu aktivieren/deaktivieren. Ist dieser Punkt nicht veränderbar, muss ein vollduplex-fähiger Treiber für die Soundkarte installiert werden.

4) Einseitige Sprechverbindungen

5)
- vollduplex aktiviert
- Mikrofon angeschlossen
- Mikrofon bei der Voiceapplikation aktiviert
- Einstellung der Lautstärkeregelung im PC überprüfen, unter Aufnahme **Mikrofon** aktivieren

6) Man hört sich selbst direkt oder verzögert

7)
- Einstellung der Lautstärkeregelung im PC überprüfen, unter Wiedergabe Mikrofon deaktivieren und unter Aufnahme **Wave** deaktivieren

8) Gesprächspartner hört mich nur sehr leise

9)
- Einstellung der Lautstärkeregelung im PC oder der Voice-applikation überprüfen, Lautstärke erhöhen
- wenn vorhanden, Mikrofon-Booster in der **Lautstärkeregelung** > **Wiedergabe** > **erweiterte Einstellungen** für Mikrofon aktivieren

10) Gesprächspartner hört laute Nebengeräusche (übersteuern)

11)
- wenn vorhanden, Mikrofon-Booster in der Lautstärkeregelung > Wiedergabe > erweiterte Einstellungen für Mikrofon deaktivieren
- Empfindlichkeit des Mikrofons in der Voice-Applikation verändern, z. B. bei Netmeeting unter **Optionen** > **Audio Mikrofon** 'Manuell einstellen' aktivieren und Empfindlichkeit verändern
- Aufnahmelautstärke verändern, z. B. bei Netmeeting unter **Optionen** > **Audio** den Audioassistenten starten
- Audio-Standard verändern, z. B. bei Netmeeting unter **Optionen** > **Audio** > **Erweitert von G.723 Audio-Codec** auf **G.711 Audio-Codec** stellen (auf Kosten der LAN- Last)

11 Anhang: Internetreferenzen

Die nachfolgenden Internet-Quellen bieten Original- oder Detail-Informationen zu technischen Standards, die im HG 3500/3575 zum Einsatz kommen.

11.1 RFCs

RFCs (Requests for Comments) sind 'internet-offizielle' Beschreibungen von relevanten Netz-Standards.

http://tools.ietf.org/html/rfc793

1) RFC für das TCP-Protokoll

http://tools.ietf.org/html/rfc791

RFC für das IP-Protokoll

http://tools.ietf.org/html/rfc768

RFC für das UDP-Protokoll

http://tools.ietf.org/html/rfc2616

RFC für das HTTP-Protokoll

http://tools.ietf.org/html/rfc2821

RFC für das SMTP-Protokoll

http://tools.ietf.org/html/rfc1157

RFC für das SNMP-Protokoll

http://tools.ietf.org/html/rfc959

Standard für das FTP-Protokoll

http://tools.ietf.org/html/rfc3550

RFC für das RTP-Protokoll (Real-Time Applications Protocol)

http://tools.ietf.org/html/rfc1994

PPP Challenge Handshake Authentication Protocol (CHAP)

http://tools.ietf.org/html/rfc2030

RFC für das SNTP-Protokoll

http://tools.ietf.org/html/rfc1340

RFC für 'Assigned Numbers' (Protokoll- und Portnummern)

http://tools.ietf.org/html/rfc1631

IP Network Address Translator (NAT)

http://tools.ietf.org/html/rfc3022

Traditional IP Network Address Translator (Traditional NAT)

http://tools.ietf.org/html/rfc3714

IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet

http://tools.ietf.org/html/rfc3715

IPsec-Network Address Translation (NAT) Compatibility Requirements

http://tools.ietf.org/html/rfc3762

Telefonnummern-Mapping (ENUM) Service Registration für H.323

http://tools.ietf.org/html/rfc3508

H.323 Uniform Resource Locator (URL) Scheme Registration

http://tools.ietf.org/html/rfc3709

Internet X.509 Public Key Infrastructure

http://tools.ietf.org/html/rfc3647

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

http://tools.ietf.org/html/rfc3279

Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

http://tools.ietf.org/html/rfc3280

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

http://tools.ietf.org/html/rfc3394

Advanced Encryption Standard (AES) Key Wrap Algorithm

http://tools.ietf.org/html/rfc3670

Information Model for Describing Network Device QoS Datapath Mechanisms

http://tools.ietf.org/html/rfc3644

Policy Quality of Service (QoS) Information Model

http://tools.ietf.org/html/rfc3555

MIME Type Registration of RTP Payload Formats

http://tools.ietf.org/html/rfc3387

Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network

11.2 Sonstige Quellen

http://www.protocols.com/pbook/VoIP.htm

1) Voice Over IP Reference Page

http://en.wikipedia.org/wiki/Voice_over_IP

Wikipedia-Artikel zu 'Voice over IP'.

12 Glossar

Zahlen

3DES

Tripple DES. Verbesserung des symmetrischen DES-Verschlüsselungsverfahrens, bei dem der DES-Algorithmus drei mal angewendet wird, um eine höhere Sicherheit zu erreichen.

A

AES

Der Advanced Encryption Standard ist der Nachfolger für den Verschlüsselungstandard DES bzw. 3DES.

AF

Assured Forwarding. Bandbreitensteuerndes Verfahren für Quality of Service.

ARP

Das Address Resolution Protocol ist ein Protokoll, das IP-Adressen der Schicht 3 auf Hardwareadressen (MAC-Adressen) der Schicht 2 abbildet.

B

BBAE

Breitband-Anschlusseinheit. Der BBAE bildet auf der Seite des Teilnehmeranschlusses den physikalischen Abschluss einer breitbandig genutzten Anschlussleitung. Er trennt das Anbieternetz von der Anschlussverkabelung beim Teilnehmer und bereitet die Signale für die Übermittlung über den jeweiligen Verbindungsabschnitt auf. Bei DSL-Anschlüssen beinhaltet der BBAE meist auch den Splitter, der das Breitband- und Schmalbandsignal voneinander trennt bzw. wieder zusammenführt.

B-Kanal

Ein ISDN-Nutzdatenkanal ('bearer channel') mit einer Kapazität von 64 kbit/s.

Bandbreite

Die Bandbreite eines Kommunikationskanals ist seine Kapazität, Daten zu übertragen.

Boot

'Boot' bezieht sich auf den Startvorgang. Das Boot-ROM enthält den Startcode, âbootenâ ist ein anderer Ausdruck für âstartenâ.

C

CA

Certification Authority. Vertrauenswürdige Institution zur Ausstellung von Zertifikaten.

CAPI

Common ISDN Application Interface. Wichtige Eigenschaften der CAPI-Schnittstelle sind die Unterstützung mehrerer B-Kanäle für Daten und Sprache, die Behandlung des B-Kanal-Protokolls zur Verbindungssteuerung, die Auswahl verschiedener Services, die Unterstützung mehrerer logischer Verbindungen über eine physikalische Verbindung, die Unterstüzung mehrerer Anwendungen,

die Verwendung mehrerer Kommunikationsprotokolle sowie die Unterstützung eines oder mehrerer Basisanschlüsse oder Primärmultiplexanschlüsse.

CHAP

Challenge Handshake Authentication Protocol. Die Authentifizierung wird bei CHAP vom Host gesteuert. Hat sich der Client eingewählt, wird er vom Host zur Authentifizierung aufgefordert. Die Kombination aus Benutzername und Passwort zur Authentifizierung wird vom Client per MD5 verschlüsselt übertragen.

CLI

Command Line Interface. Oberbegriff für Kommandozeilen und Shells, Terminal-Emulationen usw.

CLIR

Calling Line Identification Restriction (Rufnummernunterdrückung). ISDN-Leistungsmerkmal.

Codec

Codecs konvertieren analoge Audio- oder Videodaten in digitale Form (kodieren) und wieder zurück in eine analoge Form (dekodieren).

CorNet-NQ

CorNet NQ (von 'Corporate Networking') ist ein proprietäres Signalisierungsprotokoll. CorNet-NQ ist eine Übermenge von CorNet N, die QSIG unterstützt.

D

D-Kanal

Ein D-Kanal ist ein ISDN-Signalisierungskanal der Gesprächssteuerinformationen übermittelt.

DES

Data Encryption Standard. Herkömmliches Ver- und Entschlüsselungsverfahren mit symmetrischem Algorithmus, d.h. zur Ver- und Entschlüsselung wird derselbe Schlüssel verwendet. Die Blockgröße beträgt 64 Bits, d.h. ein 64-Bit-Block Klartext wird in einen 64-Bit-Block Chiffretext transformiert. Auch der Schlüssel, der diese Transformation kontrolliert, besitzt 64 Bits. Jedoch stehen dem Benutzer von diesen 64 Bits nur 56 Bits zur Verfügung; die übrigen 8 Bits (jeweils ein Bit aus jedem Byte) werden zum Paritäts-Check benötigt.

DID

Abkürzung für 'Direct Inward Dialing'. DID ist eine Methode, um eingehende Anrufe direkt an H.323-Endpunkte weiterzuleiten.

DLS

Der DLS (Deployment Service) ist eine OpenScape Management Anwendung zum Administrieren von Workpoints (optiPoint-Telefone und optiClient-Installationen) in OpenScape- und nicht-OpenScape-Netzwerken.

DLI

DLI ist die Abkürzung für DLS Interface.

DMA

Direct Memory Access. Die DMA-Technik erlaubt an PCs angeschlossenen Peripheriegeräten wie Netzwerkkarte oder Soundkarte, ohne Umweg über die CPU direkt miteinander zu kommunizieren. Der Vorteil der DMA-Technik ist die schnellere Datenübertragung bei gleichzeitiger Entlastung des Prozessors.

DMC

Direct Media Connection. Zur Unterstützung des Leistungsmerkmals 'Payload Switching' wird in der OpenScape für VoIP (Voice over IP)-Verbindungen das Leistungsmerkmal DMC

verwendet.

Die Payload (Sprachkanal) einer OpenScape-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 OpenScape-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

DNS

Domain Name System. Das DNS ist eine auf viele Internet-Hosts verteilte Datenbank, die für das korrekte Routing nach Domain-Namen verantwortlich ist. DNS leistet die Zuordnung von Domain-Namen an IP-Adressen.

DSA

Digital Signature Algorithm, ein Verschlüsselungsalgorithmus. DSA arbeitet mit einer variablen Schlüssellänge zwischen 512 und höchstens 1024 Bit.

DSL

Digital Subscriber Line. Die DSL-Technik ermöglicht es, über herkömmliche Telefonleitungen die Datenübertragung wesentlich zu beschleunigen und bietet sich somit vor allem für die schnelle Internetnutzung an. DSL-Anschlüsse werden vor allem mit den Technologien Asymmetric DSL (ADSL) und Single Pair DSL (SDSL) angeboten. Das wesentlich verbreitetere ADSL überträgt die Internetdaten im vorhandenen Telefonnetz oberhalb der Telefoniefrequenzen zwischen 138 und 1.104 kHz. ADSL ist beispielsweise auch die Basis für das T-DSL-Angebot der Deutschen Telekom AG.

DSP

Das HG 3500/3575 ist mit DSP-Modulen (DSP – digitaler Signalprozessor) ausgestattet. Ein DSP stellt zwei VoIP-Kanäle zur Verfügung.

DTMF

Abkürzung für 'Dual-tone multifrequency'. DTMF ist das Mehrfrequenz-Signalverfahren für die Übermittlung von Telefonnummern.

E

E-DSS1

Abkürzung für 'European Digital Subscriber System No. 1'. E-DSS1 ist das ISDN-Übertragungsprotokoll, das normalerweise in Europa verwendet wird.

EF

Expedited Forwarded. Bandbreitensteuerndes Verfahren für Quality of Service.

Endpunkt

Ein Endpunkt ist eine H.323-Komponente, die Gespräche initiieren oder empfangen kann. Informationsströme beginnen oder enden hier. Beispiele sind Clients, Gateways oder MCUs.

F

FTP

File Transfer Protocol. Plattformunabhängiges, auf TCP/IP basierendes Netzwerkprotokoll zur Übertragung von Dateien zwischen einem Client und einem Server (Download und Upload) und für einfache Dateioperationen auf dem Server.

G

G.711

G.711 ist ein Standard der ITU (International Telecommunication Union) für Sprachcodecs für eine Datenrate von 64 kbit/s.

G.723.1

G.723.1 ist ein Standard der ITU (International Telecommunication Union) für Sprachcodecs für Datenraten von 5,3 und 6,3 kbit/s.

G.729

G.729 ist eine Gruppe von Standards der ITU (International Telecommunication Union) für Sprachcodecs für Datenraten von 8 kbit/s.

Gatekeeper

Ein Gatekeeper ist eine H.323-Komponente, die Adresskonvertierung- und Zugangskontrolldienste für Endpunkte in einem H.323-Netz bereitstellt.

Gateway

Ein Gateway ist eine H.323-Komponente, die H.323-Endpunkte in einem IP-Netz mit Telefonen im öffentlichen Telefonnetz verbindet. Es übersetzt zwischen H.323- und ISDN-Protokollen.

GSM

Global System for Mobile Communications. Standard für den digitalen Mobilfunk, der auch die technische Grundlage des deutschen D- und E-Mobilfunknetzes ist.

GW

Abkürzung für 'Gateway'.

H

H.323

H.323 ist eine Gruppe von Standards, die die Übertragung von Gesprächs- und Faxdaten in paketorientierten Netzen wie IP-Netzen beschreibt. Diese Standards sind in der H.323-Reihe von Empfehlungen der ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) niedergelegt.

HFA

HiPath Feature Access.

HTML

Hypertext Markup Language. Standard zur Darstellung von Webseiten, entwickelt vom W3-Konsortium, das für Standardisierungsfragen im World Wide Web zuständig ist.

HTTP

Hypertext Transfer Protocol. Plattformunabhängiges, auf TCP/IP basierendes Netzwerkprotokoll für die Datenübertragungen im World Wide Web.

HTTPS

Hypertext Transfer Protocol Secure. Im Gegensatz zu HTTP werden alle Daten verschlüsselt übertragen.

I

IKE

Internet Key Exchange Protokoll. Verfahren zum Aufbau sicherer, authentifizierter Verbindungen. IKE unterscheidet Modes, in denen Schlüssel ausgetauscht werden. In der ersten Phase wird eine sichere, authentifizierte Verbindung aufgebaut. In der zweiten Phase werden die in den verschiedenen Protokollen benötigten Schlüssel ausgetauscht, wobei in der Regel einzelne Schlüssel (Verschlüsselung, Hashes) von einem Masterschlüssel abgeleitet werden.

ILS

Internet Locator Service. Verzeichnis-Service, der vor allem von dem Microsoft-Produkt NetMeeting verwendet wird.

IP-Adresse

Eine IP-Adresse (IP – Internet Protocol) ist eine Gruppe von vier Zahlen, die ein Gerät identifizieren. Jede Zahl kann Werte zwischen 0 und 255 annehmen.

ISDN

Abkürzung für 'Integrated Services Digital Network'. ISDN ist ein vollständig digitales öffentliches Telefonnetz.

IVR

Abkürzung für 'Interactive Voice Response'. IVR ist eine Verfahren für die Weiterleitung von Gesprächen, wenn eine einzelne Leitung nicht über Nummern zur direkten Anwahl von H.323-Endpunkten verfügt. Das HG 3500/3575 unterstützt IVR nicht.

L

LAN

Abkürzung für 'local area network'. Ein lokales Netz (LAN) verbindet PCs innerhalb eines Betriebs.

LCP

Link Control Protocol. Das LCP wird zu Aufbau, Konfiguration, Test und Abbau einer PPP-Verbindung verwendet. Der Verbindungsaufbau läuft in mehreren Phasen ab. Zuerst werden die Parameter der Verbindung ausgehandelt, unter anderem, welche Authentifizierung (PAP, CHAP) durchgeführt werden soll.

LCS

Abkürzung für 'Life Communications Server'. Live Communications Server ist die neue Instant Messaging-Lösung für Ihr Unternehmen und eine erweiterbare Echtzeit-Kommunikationsplattform von Microsoft.

M

MAL

Abkürzung für 'Magic Adaption Layer' . Ist die Schicht zwischen Applikation und Plattform.

MCU

Abkürzung für 'Multipoint Controller Unit'. MCUs werden für Audio- und Videogespräche mit mehreren Teilnehmern verwendet. Sie zentralisieren die Datenverteilung und kombinieren Sprache und Video.

MD5

Message Digest-Algorithmus, der aus einem beliebig langen Text eine 128-Bit lange digitale Unterschrift erzeugen kann. Mit Hilfe der digitalen Signatur lässt sich erkennen, ob der Text nachträglich verändert wurde. MD5 wird daher als Authentifizierungsverfahren eingesetzt.

MIB

Abkürzung für 'Management Information Base'. Eine MIB fasst Informationen und Parameter eines Netzwerkgeräts zusammen. Sie ist für die Verwaltung über SNMP erforderlich.

MFV

Mehrfrequenzwahlverfahren, auch Tonwahlverfahren genannt. Verfahren zur Übermittlung von Rufnummern und anderen Daten. Jeder Taste eines Endgerätes sind dabei zwei Frequenzen zugeordnet. Beim Druck auf eine Taste wird aus den beiden Frequenzen, die ihr zugeordnet sind, ein Ton erzeugt. Das Wählen einer Rufnummer durch einen Teilnehmer erzeugt somit eine Folge von auf Mischfrequenzen basierenden Tönen.

MoH

Music on Hold. Eine Melodie oder auch ein Ansagetext, die/den der wartende Teilnehmer hört, wenn eine Verbindung innerhalb einer Telekommunikations-Anlage gehalten oder weitervermittelt wird.

MPPC

Microsoft Point-to-Point-Compression. Datenkompressionsverfahren, das zur Beschleunigung bei Datenübertragungen eingesetzt wird.

MSC

Abkürzung für 'Media Stream Control'. Die Medienstromsteuerung (MSC) überwacht und verwaltet die Medienströme, die durch das HG 3500/3575 geleitet werden. Sie sorgt für die Übermittlung von Mediendaten zwischen LAN und ISDN.

Multicast

Multicast bezeichnet die gleichzeitige Datenübertragung von einer Quelle zu mehreren Empfängern in Netzen.

N

NAT

Network Adress Translation. Verfahren, bei dem private IP-Adressen auf öffentliche IP-Adressen abgebildet werden. NAT ist notwendig, weil öffentliche IP-Adressen immer knapper werden. NAT dient jedoch auch der

Datensicherheit, weil die interne Struktur eines LAN nach außen hin verborgen bleibt

NTBA

Netzabschlußadapter. Ist bei einem ISDN-Basisanschluß für die Umsetzung der Uk0-Schnittstelle (national) auf den S0-Bus (international) zuständig.

NTBBA

Network Termination Broadband Access. Der NTBBA bildet am DSL-Teilnehmeranschluss den Netzwerkabschluss für den breitbandigen Signalanteil. Bei ADSL-Anschlüssen übernimmt diese Funktion der ADSL-Controller bzw. das ADSL-Modem. Der ADSL-Controller setzt das ADSL-Signal von der Netzschnittstelle auf eine für den PC geeigneten meist hardwarespezifischen Nutzerschnittstelle um.

O

OAM

Operation, Administration, and Maintenance. Unter OAM sind alle Einrichtungen zu verstehen, die dem Betrieb, der Administration und der Wartung von Netzen dienen.

OSPF

Open Shortest Path First. ein von der IETF entwickeltes Routing-Protokoll. Es ist im RFC 1247 festgelegt und basiert auf dem von Edsger Dijkstra entwickelten Algorithmus "Shortest Path First".

P

PAP

Password Authentication Protocol. Verfahren zur Authentifizierung über das Point-to-Point Protocol, beschrieben im RFC 1334. Bei PAP wird das Passwort für die Authentifizierung im Gegensatz zu CHAP im Klartext übertragen.

PBX

Abkürzung für 'Private Branch Exchange'. Eine PBX ist eine Nebenstellenanlage.

PCM

Physical Connection Management. Gehört zu den funktionalen Blöcken des Verbindungs-Management (CMT) im FDDI-Ring.

PKI

Public Key Infrastructure. Umgebung, in der Services zur Verschlüsselung und digitalen Signatur auf Basis von Public-Key-Verfahren bereitgestellt werden. Bei dieser Sicherheitsstruktur wird der öffentliche Schlüssel eines Zertifikatnehmers (ZN) mit den entsprechenden Identifikationsmerkmalen durch eine digitale Signatur von einer Zertifizierungsinstanz (CA) autorisiert. Der Einsatz von PKI bietet eine vertrauenswürdige Netzwerkumgebung, in der Kommunikation vor unberechtigtem Zugriff durch Verschlüsselung geschützt und die Authentizität des Kommunikationspartners durch die digitale Signatur gewährleistet ist.

PPP

Point to Point Protocol. Protokoll zum Verbindungsaufbau über Wählleitungen (zumeist über Modem oder ISDN). Es ermöglicht die Übertragung verschiedenster Netzwerkprotokolle, unter anderem das IP-Protokoll des Internet.

PPPoE

PPP over Ethernet. Nutzung des Netzwerkprotokolls PPP über eine Ethernet-Verbindung. PPPoE wird heute bei ADSL-Anschlüssen in Deutschland verwendet.

PPTP

Point-to-Point Tunneling Protocol. Microsoft-Protokoll zum Aufbau eines Virtual Private Network (VPN); es ermöglicht das Tunneln des PPP durch ein IP-Netzwerk.

PSTN

Abkürzung für 'Public Switched Telephone Network'. PSTN ist das weltweite öffentliche Telefonnetz.

PRI

Abkürzung für 'Primary Rate Interface'. Ein PRI ist eine ISDN-Schnittstelle, die aus 23 (TS1) oder 30 (TS2) B-Kanälen mit einer Kapazität von je 64 kbit/s und einem D-Kanal mit einer Kapazität von 16 kbit/s besteht.

Q

Q.931

Q.931 ist ein Anruf-Signalisierungsprotokoll für den Aufbau und die Beendigung von Gesprächen.

QCU

Abkürzung für 'QoS Monitoring Control Unit'.

QDC

Abkürzung für 'Quality of Service Data Collection'.

Mit dem OpenScape IP-Service QDC steht ein Tool zur Verfügung, das Daten von OpenScape-Produkten sammelt, um diese auf Sprach- und Netzwerk-Qualität zu analysieren.

QSIG

QSIG ist ein Protokoll für das Vernetzen von Knoten, das von der ITU-T (International Telecommunication Union – Telecommunication Standardization Sector) adaptiert wurde. Mithilfe von QSIG können Nebenstellenanlagen verschiedener Hersteller verbunden werden.

QoS

Quality of Service. Priorisierung von IP-Datenpaketen anhand bestimmter Merkmale und Eigenschaften. Dadurch ist es möglich, z.B. Sprachübertragungen via IP (VoIP), die einen verzögerungsfreien und kontinuierlichen Datenstrom benötigen, stärker zu bevorzugen als Downloads von Fileservern oder Aufrufe von Webseiten.

R

RAS

Registration/Admission/Status ist ein Protokoll, dass die Signalisierung zwischen Client und Gateway im Bereich der automatischen Erkennung und der Registrierung regelt.

RIP

Das Route Information Protocol erzeugt und pflegt automatisch Netzwerkrouten zwischen Routern, die dieses Protokoll unterstützen.

Router

Ein Router ist eine Netzwerkkomponente, die Teilnetze verbindet und Pakete zwischen ihnen überträgt.

RSA

Das RSA-Kryptosystem ist ein asymmetrisches Kryptosystem, d.h. es verwendet verschiedene Schlüssel zum Ver- und Entschlüsseln. Es ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt.

RTP

Das Real-Time Transport Protocol legt die Übertragung von Echtzeitaudio- und -videopaketen von einem Endpunkt zu einem oder mehreren anderen Endpunkten fest.

S

SCN

Abkürzung für 'Swiched Circuit Network'. Leitungsvermittelndes Netzwerk, das alle digitalen Telefon- und Mobilfunknetze sowie und analoge Telefoneinrichtungen über digitale Vermittlungsstellen umfasst.

SHA1

Secure Hash Algorithmus. Dieser generiert aus einem String einen 160 Bit langen, eindeutigen Hash. Es handelt sich um eine Einwegverschlüsselung, d. h. aus dem Hash ist der verschlüsselte String nicht mehr ermittelbar.

SIP

Abkürzung für 'Session Initiation Protocol'. Das SIP ist ein Netzwerkprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern. Das Protokoll wird in den RFC 3261 spezifiziert.

SMTP

Simple Mail Transfer Protocol. Netzwerkübertragungsprotokoll zum Versenden von E-Mails.

SNMP

Simple Network Management Protocol. Das Protokoll dient der Verwaltung und Überwachung von Netzelementen, die überwiegend aus dem LAN-Bereich stammen (z.B. Router, Server, etc). SNMP überträgt und verändert Managementinformationen und Alarme. In LANs kann ein spezieller SNMP-Management-Server diese Management-Informationen sammeln und auswerten, damit der Netzadministrator die Übersicht über die wichtigsten Ereignisse im LAN behält.

SNTP

Simple Network Time Protcol. Protokoll für die Übertragung einer offiziellen Uhrzeit in Netzwerken und im Internet. Das SNTP-Protokoll zeichnet sich durch Einfachheit aus und hat eine Ungenauigkeit von mehreren hundert Millisekunden. Es ist definiert im RFC 1769. Die erweiterte Variante heißt NTP.

SRTP

Abkürzung für 'Secure Real-Time Transport Protocol'.

SSL

Secure Socket Layer. Übertragungsprotokoll, mit dem verschlüsselte Kommunikation möglich ist. Der Vorteil des SSL-Protokolls ist die Möglichkeit, jedes höhere Protokoll auf Basis des SSL Protokolls zu implementieren. Damit ist eine Unabhängigkeit von Applikationen und Systemen gewährleistet. SSL verschlüsselt mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.

STAC

Datenkompressionsverfahren, das zur Beschleunigung bei Datenübertragungen eingesetzt wird. Das sogenannte PPP Stac LZS Compression Protocol, beschrieben in RFC 1974, ist ein Konkurrenzverfahren zu MPPC.

T

T.30

T.30 ist ein Standard der ITU für Faxübertragungen. Er spezifiziert die Funktionen innerhalb der ersten drei Schichten für die Realisierung des Telefax-Gruppe-3-Dienstes.

T.38

T.38 ist ein Standard der ITU für Faxübertragungen. Er legt die Kommunkation von Gruppe-3-Faxgeräten über IP-Netze fest.

TCP

Transmission Control Protocol. TCP stellt einen virtuellen Kanal zwischen zwei Rechnern (genauer: Endpunkten zwischen 2 Anwendungen auf diesen Rechnern) her. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP setzt in den meisten Fällen auf das IP-Protokoll auf. Es ist in Schicht 4 des OSI-Netzwerkschichtenmodells angesiedelt.

TFTP

Trivial File Transfer Protocol, beschrieben in RFC 783. Dieses Protokoll kennt keine Authentisierung von Benutzern, keinen Verzeichniswechsel und keine Verzeichnis-Listings. Es dient ausschließlich dem direkten Down- und Upload von Dateien mit get- und put-Befehlen.

TLS

Abkürzung für 'Transport Layer Security' oder Secure Sockets Layer (SSL) ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS ist die standardisierte Weiterentwicklung von SSL 3.0.

U

UDP

User Datagram Protocol. Das User-Datagram-Protokoll (UDP) unterstützt den verbindungslosen Datenaustausch zwischen Rechnern. Das UDP wurde definiert, um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme zu versenden und damit die Anforderungen transaktionsorientierten Verkehrs zu erfüllen. UDP baut direkt auf dem darunter liegenden IP-Protokoll auf. UDP hat einen minimalen Protokollmechanismus und garantiert weder die Ablieferung eines Datagrammes beim Zielpartner, noch sind Vorkehrungen gegen eine Duplizierung oder eine Reihenfolgevertauschung getroffen. Der Funktionsumfang des UDP-Protokolls beschränkt sich auf den Transportdienst, dem Multiplexen von Verbindungen und der Fehlerbehandlung.

URL

Uniform Resource Locator. Adressierungsform für Internet-Dateien, die vor allem innerhalb des World Wide Web (WWW) zur Anwendung kommt. Das URL-Format macht eine eindeutige Bezeichnung aller Dokumente im Internet möglich, es beschreibt die Adresse eines Dokuments oder Objekts, das von einem WWW-Browser gelesen werden kann.

UTC

Universal Time Coordinated. Gilt als Weltzeit und löst damit die Greenwich Mean Time (GMT) ab. Bei der UTC-Zeit handelt sich um eine Referenzzeit, die als globaler Standard benutzt wird. Als Bezugszeit benutzt die koordinierte Weltzeit die internationale Atomzeit (TAI). Sie ist mit dieser identisch bis auf die eventuell Ende Juni und/oder Dezember eingefügten Schaltsekunden. Der Bezugspunkt für die koordinierte Weltzeit (UTC) ist der Längengrad von 0 Grad.

V

VCAPI

Virtual CAPI. VCAPI bietet die Möglichkeit, entfernte Rechner mittels ISDN-spezifischen Protokollen (z.B. Euro-Filetransfer) zu erreichen.

VoIP

Das Voice over Internet Protocol (VoIP) regelt Telefongespräche über IP-Netze.

W

WAN

Wide Area Network. Unter einem WAN versteht man ein Netzwerk, das über weite Strecken mehrere LANs verbindet. Zum Beispiel ein Netzwerk, das mehrere Filialen einer Firma an unterschiedlichen Standorten verbindet.

WBM

Web Based Management. Möglichkeit, PCs und Telekommunikations- Hard- und Software zu über einen Web-Browser zu konfigurieren. Es wird dazu keine spezifische, lokal zu installierende Software benötigt. Die Software ist als Web-Applikation realisiert und lässt sich über HTTP oder HTTPS aufrufen.

X

XML

Extensible Markup Language. Vom W3-Konsortium entwickelter Standard zur Definition von Auszeichnungssprachen. Bekannte, mit XML definierte Auszeichnunssprachen sind XHTML, SVG und WML.

XSL

Extensible Stylesheet Language. Vom W3-Konsortium entwickelter Standard, der das Formatieren und (in der Komponente XSLT) das Konvertieren von XML-basierten Auszeichnungssprachen in andere Formate ermöglicht.

Index

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z