A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 V10R1

HG 3500 on STMIX or STMIY

08/2024

A31003-H31A0-M102-07-00A9

Mitel

Notices

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

Trademarks

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

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 Einführung

Dieses Dokument beschreibt die Konfiguration des Gateways HG 3500 auf STMIX sowie die dafür verfügbaren Konfigurationstools.

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

- Die Zielgruppe für dieses Handbuch (siehe Abschnitt 1.1, "Zielgruppe")
- Die Inhalte der einzelnen Handbuchkapitel (siehe Abschnitt 1.2, "Inhalt dieses Buches")
- Wichtiger Hinweis für den Internet Explorer (siehe Abschnitt 1.3, "Hinweis zu Internet Explorer")
- Die verwendeten typografischen Konventionen (siehe Abschnitt 1.4, "Verwendete Konventionen")

1.1 Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die für die Konfiguration des HG 3500 auf STMIX 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 des Gateways HG 3500 auf STMIX
- Konfiguration der VoIP-Funktionen für das Gateway HG 3500 auf STMIX
- Einrichtung und kundenspezifische Konfiguration der Datenkommunikationsparameter auf dem Gateway HG 3500 auf STMIX

1.2 Inhalt dieses Buches

Dieses Handbuch enthält eine vollständige Beschreibung der Verwaltungsoptionen für das Gateway HG 3500 auf STMIX Gateway und Hintergrundinformationen zu ausgewählten Themen.

Es erläutert die Administration des Gateways HG 3500 auf STMIX nach dessen Installation in einem Baugruppenträger.

Weitere Informationen zum Gateway HG 3500 auf STMIX finden im OpenScape 4000 V8 Servicehandbuch.

Die nachfolgenden Kapitel enthalten eine systematische Beschreibung der WBM-Benutzeroberfläche zur Konfiguration und Administration des Gateways HG 3500 auf STMIX.

1.3 Hinweis zu Internet Explorer

Wichtig: Wenn Sie Änderungen an den Internet Explorer Sicherheitseinstellungen für eine WBM-Seite vorgenommen haben (z.B.: die Seite den Trusted Sites hinzugefügt), so 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:

Tabelle 1: Typographische Konventionen

Konvention	Beispiel
`Courier`	Eingabe und Ausgabe Beispiel: `LOCAL` als Dateiname eingeben `Befehl nicht gefunden`
Kursiv	Variable Beispiel: *Name* kann bis zu acht Zeichen lang sein
Kursiv	Zeigt Elemente der Benutzeroberfläche an Beispiel: Klicken Sie auf die Schaltfläche *OK* Wählen Sie *Schließen* aus dem *Dateimenü.*
Fett	Besondere Hervorhebung 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 alle Konfigurationsdaten verloren gehen und eine automatische Wiederherstellung der IP-Trunking-Verbindung wäre unmöglich. 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 des STMIX-Gateways. Das WBM für STMIX besteht aus zwei Teilen: HG 3500 auf STMIX â“ SIP/IPDA und HG 3500 auf STMIX â“ HFA.

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 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*
  – Der Modus Kompatibilitätsansicht muss beim WBM von HG 3500 auf STMIX deaktiviert werden: Extras -> Kompatibilitätsansicht

  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.

> **Wichtig:** Bei Nichterreichbarkeit eines auf dem Administrations-PC konfigurierten DNS-Servers benötigt das Laden von Applets über die WBM-Benutzeroberfläche wesentlich mehr Zeit. Wenn dieses Problem bei Ihnen auftritt, sollten sie in den Netzwerkeinstellungen des Administrations-PCs den konfigurierten DNS-Server überprüfen. Entfernen Sie nicht erreichbare DNS-Server oder tragen Sie erreichbare Server ein.

Erstkonfiguration

Dieses Kapitel beschreibt die Erstkonfiguration des Gateways.

Die Grundkonfiguration des Gateways besteht aus vier Schritten:

1) Vorbereitende Arbeiten (siehe Section 3.1, "Vorbereitung der Konfiguration").
2) Das WBM aufrufen (siehe Section 3.2, "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 des Gateways HG 3500 auf STMIX sorgfältig vorzubereiten, damit Sie diese ohne Unterbrechung durchführen können.

Wichtig: 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 das Gateway HG 3500 auf STMIX 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 3.2.1, "Über OpenScape 4000 Assistant starten" Section 3.2.2, "Über Web-Browser starten" Section 3.2.3, "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* **>** *Experten-modus* **>** *Gateway-Dashboard*. Das Fenster *Gateway-Dashboard* mit den vorhandenen Baugruppen wird angezeigt:
3) Klicken Sie in der Zeile der gewünschten HG 3500/STMIX-Baugruppe in der Spalte 'Remote-Zugang' auf *[WBM] [N/A]*. Der Webserver für das Gateway HG 3500 auf STMIX wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.

Anmerkung: 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 das Gateway HG 3500 auf STMIX administrieren.

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 CGWB konfiguriert). Diese Standardeinstellungen sollten von Ihnen im AMO CGWB geändert werden.

WBM-Sitzung starten

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

1) Ã–ffnen Sie Ihren Web-Browser.
2) Geben Sie in die Adresszeile des Web-Browsers die URL des WBM ein. Der Webserver für das Gateway HG 3500 auf STMIX 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 für das Gateway HG 3500 auf STMIX wird angezeigt.
4) Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf *Anmelden*. Die Startseite des WBMs für das Gateway HG 3500 auf STMIX wird angezeigt:
5) In den Modulen *Konfiguration* und *Wartung* können Sie jetzt das Gateway HG 3500 auf STMIX administrieren.

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 zum Gateway HG 3500 auf STMIX wird beendet und die WBM-Sitzung wird geschlossen.

Erläuterungen zum Beenden der WBM-Sitzung finden Sie in Section 3.3.1.4, "Abmelden".

3.3 Anwendungsoberfläche des WBM

Das Hauptfenster des WBM besteht aus folgenden Bereichen:

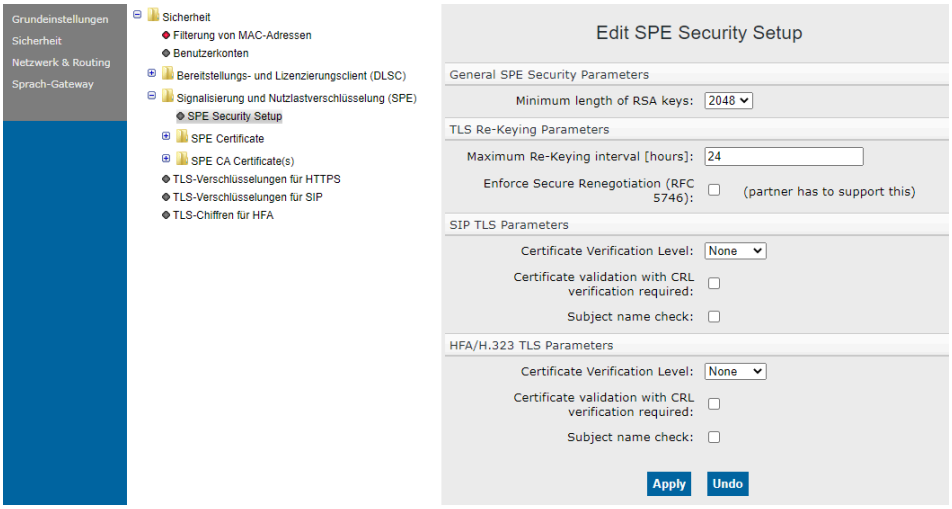


Abbildung 1: WBM-Benutzeroberfläche - HFA

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. Bei einigen ausgewählten Modulen mit Funktionalität wechselt die Schriftfarbe auf blau, wenn Sie mit der Maus auf den Text zeigen. Siehe Section 3.3.1, "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 3.3.2, "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.

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 4, "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 6, "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 STMIX-HFA`, 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 3.3.2, "Symbole im Steuerbereich des WBM-Fensters").

WBM-Pfad:

WBM **>** *Abmelden*

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:

Aktivitäts-Symbol

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

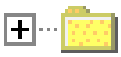
Außerdem werden folgende Statusinformationen angezeigt:

- 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

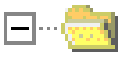
3.3.3 Symbole in den Baumdarstellungen des WBM

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 (SIP WBM)

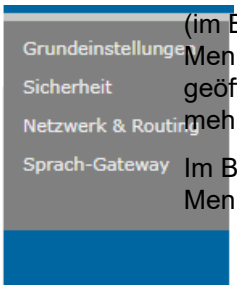


Jedes Verzeichnis, das ausgeblendete Funktionen enthält, ist durch ein Pluszeichen (+) gekennzeichnet. Durch einen Klick werden diese Funktionen eingeblendet.



Die in diesem offenen Verzeichnis enthaltenen Funktionen sind dargestellt. Durch einen Klick werden diese Funktionen ausgeblendet.

- Pfeile (HFA WBM)



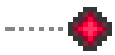
(im Bild: *Grundeinstellungen* = Menü geöffnet): Im Menübereich kann durch Klicken auf ein Dreieck ein Menü geöffnet oder geschlossen werden. Das Ã–ffnen von mehreren Menüs ist möglich.

Im Bild: Ein nicht aktiver Menüpunkt ist grün, ein aktiver Menüpunkt ist weiß.

- Listenpunkte (SIP WBM)

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

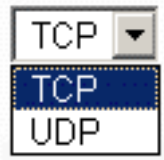
Eingaben und Änderungen im WBM werden im Browser-Fenster als grau hinterlegte Dialoge innerhalb des Browser-Fensters angezeigt. Ferner können separate Dialogfenster angezeigt werden, um z. B. einen Löschwunsch zu bestätigen.

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.

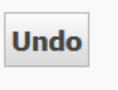
Kontrollkästchen

(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

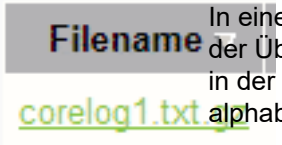


Bei Anklicken wird die Aktion ausgeführt, die als Text auf der Schaltfläche steht. Die Texte sind selbsterklärend wie z. B. *Rückgängig* oder *Übernehmen*.

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 HFA WBM - Konfiguration

4.1 Konfiguration

In diesem Kapitel wird die Konfiguration des HFA-Signalisierungsprotokolls für STMIX beschrieben.

Konfiguration

WBM-Pfad

WBM **>** *Konfiguration*

Das Modul *Konfiguration* wird geöffnet.

Auswahlmöglichkeiten im Modul *Konfiguration*

1) *Grundeinstellungen*

Sicherheit

SPE

Sonstiges

SIP-Funktionen

4.2 Grundeinstellungen

WBM-Pfad

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

Im Menü *Grundeinstellungen* können grundsätzliche Daten zum STMIX - HFA eingegeben werden.

4.2.1 Gateway

WBM-Pfad

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

Der Dialog Gateway-Eigenschaften wird angezeigt: In diesem Dialog können Sie Grunddaten eingeben.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- System-Name: Geben Sie den diesem Feld den STMIX-HFA-Namen ein (z. B. wenn mehrere STMIX-HFA-Systeme auf einem einzigen AP-Rahmen betrieben werden).
- Gateway-Standort: Dieses Feld kann nicht bearbeitet werden. Der Wert wird von AMO UCSU übernommen.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- Übernehmen: Die Eingaben werden gespeichert.
- Rückgängig: Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

4.3 Sicherheit

Im Menü *Sicherheit* können Sie die Sicherheitsoptionen und die *TLS-Konfiguration für HTTPS* administrieren.

WBM-Pfad

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

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Sicherheitsoptionen*

TLS-Konfiguration für HTTPS

4.3.1 Sicherheitsoptionen

WBM-Pfad

WBM **>** *Konfiguration* **>** Sicherheit **>** *Sicherheitsoptionen*

Der Dialog Sicherheitsoptionen wird angezeigt.

Kontrollkästchen

In diesem Dialog gibt es das folgende Kontrollkästchen:

- Sichere TLS-Neuverhandlung erzwingen (RFC 5746): Gilt nur für HFA. 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.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- Übernehmen: Die Eingaben werden gespeichert.
- Rückgängig: Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

Anmerkung: Änderungen werden erst nach einem Neustart des SoftGates aktiv.

4.3.2 TLS-Konfiguration für HTTPS

WBM-Pfad

WBM **>** *Konfiguration* **>** Sicherheit **>** *TLS-Konfiguration 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 für das HTTPS-Protokoll kann im WBM-Menü konfiguriert werden. Sie wird vom Webserver des STMIX - HFA angeboten und unterstützt.

Standardmäßig ist TLS 1.3 mit Fallback auf 1.2 voreingestellt.

4.4 SPE

Durch SPE (Signaling & Payload Encryption) werden VoIP-Nutz- und Signalisierungsdatenströme von und zu STMIX - HFA verschlüsselt. Diese Funktion basiert auf einem asymmetrischen Verschlüsselungsprozess. Ã–ffentliche und private Schlüssel werden für diese Art von Prozess verwendet.

Die einzelnen VoIP-Clients und Gateways (z.B. STMIX - HFA) müssen im Kommunikationssystem eindeutig identifizierbar sein. Dazu werden Zertifikate mit privaten oder öffentlichen Schlüsseln verwendet. Zertifikate werden entweder von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder von der internen Zertifizierungsstelle (CA) des DLS-Servers erstellt. Der DLS-Server sendet die Dateien mit diesen Zertifikaten an den Gateway-DLS-Client.

Je nach Anforderung können Sicherheitseinstellungen zur Bewertung der Zertifikate und zur Verschlüsselung von Datenströmen aktiviert oder deaktiviert werden. So wird die Verschlüsselungssicherheit erhöht oder verringert.

WBM-Pfad

WBM **>** *Konfiguration* **>** SPE

Das Menü *SPE* wird geöffnet.

Die folgenden Optionen werden in diesem Menü angezeigt:

1) *Keycert importieren (nur STMIX - HFA)*

Keycert anzeigen

Keycert löschen

SPE CA-Zertifikate

SPE-Sicherheitseinstellung für HFA

4.4.1 Keycert importieren (nur STMIX - HFA)

Anmerkung: Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat importieren, wird anschließend automatisch ein Reset durchgeführt.

Anmerkung: SPE-Zertifikate für STMIX können nur hier im HFA WBM importiert werden. Die importierten SPE-Zertifikate werden automatisch an den SIP/IPDA-Teil verteilt. Auf dem STMIX - SIP/IPDA WBM können Sie die Zertifikate zu Diagnosezwecken anzeigen.

Anmerkung: Importierte Zertifikate werden automatisch auf die SIP-Funktionen des STMIX angewendet.

WBM **>** *Konfiguration* **>** SPE **>** *Keycert importieren (nur STMIX - HFA)* **>** *Laden eines SPE Key Zertifikats über HTTP*

Der Dialog Laden eines SPE Key Zertifikats über HTTP wird angezeigt.
In diesem Dialog kann ein SPE Key Zertifikat durch Eingeben des Entschlüsselungskennworts und des Dateinamens importiert werden. Die Datei mit dem Zertifikat stammt von einer Kunden-PKI-Zertifizierungsstelle (RA/CA) oder der internen DLS-Server-Zertifizierungsstelle (CA) und muss im PEM- oder PKCS#12-Format vorliegen.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *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-Format):* In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche Durchsuchen kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- Fingerabdruck des Zertifikats anzeigen: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- Zertifikat aus Datei importieren: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu laden:

1) 1. Auswählen: WBM > *Konfiguration* > *SPE* > *Keycert importieren (nur STMIX - HFA)*. 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-Format):* Geben Sie den Pfad und den Dateinamen der Datei ein, die die zu importierenden Zertifikatsdaten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen

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

2) **a)** Überprüfen Sie den Fingerabdruck (Hexadezimalzahl). Wenn das Zertifikat geändert wird, 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.

3) 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.

4.4.2 Keycert anzeigen

WBM-Pfad

WBM **>** *Konfiguration* **>** SPE **>** *Keycert anzeigen* **>** *Zertifikatsinformationen*

Der Dialog Zertifikatsinformationen wird angezeigt. In diesem Dialog kann das SPE-Zertifikat angezeigt werden, z. B. um es zu überprüfen.

Angezeigte Daten

Die folgenden Zertifikatsdaten werden angezeigt:

- 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*, *Ã–ffentlicher Schlüssel*, *Fingerabdruck*

4.4.3 Keycert löschen

WBM-Pfad

WBM **>** *Konfiguration* **>** SPE **>** *Keycert löschen* **>** *Zertifikat für SPE löschen*

Der Dialog *Zertifikat für SPE löschen* wird angezeigt. In diesem Dialogfeld können Sie das SPE-Zertifikat entfernen, z. B. wenn ein neues Zertifikat benötigt wird.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Löschen*: Das SPE-Zertifikat kann nach einer Warnung gelöscht werden.
- *Abbrechen* Der Löschvorgang wird abgebrochen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SPE-Zertifikat zu entfernen:

1) Auswählen: *WBM* > *Konfiguration* > SPE > *Keycert löschen*. Eine Warnung wird angezeigt. Zu Prüfzwecken wird außerdem der Name des Zertifikats angegeben.
2) Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*. Das SPE-Zertifikat wird auch für SIP gelöscht.

4.4.4 SPE CA-Zertifikate

WBM-Pfad

WBM > *Konfiguration* > SPE > *SPE CA-Zertifikate*

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.

Vorgehensweise:

Führen Sie zum Importieren eines vertrauenswürdigen CA-Zertifikats die folgenden Schritte durch (siehe oben, *Keycert importieren (nur STMIX - HFA)*)

SPE CA-Zertifikat anzeigen

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

1) 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.

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¦).

4.4.5 SPE-Sicherheitseinstellungen für HFA

4.4.5 SPE-Sicherheitseinstellung für HFA

WBM-Pfad

WBM > *Konfiguration* > SPE > *SPE-Sicherheitseinstellungen für HFA*

Das Dialogfeld *SPE-Sicherheitseinstellungen für HFA bearbeiten* wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signalling

und Payload Encryption (SPE) an die Sicherheitsanforderungen des Kunden angepasst werden. Dies betrifft die Verschlüsselung der Signalisierungs- und Nutzdaten bei der Kommunikation zwischen STMIX - HFA und den VoIP-Clients bzw. zwischen zwei STMIX - HFA-Systemen.

Dropdown-Listen, Eingabefelder, Kontrollkästchen

In diesem Dialog werden folgende Einstellungen angezeigt:

- *Mindestlänge des RSA-Schlüssels: Es können die Längen 512, 1024 und 2048 gewählt werden. Je größer dieser Wert ist, desto sicherer ist der Schlüssel.*
- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]:* Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Wenn diese Zeit verstrichen ist, wird ein neuer Schlüssel definiert.
- *Sichere Neuaushandlung erzwingen (RFC 5746)*: Aktivieren durch Kontrollkästchen.
- *TLS-Protokollversion:* Sie können TLS 1.3 mit Fallback auf TLS 1.2 (Standard), nur TLS 1.3 oder nur TLS 1.2 auswählen.

TLS 1.2 Ziffernauswahl

- *Schlüsselvereinbarung*: Wählen Sie mit Perfect Forward Secrecy oder ohne.
- *Verschlüsselung*: Wählen Sie AES-128 mit Fallback auf AES-256 oder Nur AES-256.
- *AES-Betriebsmodus*: Wählen Sie GCM bevorzugt, mit Fallback auf CBC, Nur GCM oder Nur CBC.

Anmerkung: Wenn ECDSA-Zertifikate für SPE importiert wurden, muss bei der Cipher-Auswahl sichergestellt werden, dass Perfect Forward Secrecy (PFS)-Ziffern im WBM-GUI aktiviert sind (für SIP oder HFA). Andernfalls schlägt der TLS-Handshake der SIP/HFA-Clients fehl.

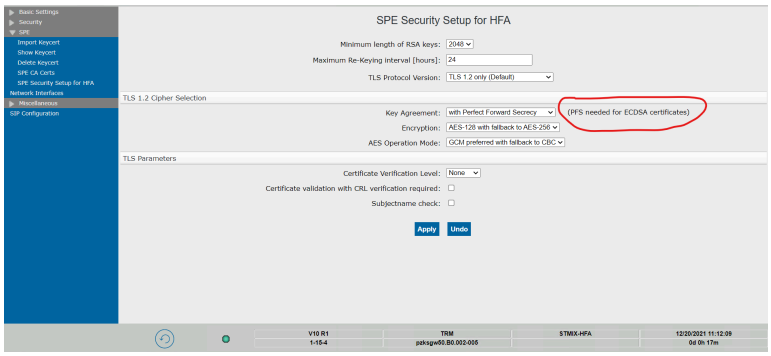


Abbildung 2: PFS in SPE-Sicherheitseinstellungen für HFA

TLS-Parameter

- *Zertifikatsprüfungsstufe* Keine, vertrauenswürdig oder vollständig
- *Zertifikatsprüfung mit CRL-Prüfung erforderlich:* Aktivieren/Deaktivieren
- *Prüfung des Antragstellers:* Aktivieren / Deaktivieren

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Apply (Übernehmen):* Die Eingaben werden gespeichert.
- *Undo (Rückgängig machen):* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

WBM-Pfad

WBM **>** *Konfiguration* **>** SPE **>** *SPE-Sicherheitseinstellung für HFA*

Der Dialog *SPE Sicherheitseinstellung für HFA* ändern wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signalling und Payload Encryption (SPE) an die Sicherheitsanforderungen des Kunden angepasst werden. Dies betrifft die Verschlüsselung der Signalisierungs- und Nutzdaten bei der Kommunikation zwischen dem STMIX - HFA und den VoIP-Clients sowie zwischen zwei STMIX-HFA-Systemen.

Dropdownlisten, Eingabefelder, Kontrollkästchen

In diesem Dialog werden folgende Einstellungen angezeigt:

- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]:* Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Wenn diese Zeit verstrichen ist, wird ein neuer Schlüssel definiert.
- *Sichere Neuaushandlung erzwingen (RFC 5746)*: Aktivieren durch Kontrollkästchen.
- *TLS-Protokollversion:* Sie können TLS 1.3 mit Fallback auf TLS 1.2 (Standardeinstellung), Nur TLS 1.3 oder Nur TLS 1.2 auswählen.

TLS 1.2 Chiffrenauswahl

- *Schlüsselvereinbarung*: Wählen Sie mit oder ohne Perfect Forward Secrecy.
- *Verschlüsselung*: Wählen Sie AES-128 mit Fallback auf AES-256 oder Nur AES-256.
- *AES-Betriebsmodus*: Wählen Sie GCM bevorzugt, mit Fallback auf CBC, Nur GCM oder Nur CBC.

TLS-Parameter

- *Zertifikatsprüfungsstufe* Keine, vertrauenswürdig oder vollständig
- *Zertifikatsprüfung mit CRL-Prüfung erforderlich:* Aktivieren/Deaktivieren
- *Prüfung des Antragstellers:* Aktivieren / Deaktivieren

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Defaultwerte zurückgesetzt.

4.5 Netzwerkschnittstellen

WBM-Pfad:

WBM **>** *Konfiguration* **>** Netzwerkschnittstellen

Sie können Details der LAN-Schnittstelle 1 konfigurieren. Die Funktion der ersten LAN-Schnittstelle ist vordefiniert:

Sie können Detaildaten zur Verwendung der LAN1/LAN2-Schnittstelle ansehen.

- Schnittstellenname: LAN1,
- Aktive Schnittstelle: eth0
- IP-Adresse: Schnittstellenadresse
- Subnetzmaske: Subnetzmaske
- *IP-Adresse des Default Routers*
- *Linkmodus*
- *Link Status*
- *Autonegotiation:* An/Aus
- Max. Datenpaketlänge (Byte): Max. Datenpaketlänge in Byte
- für das IP-Protokoll.
- IEEE802.1p/q-Tagging: Von der Baugruppe gesendetes Ethernet-Format.

Die LAN2-Konfiguration erfolgt über den AMO CGWB durch Zuweisen oder Löschen einer Management-IP-Adresse.

â¢ Das zweite LAN verwenden als: Spiegel/Bond für LAN1 oder das Management-LAN.

4.6 Sonstiges

WBM-Pfad

WBM **>** *Konfiguration* **>** Sonstiges

Das Menü *Sonstiges* wird geöffnet.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *NGS*

QoS-Data-Collection

4.6.1 NGS

WBM-Pfad

WBM **>** *Konfiguration* **>** Sonstiges **>** *NGS* **>** *NGS-Einstellungen*

Die Webservice-Lösung NextGen-Service (NGS) überträgt die IPv4- und/oder IPv6-Adressen sowie alle sonstigen im Rahmen von Routing-Informationen erforderlichen Daten vom HG 3500 auf STMIX zum NGS-Server.

Der Dialog *NGS-Einstellungen* wird angezeigt: Geben Sie in dieses Feld die IP-Adresse des NGS-Servers ein.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *IP-Adresse des NGS-Servers [IPv4 oder IPv6]:* Die IP-Adresse kann im Format IPv4 oder IPv6 eingegeben werden. Das Standardformat ist IPv4: 0.0.0.0.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- Übernehmen: Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das HG 3500 auf STMIX neu gestartet werden.
- Rückgängig: Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

4.6.2 QoS-Data-Collection

Quality of Service Data Collection (QDC) â“ 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 zu QDC

Siehe *OpenScape 4000 V8 Gateways HG 3500 und HG 3575, Administratordokumentation.*

WBM-Pfad

WBM **>** *Konfiguration* **>** Sonstiges **>** QoS-Data-Collection **>** *Quality of Service Data Collection*

Auswahl- und Eingabefelder

QDC-Konfiguration

- *Senden an QCU:* Aktivieren Sie dieses Kontrollkästchen, wenn Daten an die QCU gesendet werden sollen. Standardwert: Kontrollkästchen ist nicht aktiviert.

- 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 aktiviert: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an das Network Management gesendet werden sollen. Standardwert: Kontrollkästchen ist nicht aktiviert.
- IP-Adresse des Network Managements Geben Sie die IP-Adresse des Ziels ein. Standardwert: 0.0.0.0.
- Community String: n/a

Wichtig: Wenn eines der Kontrollkästchen Senden an QCU oder Senden an Network Management 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.Folgende Felder können Sie bearbeiten:
- *Berichtsintervall (s):* 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. Defaultwert: 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

Wichtig: Die Zeitskala ist im Beobachtungszeitraum und im Berichtsintervall segmentiert. Jeder Beobachtungszeitraum wird auf eine Schwellwertüberschreitung geprüft. Für jedes 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:

Tabelle 2: Codecs - Typen

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.

Schaltflächen

Dieser Dialog enthält folgende Schaltflächen:

- Übernehmen: Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen muss das HG 3500 auf STMIX neu gestartet werden.
- Rückgängig: Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt

4.7 SIP-Funktionen

WBM-Pfad

WBM **>** *Konfiguration* **>** SIP-Funktionen

Unter Chapter 5 und Chapter 7 finden Sie eine Beschreibung des STMIX - SIP/IPDA WBM.

5 SIP/IPDA WBM - Konfiguration

In diesem Kapitel wird die Konfiguration des SIP-Signalisierungsprotokolls für STMIX beschrieben.

5.1 Konfiguration

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*

HFA-Funktionen

5.2 Grundeinstellungen

WBM-Pfad:

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

Die Baumstruktur für *Grundeinstellungen* wird angezeigt.

Einträge unter *Grundeinstellungen*:

1) *System Gateway Quality of Service*

5.2.1 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) *Sachnummer*

Software-Build

Der Dialog *Gateway-Eigenschaften* wird angezeigt. Feldbeschreibungen siehe Section 5.2.2, "Gateway".

5.2.1.1 Sachnummer

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *System* **>** *Sachnummer*

Das Fenster Sachnummern wird angezeigt. Es enthält die Hardware-ID und die Teileliste.

5.2.1.2 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*

OpenScape System:

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

Third-Party- und Open-Source-Software

5.2.2 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 OpenScape 4000-Systems. Format: 0-0-0
- *Gateway-Standort*: Dieses Feld enthält Informationen zum Aufstellungsort des HG 3500 auf STMIX. 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*: Das Länderkennzeichen wird vom OpenScape 4000-System eingestellt und per AMO konfiguriert.
- Globales Gateway vom Typ G.711: wird per AMO konfiguriert und ist im WBM nur anzeigbar. Default ist A-law.

- Globales Gateway vom Typ G.711 für die LAN-Seite: Entsprechend der ITU-T Empfehlung G.711 können die Digitalisierungsverfahren für analoge Audiosignale A-law oder Âµ-law eingestellt werden. Default ist A-law.
- Unterstützte IP-Versionen: werden über den AMO CGWB konfiguriert und sind im WBM nur anzeigbar. Mögliche Werte: Nur IPV4, IPV4 und IPV6 (Dual Stack) oder Nur IPV6
- *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:

- *Konferenz-Optimierung:* Bei einer Konferenz wird ein gezielter Fallback auf die G.711-Kodierung durchgeführt.
- *Unterstützung für Dispatch-Applikation* â“ nur für Native SIP Trunking-GW
- *SIP-Register für Trunking erlauben* â“ Nur für Native SIP Trunking mit Profil.
- *Instant-DMC verwenden* â“ Nur für Native SIP Trunking und SIP-Endpunkte.
- *Early Media bei SIP-Trennung verwenden* â“ Nur für Native SIP Trunking-GW.
- *Signalisierungsprotokoll für IP-Networking:* SIP. Diese Einstellung wird per AMO konfiguriert und ist im WBM nur anzeigbar. Mögliche Werte: *SIP*, *H.323* oder *Nicht konfiguriert*.
- *Displayname Charactercode-Set*: Unterstützung für kyrillische Anzeigenamen. 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.

5.2.3 Quality of Service

'Quality of Service' (Dienstgüte) wird im HG 3500 auf STMIX 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 auf STMIX selbst produziert, in verschiedene Gruppen aufgeteilt.

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.

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

5.2.4 Zeitzonen-Einstellungen

WBM-Pfad:

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

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

5.3 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) *Ruf-Statistiken*

5.3.1 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

5.3.1.1 Statistiken löschen

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

WBM-Pfad:

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

5.3.1.2 Ruf-Statistik (1h)

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

WBM-Pfad:

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

5.3.1.3 Ruf-Statistik (24h)

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

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *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 5.3.1.2, "Ruf-Statistik (1h)".

5.3.1.4 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* **>** *Grundeinstellungen* **>** 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 5.3.1.2, "Ruf-Statistik (1h)".

5.3.1.5 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* **>** *Grundeinstellungen* **>** 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 5.3.1.2, "Ruf-Statistik (1h)".

5.3.1.6 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* **>***Grundeinstellungen* **>** 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.

5.3.1.7 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* **>** *Grundeinstellungen* **>** 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 5.3.1.6, "LAN-Ruf-Statistik". Alle Zahlen beziehen sich jedoch bei dieser Statistik ausschließlich auf Verbindungen, die über PBX zustande kamen.

5.3.1.8 Aktuelle Verbindungen

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

WBM-Pfad:

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

5.4 Sicherheit

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit*

Die Baumstruktur für *Sicherheit* wird angezeigt.

Einträge in der Baumstruktur *Sicherheit*:

1) *Benutzerkennungen Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))*

TLS-Chiffren für SIP

5.4.1 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

5.4.2 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)*

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

1) *SPE-Sicherheitseinstellung für SIP*
   SPE-Zertifikat SPE CA-Zertifikate

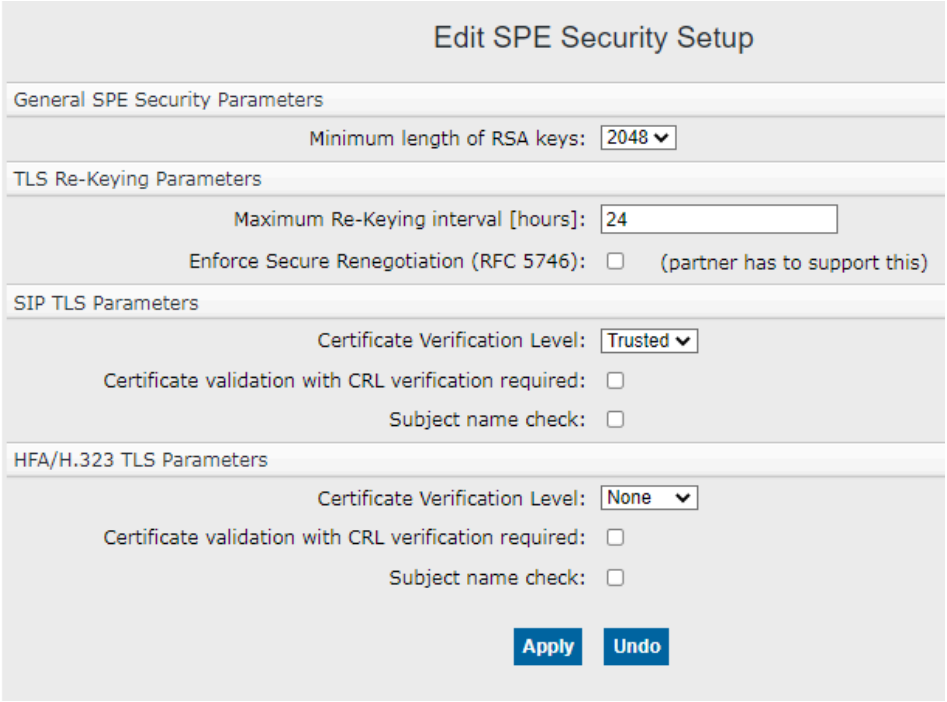
5.4.2.1 SPE-Sicherheitseinstellung für SIP

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:



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:

WBM > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellung ändern* **>** Minimale Länge des RSA Schlüssels

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 167 Stunden
- Minimal 6 Stunden
- Deaktiviert 0 (NICHT EMPFOHLEN)

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellung ändern* **>** *TLS Schlüssel-Neuverhandlung* > *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]*

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:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellung ändern* **>***TLS Schlüssel-Neuverhandlung* **>** *Sichere Neuverhandlung erzwingen (RFC 5746)*

Zertifikatsprüfungsstufe

Während des Aufbaus der TLS (Transport Layer Security)-Sitzung muss das Produkt die angegebene Identität (das Zertifikat) der Gegenstelle im Kommunikationskanal überprüfen. Diese Prüfung muss auf der Client-Seite der TLS-Sitzung durchgeführt werden, wenn es um die Identität der Serverseite geht, oder sowohl auf der Client- als auch auf der Server-Seite, wenn MTLS (Mutual TLS) verwendet wird.

Wichtig: Wenn aufseiten des TLS-Servers die Stufe Trusted (Vertrauenswürdig) oder Full (Vollständig) eingestellt ist, wird

das Zertifikat des TLS-Clients angefordert (Mutual TLS). Wenn auf dem Gateway Teilnehmer konfiguriert sind, die 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).

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

Wichtig: 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.

Wichtig: Die eingestellte Zertifikatsprüfungsstufe gilt für alle SIP-Schnittstellen eines Gateways. Daher ist es nicht möglich, auf einem Gateway SIP-Q-Trunking und zugleich SIP-Teilnehmer ohne Zertifikate zu konfigurieren.

Für die Zertifikatsprüfung sind drei verschiedene Stufen definiert, die ausgewählt werden können:

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellung ändern* **>** SIP TLS Parameter

- None â“ die Remote-Entity wird nicht authentifiziert
- Das Zertifikat der Remote-Entity wird nicht angefordert und nicht geprüft.
- Trusted â“ 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 â“ 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:

  WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellung ändern* **>** SIP 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:

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE-Sicherheitseinstellung für SIP* **>** *SPE Sicherheitseinstellungen ändern* **>** SIP TLS Parameter **>** Namensprüfung Antragsteller.

5.4.2.2 SPE-Zertifikat

Dieser Ordner enthält das SPE-Zertifikat mit dem privaten Schlüssel. Per Default ist dieser Ordner leer. Das Zertifikat muss erst importiert werden. Bei Bedarf können Sie das importierte Zertifikat anzeigen. Die Datei, welche das Zertifikat enthält, muss im PEM- oder im PKCS#12-Format vorliegen. Diese Datei stammt von einer Kunden PKI-Zertifizierungsstelle (RA/CA) oder der internen Zertifizierungsstelle (CA) des DLS-Servers.

WBM-Pfad:

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

Ordner *SPE Zertifikat*:

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

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. Um dieses Zertifikat zu benutzen, können Sie die entsprechende PEM oder PKCS#12-Datei importieren.

WBM-Pfad:

WBM > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE-Zertifikat* > *SPE Zertifikat und privaten Schlüssel importieren (PEM oder PKCS#12)* > *Laden eines SPE Key Zertifikats über HTTP*

Vorgehensweise:

Anmerkung: Sie können Zertifikate über das WBM des STMIX-HFA importieren (siehe Section 4.4.1, "Keycert importieren (nur STMIX - HFA)").

SPE-Zertifikat anzeigen

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

WBM-Pfad:

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

Vorgehensweise:

1) Auswählen: *WBM* > *Konfiguration* > *Sicherheit* > *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* > *SPE-Zertifikat* > *SPE-Zertifikat* > *(Linksklick) SPE-Zertifikat*. Der Dialog *Zertifikat-sinformationen* 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.

5.4.2.3 SPE CA-Zertifikate

Dieser Ordner enthält vertrauenswürdige SPE CA-Zertifikate.

STMIX-SIP/IPDA unterstützt 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 Vertrauenswürdiges CA-Zertifikat importieren (PEM oder binär)*

Vorgehensweise:

Anmerkung: Sie können Zertifikate über das WBM des STMIX-HFA importieren (siehe Section 4.4.1, "Keycert importieren (nur STMIX - HFA)").

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* **>** SPE CA-Zertifikate **>** *(Linksklick) SPE CA-Zertifikat*

Vorgehensweise:

1) Auswählen: *WBM* **>** *Konfiguration* **>** *Sicherheit* **>** *Signalisierungs- und Sprachverschlüsselung (Signaling and Payload Encryption (SPE))* **>** *SPE CA-Zertifikate* **>** SPE CA Zertifikate **>** *SPE CA Zertifikat anzeigen*. 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* **>** SPE CA-Zertifikat **>** *Zertifikatsinformationen*

Vorgehensweise:

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

5.4.3 TLS-Chiffren für SIP

Unterstützt werden Protokolle ab TLSv1.0. SSLv2 und SSLv3 sind aufgrund von Sicherheitsproblemen nicht zulässig.

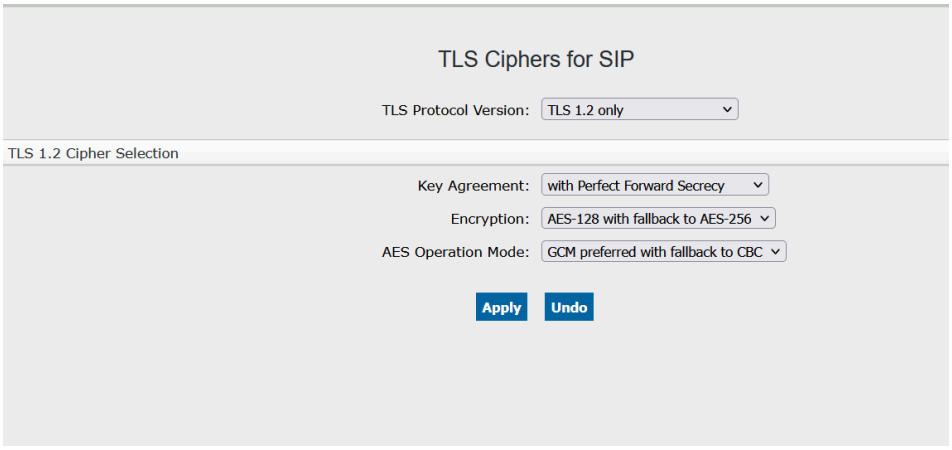
Die TLS-Version kann im WBM-Menü konfiguriert werden.

WBM-Pfad:

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

Die TLS-Version und für TLSv1.2 auch die Schlüsselaushandlungsmethode, der Verschlüsselungsalgorithmus und der AES-Betriebsmodus können konfiguriert werden. (weitere Informationen zu TLSv1.2 finden Sie unter https://www.ietf.org/rfc/rfc5246.txt).

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



5.5 Netzwerk und Routing

WBM-Pfad:

WBM > *Konfiguration* > *Netzwerk und Routing*

Die Baumstruktur für *Netzwerk und Routing* wird angezeigt:

1) *Routing*

5.6 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.

WBM-Pfad:

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

Die Baumstruktur für *Routing* wird angezeigt.

Einträge in der Baumstruktur *Routing*:

1) *IP-Routing*

Wahlparameter

5.6.1 IP-Routing

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) *Default Router DNS-Server ICMP-Anforderung*

5.6.2 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.

5.6.3 DNS-Server

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* > Routing > IP-Routing > DNS-Server > *DNS-Einstellungen*

Das Fenster *DNS-Einstellungen* erscheint. Die *DNS-Server*-Adressen werden im AMO CGWB konfiguriert.

- *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.

5.6.3.1 ICMP-Anforderung

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

WBM-Pfad:

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

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

1) *Ping Traceroute*

5.6.3.2 Ping

Zur Kontrolle können Sie einen ping-Befehl absetzen, um das Routing zwischen dem HG 3500 auf STMIX 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 STMIX-SIP 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.

5.6.3.3 Traceroute

Zur Kontrolle können Sie einen traceroute-Befehle absetzen, um das Routing zu testen. Das Traceroute überprüft die Netzwerkverbindung zwischen HG 3500 auf STMIX 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 STMIX/ SIP 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.

5.6.4 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

5.6.4.1 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 auf STMIX.
- *Ortskennzahl*: Die Ortskennzahl für den Standort des HG 3500 auf STMIX.
- *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*.

5.6.4.2 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.

5.6.4.3 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.

5.7 Sprachgateway

Das STMIX-SIP/IPDA bietet Ihnen mit Voice over IP (VoIP) die Möglichkeit, die Leistungsmerkmale von OpenScape 4000 V10 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 Codec-Parameter IP-Networking-Modus SIP-Trunk-Profilparameter

SIP-Trunk Profile

Sammelanschluss

Ziel-Codec-ParameterKZPs für MLPP *Clients ISDN Classmarks*

5.7.1 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*.

5.7.2 SIP-Parameter

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.

5.7.3 Codec-Parameter

Sie können die Einstellungen für die Codecs G.711-A-law, G.711-Âµ-law, G.729, G.729A, G.729B und G.729AB sowie für das Faxprotokoll T.38 ansehen.

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.729, G.729A, G.729B, G.729AB und anzeigen:

- *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.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).
- Zeitbereich für die sofortige Umschaltung auf T.38-Fax (s): Es sind Werte von 0 bis 60 erlaubt. Der Wert '0â bedeutet, dass keine Umschaltung vorgenommen wird.

Wichtig: 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.

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

Wichtig: 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.

Wichtig: 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: 0â“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*. Klicken Sie auf *Rückgängig*, um die Änderungen zu verwerfen.

5.7.4 IP-Networking-Modus

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *IP-Networking-Modus*

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

- *Signalisierungsprotokoll für IP-Networking*: z. B. SIP, wird über AMO konfiguriert
- *Anzahl der für IP-Networking konfigurierten Ports*: z. B. 0, 2

Das Fenster enthält eine Tabelle mit allen IP-Networking-Ports:

- *Portnummer (circuit)Gesperrt*: Ja/Nein
- *Use DMC (DMC verwenden) Aktiviert/Deaktiviert*
- *Instant-DMC verwenden: Aktiviert/Deaktiviert*
- *Gesperrt: Ja/Nein*

5.7.5 SIP-Trunk-Profilparameter

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:

- *Profile für Trunks via SIP-Q verwenden*: Aktivierbar/Deaktivierbar. Ist per Default deaktiviert.
- *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.

5.7.6 SIP-Trunk Profile

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.

WBM > *Konfiguration* > *Sprachgateway* > SIP-Trunk Profile > *(Einzelklick)* <SIP-Provider Unterordner> > *SIP-Trunk-Profil*

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

- *Profilname*: nicht änderbar
- *Konto/Authentifizierung erforderlich:* Aktivierbar/Deaktivierbar.
- *Remotedomänenname:* 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:* Mikey und SDES
- *Verwendung von Payload Encryption:* Nicht konfigurierbar

Registrar:

- *Registrar verwenden:* Aktivierbar/Deaktivierbar. Festlegen, ob ein Domain-Name-Registrar verwendet werden soll.
- *IP Adresse/Hostname:* IP-Adresse oder Hostname des Domain-Name-Registrars eingeben.
- *Port definieren:* Aktivierbar/Deaktivierbar. Port für den Domain-Name-Registrar festlegen.

- *Reregistrations-Intervall (s):* Festlegen, in welchen Zeitabständen eine Neuregistrierung erforderlich ist.

Proxy:

- *IP Adresse/Hostname:* IP-Adresse oder Hostname des Proxy-Servers eingeben. Das ist der SIP-Server des Providers.
- *Port definieren:* 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/Hostname:* IP-Adresse oder Hostname des Outbound-Proxy-Servers eingeben.
- *Port definieren:* 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/Hostname:* IP-Adresse oder Hostname des Inbound-Proxy-Servers eingeben.
- *Port definieren:* 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 oder auf*Löschen*, um das SIP-Trunk-Profil zu löschen.

5.7.7 Sammelanschluss

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Sammelanschluss* > Sammelanschluss für SIP-Videoteilnehmer

Die Tabelle Sammelanschluss für SIP-Videoteilnehmer wird angezeigt. Sie enthält die Sammelanschlüsse für SIP-Videoteilnehmer mit der Hauptrufnummer und zwei Nebenrufnummern.

5.7.7.1 Hinzufügen

Ein Sammelanschluss für SIP-Videoteilnehmer kann hinzugefügt werden. Der hinzugefügte Sammelanschluss erscheint nach dem Hinzufügen in der Tabelle Sammelanschluss für SIP-Videoteilnehmer.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *Sammelanschluss* > *Hinzufügen* > Sammelanschluss für SIP-Videoteilnehmer

Das Eingabefenster Sammelanschluss für SIP-Videoteilnehmer wird angezeigt. Die Hauptrufnummer und bis zu vier Nebenrufnummern können eingegeben werden.

Klicken Sie auf Übernehmen und im Bestätigungsdialog auf OK. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen, oder klicken Sie auf Löschen, um die Änderungen zu entfernen.

5.7.8 Ziel-Codec-Parameter

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

WBM-Pfad:

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

5.7.8.1 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.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, G.711-Âµ-law Priorität 2, G.729A Priorität 4 und G.729AB Priorität 3. 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 und im Bestätigungsdialog auf OK. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen; klicken Sie auf Löschen, um die Regel für die Hauptanschlussnummer zu entfernen.

5.7.8.2 KZPs für MLPP

Sie können die Kennzahlpunkte für MLPP anzeigen und bearbeiten.

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *KZPs für MLPP* > *KZPs für MLPP*

Die Tabelle *KZPs für MLPP* wird angezeigt. Sie enthält Kennzahlpunkte für Anrufe.

Die Kennzahlpunkte können geändert werden. Es sind maximal 16 Zeichen erlaubt. Diese sind: 0â“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.

5.7.9 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) *UFIP SIP*

Klassische SIP-Clients

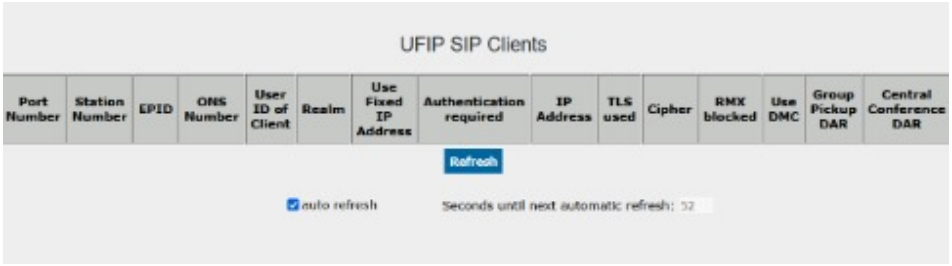
5.7.9.1 UFIP SIP

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.
- *ONS-Nummer:* Zeigt die One Number Service-Nummer 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.
- *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

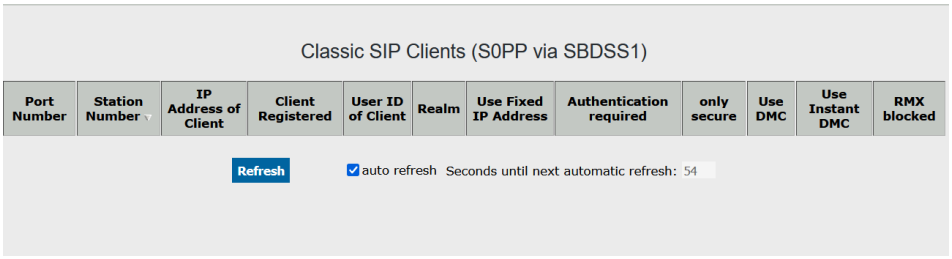
Aktualisieren: Aktivierbar/Deaktivierbar. Wenn die Checkbox aktiviert ist, wird die Tabelle 'SIP-Clients' in regelmäßigen Zeitabständen aktualisiert, wie im Eingabefeld *Sekunden bis zur nächsten Aktualisierung* angegeben.

5.7.9.2 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.

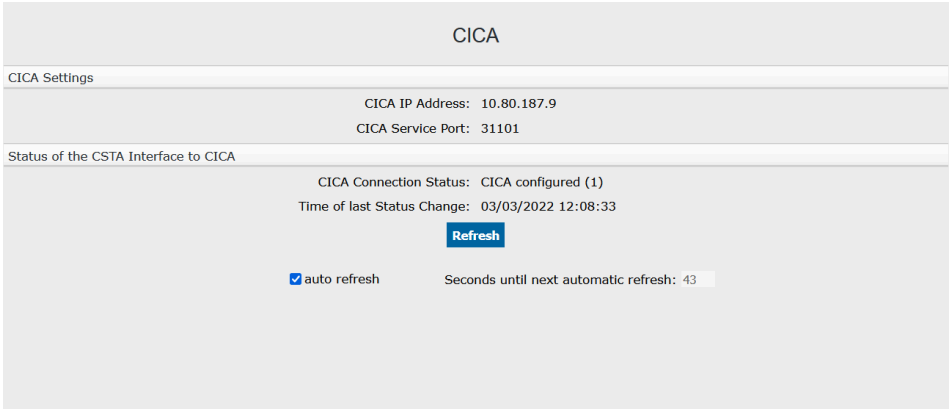


5.7.10 CICA

Auf dieser Seite sehen Sie den Status der Verbindung vom HG3500 auf STMIX zum CA4000/CICA auf dem zentralen Host. Die Konfiguration der IP-Adresse des NPS erfolgt zentral über den AMO SIPCO

WBM-Pfad:

WBM > *Konfiguration* > Sprachgateway > Clients



5.7.11 ISDN Classmarks

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

WBM-Pfad:

WBM > *Konfiguration* > *Sprachgateway* > *ISDN Classmarks*

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.

5.8 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) *Payload-Parameter*

Fax/Modem Ton-Behandlung

5.8.1 Payload-Parameter

WBM-Pfad:

WBM **>** *Konfiguration* **>** *Payload* **>** Payload-Parameter

Sie können sich die Liste der Fax-Parameter anzeigen lassen.

Der Dialog Payload-Parameter wird angezeigt. Er enthält im Bereich Fax-Parameter die folgenden Einstellungen:

- Fehler-Korrektur-Modus Aktivieren/Deaktivieren
- Fax-Kanal mit ermitteltem Ton öffnen: Aktivieren/Deaktivieren
- Anzahl redundanter Pakete: Wertebereich 0 bis 2; Default 2
- Maximaler Netzwerk-Jitter (ms): Wertebereich 140 bis 500; Default 200

Klicken Sie auf Übernehmen und im Bestätigungsdialog auf OK. Klicken Sie auf Rückgängig, um die vorherigen Werte wiederherzustellen.

5.8.2 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*.

5.9 HFA-Funktionen

WBM-Pfad

WBM **>** *Konfiguration* **>** HFA-Funktionen

Siehe Chapter 4 und Chapter 6 für eine Beschreibung von STMIX - HFA WBM.

6 HFA WBM - Wartung

6.1 Wartung

Das Modul *Wartung* stellt Funktionen für die Wartung und Administration des STMIX zur Verfügung. Dazu gehören das Durchführen von Software-Updates, das Sichern der Konfiguration, das Arbeiten mit Protokolldateien, das Aktivieren von Trace-Profilen, das Erstellen eines Secure Trace, das Erstellen von Diagnosedateien und das Ermitteln von Status-Informationen über OpenScape 4000 SoftGate und H.323-Telefone.

WBM-Pfad

WBM > Wartung

Das Modul *Wartung* wird geöffnet.

Auswahlmöglichkeiten im Modul *Wartung*:

1) *SW-Update*

Backup/Restore

Logs

Secure Trace

DLS Client

Diagnose

Status-Information

Reboot OS

6.2 SW-Update

Im Menü (SW: Software) werden Funktionen zum Anzeigen der Software-Version, für das Software-Update und für die Software-Aktivierung des STMIX â“ HFA zur Verfügung gestellt.

WBM-Pfad

WBM **>** *Wartung* **>** SW-Update

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *SW-Version anzeigen*

LW-Update

LW-Aktivierung

OS-Update

6.2.1 SW-Version anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** SW-Update **>** *Softwareversion*

Der Dialog Softwareversion wird angezeigt. Dieser Dialog enthält Details über die momentan installierten Software- und Hardwareversionen.

Angaben

Im Einzelnen werden folgende Angaben gemacht:

- *System Version (PBX):* Dieser Bereich zeigt die OpenScape 4000 Version unter:
- *Plattform-Version:* Die Angaben dazu sind:
- Hardware, Seriennummer, Platform Version, Importierte Platform Version, OS-Update Status
- **Loadware-Version:** Dieser Bereich zeigt die installierten Software- und Loadwareversionen an. Beispiel:
- *Loadware-Version, APS-Version*
- *Komponentenversionen:* Dieser Bereich zeigt die installierten SoftGate-Komponenten und ihre Versionen. Beispiel:
- *IMS SVN Version, SoftGate SVN Version, Soco-common Version*
- *Zusätzliche Packageversionen:* Dieser Bereich zeigt zusätzlich benötigte Software und ihre Versionen. Beispiel:
- Java Version

6.2.2 LW-Update

WBM-Pfad

WBM **>** *Wartung* **>** LW-Update **>** *Loadwareaktualisierung*

Der Dialog Loadwareaktualisierung wird angezeigt. In diesem Dialog kann die STMIX-Anwendung geladen werden. Die Loadware-Datei ist dieselbe Datei wie beim OpenScape 4000 SoftGate.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die aktuelle Software enthält. Über die Schaltfläche Durchsuchen kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- Rückgängig: Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Laden der STMIX-Anwendung die folgenden Schritte durch:

- Geben Sie den Pfad und den Namen der Datei ein, welche die aktuelle Software enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.

Klicken Sie auf die Schaltfläche Laden. Die Software wird geladen. Nach dem Laden wird die nächste WBM-Seite automatisch eingeblendet.

6.2.3 LW-Aktivierung

WBM-Pfad

WBM **>** *Wartung* **>** LW-Aktivierung **>** *Loadwareaktivierung*

Der Dialog Loadwareaktivierung wird angezeigt. In diesem Dialog kann die geladene STMIX-Anwendung entweder sofort oder zeitgesteuert â“ zu einem bestimmten Zeitpunkt oder nach einer bestimmten Dauer â“ aktiviert werden.

Angaben

In diesem Dialog gibt es die folgenden Angaben:

- *Softwareversion:* Zeigt die Softwareversion der im Dialog Softwareaktualisierung geladenen STMIX-Anwendung an.
- *Start der Aktion am:* Die Aktivierung der geladenen STMIX-Anwendung soll zu einem bestimmten Zeitpunkt stattfinden. Der Tag dieses Zeitpunktes ist entweder über die Auswahlfelder oder über die Schaltfläche Kalender festlegbar.
- *Start der Aktion in:* Die Aktivierung der geladenen STMIX-Anwendung soll nach Ablauf einer bestimmten Zeitdauer stattfinden.
- *Aktion stoppen:* Eine bereits vorher gestartete Aktion für die zeitgesteuerte Aktivierung wird gestoppt.
- *Systemzeit:* Diese Zeit ist die lokale Zeit von OpenScape und die Bezugszeit für die zeitgesteuerte Aktivierung. Die Angaben sind nicht editierbar.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.
- *Sofort starten:* Die Aktivierung der STMIX-Anwendung wird sofort gestartet.

Vorgehen für sofortige Aktivierung

Führen Sie zum sofortigen Aktivieren der geladenen Software die folgenden Schritte durch:

1) Klicken Sie auf die Schaltfläche Sofort starten. Die Software wird aktiviert.

Vorgehen für zeitgesteuerte Aktivierung

Führen Sie zum zeitgesteuerten Aktivieren der geladenen Software die folgenden Schritte durch:

1) Zeitpunkt oder Dauer festlegen:

2) • Zeitpunkt, zu dem die Aktivierung gestartet werden soll: Aktivieren Sie den Radio-Button Start der Aktion am und geben Sie in den Auswahl-

und Eingabefeldern Tag, Monat, Jahr, STD:MM den Zeitpunkt an. Die Schaltfläche Kalender kann dazu ebenfalls benutzt werden.

- Dauer, nach der die Aktivierung gestartet werden soll: Aktivieren Sie den Radio-Button Start der Aktion in und geben Sie in den Eingabefeldern Tagen und STD:MM die Dauer an.

3) Klicken Sie auf Übernehmen. Die Änderungen werden gespeichert. Die Aktion für die zeitgesteuerte Aktivierung wird gestartet.

Vorgehen für Stoppen der zeitgesteuerten Aktivierung

Führen Sie zum Stoppen einer Aktion für die zeitgesteuerte Aktivierung die folgenden Schritte durch:

1) Aktivieren Sie den Radio-Button Aktion stoppen.
2) Klicken Sie auf die Schaltfläche Übernehmen. Die Aktion wird gestoppt.

6.2.4 OS-Update

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** OS-Update

In diesem Menü gibt es die folgende Auswahlmöglichkeit:

1) *OS-Update Einstellungen*

OS-Update Aktionen

6.2.4.1 OS-Update Einstellungen

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** OS-Update **>** OS-Update Einstellungen

Der Dialog OS-Update Einstellungen wird angezeigt. In diesem Dialog können die Transferparameter vom zentralen Host für das Update des STMIX OS (Operating System) eingestellt werden.

P2P-Transferparameter vom zentralen Host (Standalone SoftGates und STMIX)

- *Max. Downloadgeschwindigkeit beschränken:* Kontrollkästchen aktivieren/deaktivieren. Die maximale Downloadgeschwindigkeit für das Update des OS kann auf den Wert, der im darunterstehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Downloadgeschwindigkeit (KB/s):* Eingabefeld für die maximale Downloadgeschwindigkeit in KByte je Sekunde
- *Max. Uploadgeschwindigkeit beschränken:* Kontrollkästchen aktivieren/deaktivieren. Die maximale Uploadgeschwindigkeit für das Update des OS kann auf den Wert, der im darunterstehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Uploadgeschwindigkeit (KB/s):* Eingabefeld für die maximale Uploadgeschwindigkeit in KByte je Sekunde

Schaltflächen

- Übernehmen: Die Eingaben werden gespeichert.

- Rückgängig: Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

6.2.4.2 OS-Update Aktionen

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** OS-Update **>** OS-Update Aktionen

Der Dialog OS-Update Aktionen wird angezeigt. In diesem Dialog kann der Transfer vom zentralen Host für das Update des OS (Operating System) abgebrochen werden.

Wichtig: Diese Einstellungen sind mit OpenScape 4000 V7R1 bei einzelnstehenden SoftGates noch nicht möglich. Benutzen Sie stattdessen die Funktion 'Remote Appliance Reinstall (RAR)â.

OS-Update Transfer vom zentralen Host (nur Standalone SoftGates)

Schaltfläche:

- *Transfer abbrechen:* Der Transfer der OS-Software wird abgebrochen.

OS-Update Aktivierung

- *Platform Version*: Anzeige der Plattform-Version des STMIX.
- *Importierte Platform Version*: Anzeige der importierten Plattform-Version des STMIX
- *OS-Update Status:* Anzeige, ob ein neues Update-Packet für das OS verfügbar ist.
- *SoftGate-LW aus dem Updatepaket verwenden (empfohlen):* Aktivierbar/ Deaktivierbar. Wenn diese Option nicht ausgewählt ist, bleibt die aktuell installierte SoftGate LW / STMIX-Anwendung nach dem OS-Update erhalten.

Schaltfläche:

- *OS-Update aktivieren:* Das OS-Update aktivieren.

6.3 Backup/Restore

Im Menü *Backup/Restore* kann die Konfiguration und die STMIX-Konfiguration lokal gesichert (exportiert) werden. Diese lokale Sicherung kann geladen (importiert) und anschließend aktiviert werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore*

Das Menü *Backup/Restore* wird geöffnet.

Menü *Backup/Restore*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Export Konfiguration*

   Export Sicherheitskonf.

6.3.1 Export Konfiguration

WBM-Pfad

WBM > *Wartung* > Backup/Restore > *Export Konfiguration* > *Konfiguration exportieren*

Der Dialog *Konfiguration exportieren* wird angezeigt. In diesem Dialog kann die STMIX-Konfiguration lokal gesichert (exportiert) werden. Diese Sicherung enthält auch den SIP-Teil

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Das Exportieren der Konfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Konfiguration wird abgebrochen.

Vorgehen

Führen Sie zum Exportieren der Konfiguration die folgenden Schritte durch:

1) Klicken Sie auf *Übernehmen*. Die Sicherheitskonfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster *Dateidownload* mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2) Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

6.3.2 Export Sicherheitskonf.

WBM-Pfad

WBM > *Wartung* > Backup/Restore > *Export Sicherheitskonf.* > *Sicherheitskonfiguration exportieren*

Der Dialog *Sicherheitskonfiguration exportieren* wird angezeigt. In diesem Dialog kann die STMIX-Konfiguration (einschl. SIP-Sicherheitskonfiguration) lokal gesichert (exportiert) werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Übernehmen: Das Exportieren der Konfiguration wird gestartet.
- Rückgängig: Das Exportieren der Konfiguration wird abgebrochen.

Vorgehen

Führen Sie zum Exportieren der Sicherheitskonfiguration die folgenden Schritte durch:

1) Klicken Sie auf Übernehmen. Die Konfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster Dateidownload mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.

2) Klicken Sie auf die Schaltfläche Speichern und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche OK. Die zip-Datei wird gespeichert.

6.3.3 Import Konfiguration

WBM-Pfad

WBM **>** *Wartung* **>** Backup/Restore **>** *Import Konfiguration* **>** *Konfiguration importieren*

Der Dialog *Konfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte STMIX-Konfiguration wieder importiert werden.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Konfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Konfigurationsdatei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Importieren einer Konfigurationsdatei die folgenden Schritte durch:

1) Geben Sie den Pfad und den Namen der Konfigurationsdatei ein oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2) Klicken Sie auf die Schaltfläche *Laden*. Die Konfigurationsdatei wird geladen.

Damit alle Konfigurationsänderungen wirksam werden, muss STMIX neu gestartet werden.

6.3.4 Import Sicherheitskonf.

WBM-Pfad

WBM **>** *Wartung* **>** Backup/Restore **>** *Import Sicherheitskonf.* **>** *Sicherheitskonfiguration importieren*

Der Dialog Sicherheitskonfiguration importieren wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte STMIX-Sicherheitskonfiguration wieder importiert werden.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- Dateiname: In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Sicherheitskonfiguration enthält. Über die Schaltfläche Durchsuchen kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Laden: Die angegebene Datei wird geladen.
- Rückgängig: Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Importieren einer Sicherheitskonfiguration die folgenden Schritte durch:

- Geben Sie den Pfad und den Namen der Datei ein, welche die zu importierende Sicherheitskonfiguration enthält oder wählen Sie über die Schaltfläche Durchsuchen die Datei aus.
- Klicken Sie auf die Schaltfläche Laden. Die Datei wird geladen.

Wichtig: Damit alle Konfigurationsänderungen wirksam werden, muss STMIX neu gestartet werden.

6.3.5 Import klassischer STMI-Sicherungsdaten in STMIX

WBM-Pfad

Klassische STMI-Sicherungsdaten lassen sich mit dem vorhandenen Importmechanismus in STMIX importieren:

Maintenance > Backup/Restore > Import Config (Wartung > Sichern/ Wiederherstellen > Importkonfig.)

Anmerkung: Der automatische HBR-Wiederherstellungsmechanismus über den Assistenten funktioniert auch, wenn eine STMI-Platine durch eine STMIX-Platine ersetzt wird.

Implementierung

Die folgenden Daten werden von STMI in STMIX importiert:

- Status und Parameter des aktiven SIP-Leitungsprofils
- SIP-Parameter
- Konfiguration der Codecs

Die SPE-Konfiguration erfolgt über DLS oder Assistent.

Die STMI-Sicherung basiert auf einer Datei namens export.xml. Der STMIX akzeptiert ZIP-Dateien, die eine Datei mit diesem Namen enthalten.

Eine positive HBR-Wiederherstellung wird durch die folgende HISTA-Meldung bestätigt:

```
F5749 E8 N4394 NO ACT   BPA   BOARD    LW REQUEST              21-10-21 08:49:09
      ALARM CLASS:CENTRAL:002
        **  :LTG1 :LTU99:005: 00    : 0 Q2343-X    STMIX/1    BST:01  PLS:-02
      FORMAT:43
      REASON:00H  ONLY SIGNALING
      HBR AUTO-RESTORE WARN
      CLASSIC STMI BACKUP IMPORTED TO STMIX, A NEW HBR BACKUP SHOULD
      BE INITIATED.
```

Abbildung 3: HISTA-Nachricht F5749

Anmerkung:

Diese Meldung ist bei einer Wiederherstellung über das WBM nicht sichtbar.

Nach dem Import wird das Erstellen einer neuen HBR-Sicherung empfohlen.

Ein Beispiel für ein von der STMI-Platine importiertes SIP-Profil ist in der folgenden Abbildung dargestellt:

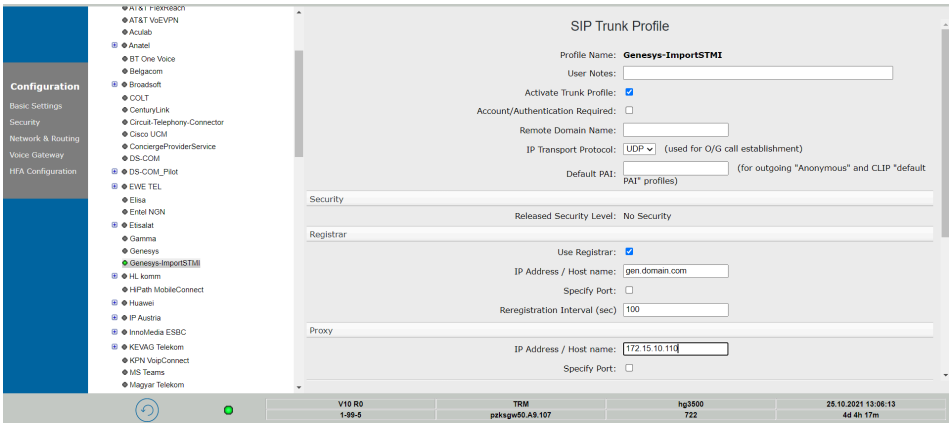


Abbildung 4: SIP-Leitungsprofil

6.3.6 Rücksetzen auf Werkseinstellung

WBM-Pfad

WBM>Wartung > Sichern/Wiederherstellen >Werksreset

Das Dialogfeld **Konfiguration auf Werkseinstellungen zurücksetzen** wird angezeigt.

Mit diesem Dialogfeld können Sie die STMIX/STMIY-Platine auf die Werkseinstellungen zurücksetzen.

Warnung:

Durch die Auswahl von Werksreset wird die Platine heruntergefahren.

Schaltflächen

In diesem Dialogfeld wird die folgende Schaltfläche angezeigt:

- **Zurücksetzen auf Werkseinstellungen**: Starten Sie den Werksreset.

Prozedur

Um den Werksreset auszulösen, befolgen Sie die folgenden Schritte:

1) Klicken Sie auf **Zurücksetzen auf Werkseinstellungen.** Dadurch wird die Prozedur im Hintergrund ausgelöst und die Platine wird nach Abschluss der Prozedur heruntergefahren.
2) Entfernen Sie die Platine nach dem Reset.

6.4 Logs

Im Menü *Protokolle* können für Diagnosezwecke die Protokolldateien in eine zip-Datei exportiert werden. Zum Anlegen neuer Protokolldateien ist das Löschen der alten, d. h. exportierten, Protokolldateien möglich.

WBM-Pfad

WBM **>** *Wartung* **>** *Logs*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Logs exportieren*

   Logs löschen

   Trace-Profile

6.4.1 Logs exportieren

WBM-Pfad

WBM **>** *Wartung* **>** *Logs* **>** *Logs exportieren* **>** *Protokolldateien exportieren*

Der Dialog *Protokolldateien exportieren* wird angezeigt. In diesem Dialog können die STMIX-Protokolldateien lokal gespeichert (exportiert) werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Exportieren: Die über die Kontrollkästchen ausgewählten Protokolldateien werden lokal gesichert (exportiert).

Vorgehen

Führen Sie zum Exportieren von Protokolldateien die folgenden Schritte durch:

1) Klicken Sie auf die Schaltfläche Exportieren. Die Protokolldateien werden in eine zip-Datei exportiert. Es erscheint eine Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2) Klicken Sie auf die Schaltfläche Speichern und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche OK. Die zip-Datei wird gespeichert.

6.4.2 Logs löschen

WBM-Pfad

WBM > *Wartung* > *Logs* > *Logs exportieren* > Logs löschen > *Protokolldateien löschen*

Der Dialog Protokolldateien löschen wird angezeigt. In diesem Dialog können die aufgelisteten Protokolldateien einzeln oder insgesamt markiert und gelöscht werden.

Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen:

- *Soco, JLM, IMS, SPA, ETS, Status Collector, Update, Backtrace, Heap-Dump, Corelogs, Garbage collection, Gateway (vHG) Logs, LS-DCL, Load-Balancer, DHCP, System Diagnostics*
- *Alles:* Es werden alle Protokoll-(Diagnose)dateien markiert.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Löschen:* Alle über die Kontrollkästchen markierten Protokolldateien werden gelöscht.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

Vorgehen

Führen Sie zum Löschen von Protokolldateien die folgenden Schritte durch:

1) Aktivieren Sie die Kontrollkästchen derjenigen Protokolldateien, die Sie löschen möchten.
2) Klicken Sie auf die Schaltfläche Löschen. Die markierten Protokolldateien werden gelöscht.

6.4.3 Trace-Profile

WBM-Pfad

WBM > *Wartung* > *Logs* > Trace-Profile > *Trace-Profile-Konfiguration editieren*

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

Der Dialog *Trace-Profile-Konfiguration editieren* wird angezeigt. In diesem Dialog können Trace-Profile für eine detaillierte Analyse des STMIX aktiviert werden. Durch jedes Trace-Profil werden spezielle Informationen aufgezeichnet. Die Trace-Profileinstellungen werden während des Loadware- oder OS-Updates auf die Default-Werte zurückgesetzt.

Trace-Profile

Durch Aktivierung der hier genannten Trace-Profile können die folgenden Probleme untersucht werden:

- *acw-cc:* Entwickler-spezifisch
- *cg:* Entwickler-spezifisch
- *dataloading:* Entwickler-spezifisch
- *dcl2:* Entwickler-spezifisch
- *debug-all:* Entwickler-spezifisch
- *dls-client:* Entwickler-spezifisch
- *dmc-detail:* Entwickler-spezifisch
- h323-performance:
- *heap-diag:* Entwickler-spezifisch
- *hfa-call:* Wird verwendet bei Problemen mit der Signalisierung von HFA-Verbindungen und dem An- und Abmelden der HFA-Endgeräte.
- *hfa-reg:* Wird verwendet bei Problemen mit der Registrierung der HFA-Endgeräte, z. B. bei fehlerhaften Anzeigen in den Endgeräte-Displays.
- *ipconfig:* Entwickler-spezifisch
- *ipv6:* Wird verwendet, wenn Probleme bei der Vernetzung über IP V6 bestehen.
- *icphone:*
- *maintenance:* Entwickler-spezifisch
- *osa:* Trace-Profil für OpenScape Access
- *osa-clock:* Trace-Profil für OpenScape Access
- *osa-light:* Trace-Profil für OpenScape Access
- *osa-trace:* Trace-Profil für OpenScape Access
- *payload:* Wird verwendet bei Problemen mit der Sprachdurchschaltung (wie payload-light). Beeinträchtigt die Leistung des Systems! Aufgrund der Erzeugung umfangreicher Trace-Ausgaben darf dieses Profil nicht bei hoher Systemlast aktiviert werden.
- *payload-light:* Wird verwendet bei Problemen mit der Sprachdurchschaltung. Kann bei erhöhter Systemlast aktiviert werden. Siehe auch Absatz 'payload'.
- *payload-native:* Entwickler-spezifisch
- *qdc:* Entwickler-spezifisch
- *reconnect:* Entwickler-spezifisch
- *scc:* Wird verwendet bei allgemeinen Payload-Problemen, bei Konferenz-Verbindungen und bei IPDA-Verbindungen.
- *sip:* Nach Aktivierung dieses Trace-Profils werden die STMIX - SIP Trace-Meldungen, die im lokalen STMIX - SIP WBM konfiguriert wurden, in die SoftGate-Protokolldatei übernommen. Gleichzeitig werden die SIP-relevanten scc-Traces aufgezeichnet.
- snmp:
- *startup:* Wird verwendet bei Hochlaufproblemen des SoftGates und der virtuellen Baugruppen.
- stmix:
- *system:* Dieses Traceprofil ist immer aktiviert und kann nicht ausgeschaltet werden.
- *thread-profiling:* Entwickler-spezifisch
- *wbm:* Entwickler-spezifisch

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Übernehmen: Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.

- Rückgängig: Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden auf die Default-Einstellungen zurückgesetzt.
- *Standard wiederherstellen:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden auf die Default-Einstellungen zurückgesetzt.

Vorgehen

Führen Sie zum Aktivieren von Trace-Profilen die folgenden Schritte durch:

1) Aktivieren Sie die Kontrollkästchen derjenigen Trace-Profile, die Sie für eine Analyse benötigen.
2) Klicken Sie auf Übernehmen. Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.

6.5 Secure Trace

Ein Secure Trace dient zum Ermitteln von Störungen im Kommunikationssystem. Durch den Secure Trace werden Aufzeichnungen über verschlüsselte VoIP-Nutz- und Signalisierungsdatenströme vom und zum STMIX - HFA angefertigt.

Der Secure Trace enthält verschlüsselte Aufzeichnungen. Diese Aufzeichnungen können vom Entwickler durch einen Schlüssel entschlüsselt werden.

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace

Das Menü *Secure Trace* wird angezeigt.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Zertifikat importieren*

   Zertifikat anzeigen

   Status

   Trace starten

   Trace stoppen

Prinzipieller 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) Die Entwicklung 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 bzw. kann von der HiSat Homepage (https://hisat.global-intra.net/wiki/index.php/SecureTrace) heruntergeladen werden.

5) Der Servicetechniker informiert den Kunden über den Beginn der Trace-Aktivitäten. Der Kunde muss die betroffenen Teilnehmer informieren.

Wichtig: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, wenn die betroffenen Teilnehmer nicht informiert wurden!

---

1) Der Servicetechniker stellt dem Gateway vHG 3500 HFA, für das ein Secure Trace zu erstellen ist, das Zertifikat zur Verfügung; siehe Abschnitt 6.14.1, 'Zertifikat importieren'.

2) Der Servicetechniker aktiviert die Secure Trace-Funktion, siehe Abschnitt 6.14.4, 'Trace starten'. Ein Secure Trace wird erstellt. Die Aktivierung und die spätere Deaktivierung (Abschnitt 6.14.5, 'Trace stoppen') werden von den beteiligten Kommunikationssystemen 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.

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.

6.5.1 Zertifikat importieren

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace **>** *Zertifikat importieren* **>** *Laden des Secure Trace Zertifikats über HTTP*

Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
In diesem Dialog kann ein Secure Trace-Zertifikat importiert werden. Dieses Zertifikat ist die Voraussetzung dafür, dass ein Secure Trace erstellt werden kann. Der Servicetechniker bekommt es vom Entwickler. Es enthält den öffentlichen Schlüssel und muss im PEM- oder im binären Format vorliegen. Das Zertifikat ist maximal einen Monat gültig.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Datei mit dem Zertifikat (PEM- oder Binär-Format):* In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält die folgenden Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehen

Führen Sie zum Importieren des Zertifikats die folgenden Schritte durch:

1) Wählen Sie: *WBM* **>** *Wartung* **>** Secure Trace **>** Zertifikat importieren. 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 *Ã–ffnen*. Die Datei wird geladen.

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

4) **a)** 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.

5) 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.

6.5.2 Zertifikat anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace **>** Zertifikat anzeigen **>** *Zertifikatsinformationen*

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialog kann das Secure Trace-Zertifikat angezeigt werden, z. B. um es zu überprüfen.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- *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*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Ã–ffentlicher Schlüssel*, *Fingerabdruck*

6.5.3 Status

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace **>** Status **>** *Secure Trace Status*

Der Dialog *Secure Trace Status* wird angezeigt. In diesem Dialog können Sie feststellen, ob gerade ein Secure Trace erstellt wird.

Angezeigte Daten

Es werden die folgenden Daten angezeigt:

- *Secure Trace aktiviert*: Diese Zeile zeigt an, ob gerade ein Secure Trace erstellt wird.
- *Automatischer Deaktivierungszeitpunkt*: Diese Zeile zeigt an, wann der Secure Trace voraussichtlich erstellt ist und die Secure Trace-Funktion automatisch deaktiviert wird.

Secure Trace für folgende Protokolle: Diese Zeile zeigt an, für welche Protokolle der Secure Trace erstellt wird. Das kann sein: Media Server (SRTP).

6.5.4 Trace starten

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace **>** Trace starten **>** *Secure Trace einschalten*

Der Dialog *Secure Trace einschalten* wird angezeigt. In diesem Dialog kann der Secure Trace gestartet werden. Dazu müssen 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.
- Sie haben einen öffentlichen Schlüssel vom Entwickler bekommen und in das WBM geladen.

Eingabefelder und Kontrollkästchen

- *Start Parameter*:
- – *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.

  Eine Passphrase ist ein aus mehreren Wörtern bestehendes Passwort mit einer maximalen Länge von 20 Zeichen.

  – *Dauer des Secure Trace (Min.)*: Das Eingeben der Dauer des Secure Trace (in Minuten) ist unbedingt erforderlich.
- *Secure Trace für folgende Protokolle*:
- – *MMX (PEP)*: Der Secure Trace für MMX wird erstellt. Das Protokoll PEP (Protocol Extension Protocol) erweitert HTTP für Applikationen wie z. B. HTTP-Clients, Server und Proxy-Server.
  – *MediaServer (SRTP)*: Der Secure Trace für MediaServer wird erstellt. Das Protokoll SRTP (Secure Real-Time Transport Protocol) dient der

verschlüsselten Übertragung über IP-basierte Netze und verwendet AES (Advanced Encryption Standard) für die Verschlüsselung.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace einschalten*: Der Secure Trace wird gestartet. Die oben genannten Voraussetzungen für das Starten des Secure Trace müssen vorliegen.

Vorgehen

Führen Sie zum Starten des Secure Trace die folgenden Schritte durch:

1) Prüfen Sie, ob die oben genannten Voraussetzungen vorliegen.
2) Wählen Sie: *WBM* **>** *Wartung* **>** Secure Trace **>** Trace starten. Der Dialog *Secure Trace einschalten* wird angezeigt.
3) Geben Sie im Bereich *Start Parameter* die *Secure Trace Aktivierungs-Passphrase* und die *Dauer des Secure Trace (Min.)* ein.
4) Aktivieren Sie das Protokoll *MediaServer (SRTP)*.

Klicken Sie auf die Schaltfläche *Secure Trace einschalten*. Der Secure Trace wird für die angegebene Zeitdauer erstellt.

6.5.5 Trace stoppen

WBM-Pfad

WBM **>** *Wartung* **>** Secure Trace **>** Trace stoppen **>** *Secure Trace beenden*

Der Dialog *Secure Trace beenden* wird angezeigt. In diesem Dialog kann ein laufender Secure Trace gestoppt werden, wenn die unter Trace starten festgelegte Zeitdauer noch nicht abgelaufen ist.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

Secure Trace beenden: Der Secure Trace wird gestoppt.

6.6 DLS Client

1) Der DLS-Client dient der Administration von PKI-Daten und der QDC-Konfiguration (DLS: **D**ep**l**oyment **S**ervice oder **D**eployment- und **L**icencing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

Anmerkung: Der DLS-Client kann nur im WBM des STMIX - HFA konfiguriert werden. Die Konfigurationen werden an den STMIX - SIP/IPDA-Teil verteilt.

WBM-Pfad

WBM **>** *Wartung* **>** DLS Client

Der Menü *DLS-Client* wird angezeigt.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *DLS Einstellungen*

PIN Eingabe

Bootstrapping zurücksetzen

DLS kontaktieren

Bootstrapping

Durch das Bootstrapping soll eine auf Zertifikaten basierende zuverlässige SSL-Verbindung zwischen DLS-Server und DLS-Client aufgebaut werden.

Ausgehend von einer Verbindungsanfrage des DLS-Clients an einen DLS-Server sowie der darauffolgenden Antwort â“also einer noch unzuverlässigen Verbindungâ“, wird über die wechselseitige Authentifizierung und den Austausch von Zertifikaten eine zuverlässige Verbindung aufgebaut (d. h. Bootstrapping = ein einfaches System entwickelt sich zu einem komplexen System aus sich selbst heraus).

Da sich auf die Verbindungsanfrage des DLS-Clients anstatt des gewollten DLS-Servers auch ein anderer DLS-Server melden könnte, um die gewünschte Verbindung an sich zu ziehen, sind Sicherungsmaßnahmen notwendig. Mittels AMO kann der DLS-Server (d. h. dessen IP-Adresse und Port) administriert werden, den der DLS-Client kontaktieren soll.

Es wird empfohlen, den DLS-Client gegenüber dem DLS-Server durch Eingeben einer Bootstrap-PIN am STMIX WBM, die zuvor vom DLS-Server per Zufall generiert wurde, zu autorisieren. Die Autorisierung des DLS-Clients kann auch mit einer nicht einzugebenden systeminternen Standard-PIN erfolgen, oder auf die Autorisierung mittels PIN kann auch ganz verzichtet werden. Diese beiden Möglichkeiten werden jedoch nicht empfohlen.

Nach dem Herstellen der zuverlässigen Verbindung werden die Zertifikate ausgetauscht, s. u.

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 Bootstrappings 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.

Zertifikatsgenerierung und -verteilung für die sichere Verbindung des WBM zum DLS-Server:

Der Administrator sendet manuell das von der Kunden PKI-Zertifizierungsstelle erstellte WBM-Zertifikat, das den privaten Schlüssel enthält, zum OpenScape 4000 Assistant. OpenScape 4000 Assistant Der sendet dann automatisch sein WBM-Zertifikat zu allen CGWs. Mit diesem Zertifikat weist sich dann der DLS-Client gegenüber dem DLS-Server aus.

6.6.1 DLS Einstellungen

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-Modus bekannt sein. Die IP-Adresse und der Port des DLS-Servers können mittels AMO konfiguriert werden. Diese Änderung wird erst nach einem Neustart des STMIX wirksam.

Nach Setzen von IP-Adresse und Port des DLS-Servers erfolgt beim Neustart (und jedem weiteren Neustart) ein einmaliger Versuch, durch Senden einer Verbindungsanfrage das Bootstrapping einzuleiten.

Unter dem 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 **>** *Wartung* **>** DLS Client **>** DLS Einstellungen **>** *DLS Client Grundeinstellung ändern*

Der Dialog *DLS Client Grundeinstellung ändern* wird geöffnet.

Eingabefeld

Im Bereich *Aktuelle DLS Client Grundeinstellung* gibt es folgendes Eingabefeld:

- *Zeitintervall für ContactMe-Antwort*: Zeit, die der DLS-Client nach Absenden seiner Verbindungsanfrage wartet, um die ContactMe-Antwort vom DLS-Server zu erhalten. Die Wartezeit muss begrenzt sein, damit ContactMe-Antworten von ungewollten DLS-Servern nicht empfangen werden können.

Anzeigen

In diesem Dialog gibt es die folgenden Anzeigen:

- *Aktuelle DLS Client Grundeinstellung*:
- – *PIN für DLS-Bootstrapping erforderlich*: Die PIN kann unter dem Menüpunkt *PIN Eingabe* eingegeben werden. *Ja*: Es wurde eine PIN eingegeben. *Nein*: es wurde keine PIN eingegeben.
  – *Sichere Kommunikation mit DLS-Server*: *Aktiviert* oder *Deaktiviert*
- *Aktuelle DLS Client Server Einstellung*:
- – *IP-Adresse des DLS-Servers*: IP-Adresse des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. STMIX muss neu gestartet werden.
  – *Port des DLS-Servers*: Port des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. STMIX muss neu gestartet werden.
  – *Port für sichere Verbindung zum DLS-Server*: STMIX-Port für eine sichere Verbindung zum DLS-Server Der *Port für die sichere Verbindung* kann per AMO konfiguriert werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.

- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

6.6.2 PIN Eingabe

WBM-Pfad

WBM > *Wartung* > DLS Client > PIN Eingabe > *Eingabe der Bootstrap PIN*

Der Dialog *Eingabe der Bootstrap PIN* wird geöffnet. In diesem Dialog kann die vom DLS-Server per Zufall generierte Bootstrap PIN eingegeben werden.

Eingabefeld

In diesem Dialog gibt es folgendes Eingabefeld:

- *Bootstrap PIN*: Wenn in dieses Eingabefeld eine PIN eingegeben und durch Klicken auf *Übernehmen* gespeichert wurde, wird im Dialog *DLS Client Grundeinstellung ändern* (Menüpunkt *DLS Einstellungen*) angezeigt, dass für das DLS-Bootstrapping eine PIN erforderlich ist.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

6.6.3 Bootstrapping zurücksetzen

WBM-Pfad

WBM > *Wartung* > DLS Client > *Bootstrapping zurücksetzen* > *DLS Client Bootstrapping zurücksetzen*

Der Dialog *DLS Client Bootstrapping zurücksetzen* wird geöffnet.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Bootstrapping zurücksetzen*: Das Bootstrapping des DLS-Clients wird zurückgesetzt.

6.6.4 DLS kontaktieren

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche zum DLS-Server 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 > *Wartung* > DLS Client > DLS kontaktieren

Der Dialog *DLS kontaktieren* wird geöffnet.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *DLSC Client-Zertifikate*

DLSC CA-Zertifikate

Dialog *DLS kontaktieren*

In diesem Dialog gibt es folgende Schaltfläche:

1) *Kontaktieren*: Der DLS-Server wird kontaktiert, um zu überprüfen, ob er noch verfügbar ist.

6.6.4.1 DLSC Client-Zertifikate

Unter diesem Menüpunkt befinden sich die DLSC Client-Zertifikate mit dem privaten Schlüssel. Mit diesen Zertifikaten weist sich der DLS-Client gegenüber dem DLS-Server aus. Während des Bootstrapping-Modus bekommt der DLS-Client das Zertifikat vom DLS-Server.

WBM-Pfad

WBM **>** *Wartung* **>** DLS Client **>** DLS kontaktieren **>** DLSC Client-Zertifikate

Das Menü DLSC Client-Zertifikate wird geöffnet.

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

6.6.4.2 1. DLSC Client-Zertifikat

WBM-Pfad

WBM **>** *Wartung* **>** DLS Client **>** DLS kontaktieren **>** DLSC Client-Zertifikate **>** *1. DLSC Client-Zertifikat* **>** *Zertifikatsinformationen*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *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*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Ã–ffentlicher Schlüssel*, *Fingerabdruck*

6.6.5 DLSC CA-Zertifikate

WBM-Pfad

WBM **>** *Wartung* **>** DLS Client **>** DLS kontaktieren **>** *DLSC CA-Zertifikate*

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

Das Menü *DLSC CA-Zertifikate* wird geöffnet.

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

'1. DLSS CA-Zertifikat', '2. DLSC CA-Zertifikat'

6.6.5.1 '1. DLSS CA-Zertifikat', '2. DLSC CA-Zertifikat'

WBM-Pfad

WBM **>** *Wartung* **>** DLS Client **>** DLS kontaktieren **>** *DLSC CA-Zertifikate* **>** *'1. DLSS CA-Zertifikat', '2. DLSC CA-Zertifikat'*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *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*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Ã–ffentlicher Schlüssel*, *Fingerabdruck*

6.7 Diagnose

Unter *Diagnose* können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen und Diagnose-Dateien erstellt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose*

Das Menü *Diagnose* wird geöffnet.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Diagnose-Funktionen*

Diagnose-Dateien

6.7.1 Diagnose-Funktionen

WBM-Pfad

WBM > *Wartung* > *Diagnose* > Diagnose-Funktionen

Der Dialog *Diagnose-Funktionen* wird angezeigt. In diesem Dialog können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen werden, und zwar für die interne LAN Capture-Kontrolle, für das Thread Profiling und für die Heap-Überwachung.

Bereiche

In diesem Dialog gibt es die folgenden Bereiche:

1) *Interne LAN Capture-Kontrolle*

Thread-Profiling

Heap-Überwachung

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Übernehmen: Die geänderten Einstellungen werden gespeichert.
- Rückgängig: Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

Interne LAN Capture-Kontrolle

In diesem Bereich können Einstellungen für die interne Überwachung von IP-Paketen im LAN vorgenommen werden. Diese Überwachung erfolgt z. B. mit tshark oder tcpdump. Im Falle eines kritischen Neustarts wird der aktuelle Inhalt in die Backtrace-Datei geschrieben. Beim Starten der Überwachung werden ältere Capture-Dateien gelöscht. Falls diese noch benötigt werden, müssen Sie über *Logs* > *Logs exportieren* einen Export durchführen.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
- – *Nur Headers:*Es sollen nur die Header der IP-Pakete überwacht werden.
  – *Start:* Die interne LAN Capture-Kontrolle soll gestartet werden.
  – LoopBack-Schnittstelle (nur): Es soll nur die LoopBack-Schnittstelle benutzt werden.
- Auswahlfeld:
- – *Filter:*Ein Filter zum Überwachen von IP-Paketen kann ausgewählt werden. Auswählbar sind:
  – – *kein* (kein Filter)
  – *tcp* (nur IP-Pakete des Transmission Control Protocol)
  – *udp* (nur IP-Pakete des User Datagram Protocol)
- Anzeige:
- – *Status:* Es wird angezeigt, ob die interne LAN Capture-Kontrolle aktiv ist.

Thread-Profiling

Mit dem Thread Profiling kann überprüft werden, ob Threads die CPU, wie geplant, ausnutzen. D. h. ob ein Thread, von dem man eine niedrige CPU-Belastung erwartet, dies auch wirklich tut.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
- – *Start:* Das Thread Profiling soll gestartet werden.
- Eingabefelder:
- – *Sample Rate, ms (100-500):* Die Abtastrate kann eingestellt werden, Default ist 250.
  – *Thread-CPU-Nutzung-Grenzwert für Stacktrace, % (10-90):* Es kann eingestellt werden, wie hoch die maximale CPU-Nutzung sein soll, Default ist 50.
- Anzeige:
- – *Status:* Es wird angezeigt, ob das Thread Profiling aktiv ist.

Heap-Überwachung

Durch das Erzeugen eines Heap-Dumps können alle Objekte, die sich auf dem Heap befinden, in eine Datei geschrieben werden.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
- – *Start:* Die Heap-Überwachung soll gestartet werden.
- Eingabefelder:
- – Sample Rate, ms (500-5000): Die Abtastrate kann eingestellt werden, Default ist 1000.
  – Speichergebrauch-Grenzwert für Heapdump, % (50-90): Es kann eingestellt werden, wieviel Speicher für den Heapdump genutzt werden kann, Default ist 80.
- Anzeige:
- – *Status:* Es wird angezeigt, ob die Heap-Überwachung aktiv ist.

6.7.2 Diagnose-Dateien

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** Diagnose-Dateien

Der Dialog *Diagnose-Dateien* wird angezeigt.

Auf der RAM-Disk, d. h. einem virtuellen temporären Datenträger im Arbeitsspeicher, werden Protokolldateien abgelegt. Diese Protokolldateien können ausgelesen und in eine Archivdatei gepackt werden. Eine Backtrace-Datei enthält den Inhalt des Stacks im Moment des Erzeugens.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- Heap-Dump Erzeugen: Erzeugt eine Datei, die alle im Moment des Erzeugens erreichbaren Java-Objekte enthält. Anhand dieser Datei lässt sich der Arbeitsspeicherverbrauch analysieren.

Anmerkung: Die Backtrace-Archivdatei (Inhalt der RAMDISK/ramdisk.zip) enthält alle Protokolldateien der RAM-Disk und ist nun beim gewöhnlichen Log-Export enthalten.

6.8 Status-Information

WBM-Pfad

WBM **>** *Wartung* **>** Status-Information

Das Menü *Status-Information* wird geöffnet.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *System-Information*

SoftGate-Verbindungskontrolle

6.8.1 System-Information

WBM-Pfad

WBM **>** *Wartung* **>** Status-Information **>** System-Information

Das Menü System-Information wird geöffnet.

Angezeigt wird die folgende Option:

Thread Zustände anzeigen

6.8.1.1 Thread Zustände anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** Status-Information **>** System-Information **>** Thread Zustände anzeigen **>** *Thread Zustände*

Die Tabelle *Thread Zustände* wird angezeigt. In dieser Tabelle werden die gerade aktiven Threads angezeigt. Dazu werden folgende Angaben gemacht: *Thread Name, Thread ID, Hashcode Kontextklasse, blockierte Zeit [ms], max. blockierte Zeit [ms].*

6.8.2 SoftGate-Verbindungskontrolle

WBM-Pfad

WBM **>** *Wartung* **>** Status-Information **>** SoftGate-Verbindungskontrolle

Das Menü *SoftGate-Verbindungskontrolle* wird geöffnet.

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

1) *Alle Verbindungen anzeigen*

6.8.2.1 Alle Verbindungen anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** Status-Information **>** SoftGate-Verbindungskontrolle **>** Alle Verbindungen anzeigen **>** *SCC-Verbindungsliste*

Die Tabelle *SCC-Verbindungsliste* wird angezeigt. In dieser Tabelle werden alle gerade aktiven SCC-Verbindungen angezeigt. Dazu werden folgende Angaben gemacht: Baugruppe, Typ.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Autom. Aktualisierung: Aktivierbar/Deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, in wieviel Sekunden die Verbindungsliste automatisch aktualisiert wird.

6.9 Reboot OS

WBM-Pfad

WBM **>** *Wartung* **>** Reboot OS

Das Menü *Reboot OS* wird geöffnet.

6.9.1 Reboot OS

WBM-Pfad

WBM **>** *Wartung* **>** Reboot OS

In diesem Fenster kann das Betriebssystem des STMIX neu gestartet werden.

Schaltfläche

- Reboot OS: Durch Klicken auf diese Schaltfläche wird das Betriebssystem des STMIX heruntergefahren und dann automatisch neu gestartet.

7 SIP/IPDA WBM - Wartung

7.1 Wartung

In diesem Modul finden Sie Funktionen, die für die Wartung und Administration des HG 3500 auf STMIX über SIP/IPDA 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)*

7.2 Konfiguration und Update

7.2.1 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*

Konfiguration auf Lieferzustand zurücksetzen

7.2.2 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.

Der Export der SIP-Konfiguration ist ein Diagnosemechanismus für Experten. Der normale Backup & Restore erfolgt über das STMIX HFA WBM.

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*

7.2.2.1 Laden vom Gateway

Dies ist die Backup-Funktion. Sie können die aktuelle Konfiguration des STMIX - SIP an einem 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 â“ abhängig vom zur Verfügung stehenden Speicherplatz â“ 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*:
- – *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*
- *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*
- *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: *DSP-Kanalkonf.*
- *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*, *Endpunktregistrierung*
- *SIP-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: *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: *Globale Trace-Informationen*, *Ereignisprotokollkonf.*, *Ereignisreaktionstabelle, Trap-Ziel,* , *Trap-Ziel*, *E-Mail-Liste*, *Konf. Trace über LAN*
- *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*, *Port-Administration (Global)*, *Port-Administration (Lokal)*, *Versionsinformationen*, *Globale Netzwerk-Routing-DatenCodecs*, *Ziel-Codecs*, *Class Mark*, *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.

7.2.2.2 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 â“ falls erforderlich â“ einen Neustart durch (Reset-Symbol beachten! Siehe auch Section 3.3.2, "Symbole im Steuerbereich des WBM-Fensters").

Wichtig: 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 7.3, "Auftragsliste").

7.2.3 SSL-Daten

Die SSL/SPE-Konfigurationsdaten für SIP 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*

7.2.3.1 Laden vom Gateway

Anmerkung: Normale Backups erfolgen im Rahmen der HFA-Wartung.

WBM-Pfad:

WBM **>** *Wartung* **>** *Konfiguration und Update* **>** *Konfiguration* **>** *SSL-Daten* **>** *Laden vom Gateway* **>** *Laden der SSL/SPE-Konfigurationsdaten vom Gateway über HTTP*

Der Dialog *Laden der 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 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.

7.2.3.2 Laden zum Gateway

Dies ist die Restore-Funktion. Sie können eine extern gespeicherte Konfiguration zum Gateway laden.

Anmerkung: Normale Restores erfolgen im Rahmen der HFA-Wartung.

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 â“ falls erforderlich â“ einen Neustart durch (Reset-Symbol beachten. Siehe auch Section 3.3.2, "Symbole im Steuerbereich des WBM-Fensters").

Wichtig: 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 7.3, "Auftragsliste").

7.2.4 Konfiguration auf Lieferzustand zurücksetzen

Sie können die SIP-Konfiguration 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:

Anmerkung: Diese Aktion setzt die komplette SIP-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 STMIX führt während dieser Aktion einen automatischen Reboot durch.

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.

7.4 Traces und Ereignisse (Events)

In diesem Abschnitt werden Traces und Ereignisse (Events) im WBM beschrieben.

7.4.1 Traces

Ein Trace protokolliert eine Ausführung einer Softwarekomponente. Ein Fachmann kann mit Hilfe der Ablaufaufzeichnung die Ursache eines Fehlers finden.

Wichtig: Das Aktivieren von Traces kann die Performance des Systems negativ beeinflussen. 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

Trace-Profile

Alle Trace-Profile stoppen

Trace-Komponenten

Gestartete Trace-Komponenten anzeigen

Alle Trace-Komponenten stoppen

Secure Trace

M5T Trace-Komponenten

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.

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 SIP-bezogenen Protokolle, die auf dem Gateway gespeichert sind, löschen. Beispiel: Trace- und Event-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:

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.

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.

Wichtig: Alle anderen Trace-Interfaces sind automatisch deaktiviert, wenn die Trace-Ausgabe über ServiceCenter/CSDA erfolgt.

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

7.4.1.4 Laden des Trace-Protokolls

Wenn Datei-Trace aktiviert ist (siehe Section 7.4.1.3, "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 STMIX - SIP 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.

Wichtig: 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.

7.4.1.5 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*.

7.4.1.6 Trace-Profile

Trace-Profile legen fest, welche Daten in welcher Detailtiefe geloggt werden sollen. Einem Trace-Profil werden Trace-Komponenten (siehe Section 7.4.2, "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 8.1.2, "Trace-Profile".

Anmerkung: Aktivierte Trace-Profile werden während des Loadware- oder OS-Updates automatisch deaktiviert.

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.

Permanentes Trace-Profil

Mit permanenten Trace-Profilen können Sie Probleme anhand der auf dem Gateway gespeicherten Daten automatisch diagnostizieren und so die für die Analyse benötigte Zeit optimieren. Aufgrund der permanenten Aktivierung können Sie auch sporadische Probleme zu ermitteln.

Permanentes Tracing wird mit dem neuen Trace-Profil Permanentes Tracing ausgeführt. Standardmäßig ist das Profil bereits aktiviert.

7.4.1.7 Alle Trace-Profile stoppen

Sie können alle gestarteten Trace-Profile (siehe Section 7.4.1.8, "Trace-Komponenten") auf einmal stoppen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Traces und Ereignisse (Events)* **>** Traces **>** *Alle Trace-Profile stoppen*

Die Baumdarstellung *Traces* wird aktualisiert.

7.4.1.8 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 8.1.1, "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.

Wichtig: 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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.4.1.9 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 7.4.1.8, "Trace-Komponenten".

7.4.1.10 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.

7.4.1.11 Secure Trace

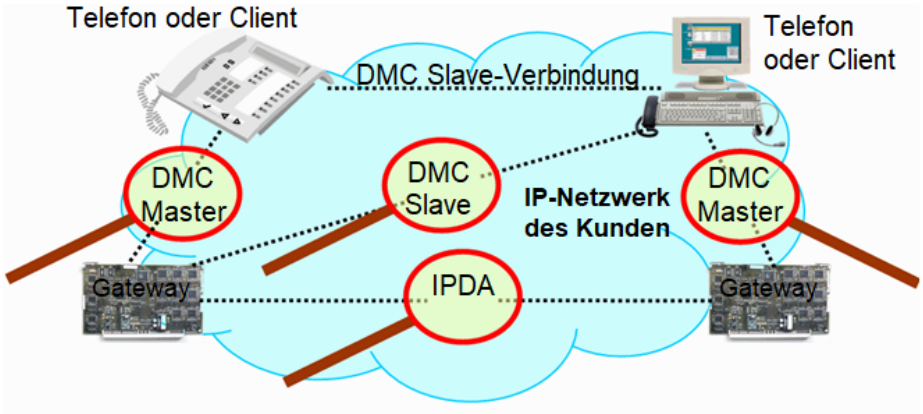
WBM-Pfad:

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.

Wichtig: 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.

Wichtig: 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 7.4.1.12, "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.

7.4.1.12 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: SIP Core/SSA (TLS), MSC (SRTP).

7.4.1.13 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 einschalten.* 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.

7.4.1.14 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*.

7.4.1.15 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 *Ã–ffnen*. 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.

7.4.1.16 M5T Trace-Komponenten

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T Trace-Komponenten **>** *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 **>** *<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 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 *<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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.4.1.17 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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.4.1.18 Service Center

Das Service Center ist ein zusätzliches Diagnosetool für Entwickler.

Anmerkung: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad:

WBM **>** Wartung **>** Traces und Ereignisse (Events) **>** Traces **>** M5T Trace-Komponenten *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 SIP-Teil des STMIX. Der Administrator sollte die Konfiguration des Netzwerks oder des Gateways überprüfen, um die irreguläre Situation zu korrigieren.

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*

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.

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

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 7.4.2.2, "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.

  Wichtig: Halten Sie die Konventionen gemäß RFC 821 und RFC 822 ein. Die SMTP-Server-Einstellungen sind erforderlich, weil das STMIX - SIP 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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.4.2.3 Reaktionstabelle

Sie können für *Ereignisse (Events)* getrennt einstellen, wie bei einem Eintreten reagiert werden soll.

Anmerkung: 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.

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 7.4.2.2, "E-Mail").
- *Zugeordnetes Trace-Profil*: Sie können diesem Event eines der vorhandenen Trace-Profile zuordnen (siehe Section 7.4.2, "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 7.4.2.3, "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.
- *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 7.4.2.2, "E-Mail").
- *Zugeordnetes Trace-Profil*: Sie können diesem Event eines der vorhandenen Trace-Profile zuordnen (siehe Section 7.4.2, "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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

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 STMIX 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 STMIX 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*. Klicken Sie auf Rückgängig, um die Änderungen zu verwerfen.

7.4.3.2 Admin.-Protokoll-Daten laden

Sie können das Admin.-Protokoll vom STMIX herunterladen.

WBM-Pfad:

WBM **>** *Wartung* **>** *Admin.-Protokoll* **>** Traces und Ereignisse (Events) **>** *Laden Admin.-Protokoll-Daten*

Laden über HTTP

Sie können die Administrations-Protokolldatei vom STMIX - SIP zu dem Rechner übertragen, über den Sie das Gateway administrieren.

Nachdem die Datei übertragen wurde, wird sie direkt im System-Editor angezeigt.

7.5 Appl. Diagnose

WBM-Pfad:

WBM > *Wartung* > Appl. Diagnose

Die Funktionen in diesem Bereich dürfen nur von Entwicklern benutzt werden.

8 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 Abschnitt 7.4, "Traces und Ereignisse (Events)", speziell Abschnitt 7.4.2, "Ereignisse (Events)" und Abschnitt 7.4.2, "Ereignisse (Events)").
- *Ereignisse (Events)*, beschrieben nach einzelnen Event-Codes. Events sind über das WBM administrierbar (siehe Abschnitt 7.4.2, "Ereignisse (Events)").

8.1 Traces

Anmerkung: Wenn Traces vom Service angefordert werden, dann werden auch die zu tracenden Komponenten und Profile mitgeteilt.

8.1.1 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
BOARDDATAMGMT
CARDADM
CFG_CODECS
CFG_H235

Übersicht der Trace-Komponenten
CFG_H323
CFG_H323ENDPOINT
CFG_H323GKI
CFG_H323GWI
CFG_H323I
CG
CIRCUITDATAMGMT
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

Übersicht der Trace-Komponenten
FAXCONV_T30UP
FAXCONVERTER
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

Übersicht der Trace-Komponenten
IPSTACK_NAT
IPSTACK_ROUTE
IPSTACK_SNTPS
ISDN_FM
JCIF
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

Übersicht der Trace-Komponenten
NWRS
OAM
OAM_ACTIONLIST
OSF_PCS
PERFM_PL
PERFM_SIG
PERS
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

Übersicht der Trace-Komponenten
SERVICE_TRACE
SESSION_MGMT
SI
SIP
SIP_CFG
SIP_CFG_INT
SIP_FM
SIP_GLOBAL_SI_DOWNLOADS
SIP_HT
SIP_PM
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)

Übersicht der Trace-Komponenten
TCP_IP_CONF (nur HG 3575)
TCPMOT_WT (nur HG 3575)
TCPSIG (nur HG 3575)
TCPSIG_WT (nur HG 3575)
TCPSUV (nur HG 3575)
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 zu Verbindungsaufbau und Verbindungsabbau.

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)???Evtl. kommt noch Erläuterung???

ASP_DSP_EVENT

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

Trace-Level **3** (INTER): Informationen zu erkannten Tonwahl- oder Fax-Geräten oder Modems

ASP_DSP_IFTASK

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

ASP_DSP_INIT

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

ASP_PS

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

ASP_VMOD

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

ASP_VMUX

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

BOARDDATAMGMT

konfiguriertes Default-Trace-Level: **0** (STATUS)

CARDADM

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_CODECS

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H235

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H323

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H323ENDPOINT

konfiguriertes Default-Trace-Level: 0 (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H323GKI

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H323GWI

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CFG_H323I

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

CG

konfiguriertes Default-Trace-Level: n/a

CIRCUITDATAMGMT

konfiguriertes Default-Trace-Level: **0** (STATUS)

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 sehr stark. 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)???Evtl. kommt noch Erläuterung. ???

DMC

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

DSP

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Nicht verwendet

Trace-Level 3-**9** : 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)???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

GATEWAY

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

GWGLOBAL_DATA

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

Trace-Level **6** (INTRA) ???Evtl. kommt noch Erläuterung. ???

Trace-Level 9 (DETAIL)???Evtl. kommt noch Erläuterung. ???

H323IWK

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

H323MSG

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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): Interne Debugger-Information.

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-Verwendung des H.323-Stack.

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): No standard data 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) ???Evtl. kommt noch Erläuterung. ???

Trace-Level 6 (INTRA)???Evtl. kommt noch Erläuterung. ???

Trace-Level 9 (DETAIL)???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

IFTABLE

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Zeigt Fehler an.

Trace-Level **6** (INTRA): Zeigt Funktionsaufrufe mit wichtigen Parametern an.

Trace-Level **9** (DETAIL): nicht verwendet.

IP_ROUTES

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

IPMONITOR

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

IPSTACK

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Fehlersituation bei IP-Accounting-Hash-Funktionen. Nur für Entwickler.

IPSTACK_1LAN_IF

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Handling von Konfigurationsdaten.

IPSTACK_2LAN_IF

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Handling von Konfigurationsdaten.

IPSTACK_GLOBAL

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

IPSTACK_IPFILTER

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

IPSTACK_MACFILTER

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

IPSTACK_NAT

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Initialisierung.

Trace-Level **6** (INTRA): Detaillierte Informationen über NAT-Abläufe.

Trace-Level **9** (DETAIL): Übersetzte Daten.

IPSTACK_ROUTE

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Fehlersituation bei Routing-Daten.

IPSTACK_SNTPS

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

ISDN_FM

konfiguriertes Default-Trace-Level: **3**

Trace-Level **3:** ISDN FM Trace (Voreinstellung)

JCIF

konfiguriertes Default-Trace-Level: **0** (STATUS)

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): Funktions-Beendungen und -Ergebnisse.

Trace-Level **9** (DETAIL): Weitere Details.

LOCSERV

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

LOCSERV_CFG

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

LOCSERV_QUERY

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

LOCSERV_REG

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

LOG_MSG

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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** : Interne Meldungen vom Materna-Speicher-Management.

MCP

konfiguriertes Default-Trace-Level: **0**

Trace-Level **0** (STATUS): Hoch- und Runterfahren, 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): Detail-Socket-Informationen.

MIKEY

konfiguriertes Default-Trace-Level: **3** (INTER)

MMX (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

MPH

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

MSC

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): API zu Magic (Funktionsaufrufe mit Parametern).

Trace-Level **3** (INTER): zusätzlich festgehalten 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 festgehalten. Detaillierte Informationen zu allen MSC-Funktionen.

MSC_DSP

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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 über 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)???Evtl. kommt noch Erläuterung. ???

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 â“ 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)???Evtl. kommt noch Erläuterung. ???

NWRS

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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-Threshold-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)???Evtl. kommt noch Erläuterung. ???

PERFM_SIG

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Performance-Trace für den Signalisierungsteil.

PERS

konfiguriertes Default-Trace-Level: **0** (STATUS)

PLATFORM

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

PORT

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

PORT_MGR

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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 internal program flow.

Trace-Level **3** (INTER): Status eines PPP-Verbindungsaufbaus/-abbaus

PPPM_TBAS

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6**-**9**: PPP negotiation phase.

Trace-Level **0** (STATUS): PPP-Manager: basic configuration and status messages, abnormal conditions.

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** : Interne Fehlermeldungen vom PPTP für Debugging.

PPTP_PROC

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **9** (DETAIL): Detailierte Informationen über MSC specific quality data

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, Traces werden bei Eingabe einer Funktion oder Klassenmethode angezeigt.

Trace-Level **9**: Detaillierte Informationen zu internen Daten und Schnittstellen-daten

- 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) ???Evtl. kommt noch Erläuterung. ???

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)???Evtl. kommt noch Erläuterung. ???

SDR

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SECURE_TRACE

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SECURITY_SVC

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0**: Fatale Fehler, z. B. fehlende Parameter, unbekannte Kommandos.

Trace-Level **3**: Status-Informationen und -Handling.

Trace-Level **6**: Detail-Informationen, Methoden-Aufrufe.

SENDTMT

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): Fehler beim Senden oder Posten einer Meldung (Extra-Info for TMT).

Trace-Level **3** (INTER): Empfangen einer Meldung (Extra-Info for TMT).

SENTA_API

konfiguriertes Default-Trace-Level: **0**

Trace-Level **3** (INTER): Ein Fehler ist aufgetreten.

Trace-Level **6** (INTRA): Funktionen und Ergebnisse existieren.

Trace-Level **9** (DETAIL): Details.

SERVICE_TRACE

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SESSION_MGMT

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3** (INTER): Informationen zu: 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)???Evtl. kommt noch Erläuterung. ???

SIP

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP Protokoll-Manager: Status-Information-Trace Trace-Level **3** (INTER): Meldungen zu anderen 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): Trace von internen Konfigurationsdaten

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 zu H.323 Konverter: SIP Anrufsignalisierung Trace-Level **3** (INTER): Trace-Level **6** (INTRA): Trace-Level **9** (DETAIL):

SIP_PM

konfiguriertes Default-Trace-Level: **0** (STATUS)

SIP_REG

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **0** (STATUS): SIP Stack-Adapter: REGISTER und OPTIONS 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)???Evtl. kommt noch Erläuterung. ???

SIU_STARTUP

konfiguriertes Default-Trace-Level: n/a

SLMO_HFA

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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 internen SNMP-Informationen und -Problemen. Bitte diese Trace-Komponente nur nach Absprache mit der Entwicklung verwenden!

SPE_SVC

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SPL

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SS

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SSL_UTIL

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

SSM

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

STACKTRACE

konfiguriertes Default-Trace-Level: **0** (STATUS)

STATIC_ROUTES

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

STB (nur HG 3575)

konfiguriertes Default-Trace-Level: **3** (INTER)

Trace Level **0** (STATUS): Startup und Shutdown; Erhaltene Fehler von anderen Komponenten

Trace Level **3** (INTER): Erhaltene und gesendete Nachrichten, etc

Trace Level **6** (INTRA): Funktions-spezifische Informationen

Trace Level **9** DETAIL: Funktions-spezifische Informationen mit Daten.

STRC

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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 Kommandos 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): Interne Debugger-Information.

TCP_IP_CONF (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TCPMOT_WT (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TCPSIG (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TCPSIG_WT (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TCPSUV (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TCPSUV_WT (nur HG 3575)

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

TESTLW

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

Trace-Level **0**-9: Detaillierte Information über TESTLW Aktionen â“ 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 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: - 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): Interne Debugger-Information.

WAN

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

WEBAPPL

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **3/6** (INTER/INTRA): Eingang/Ausgang wichtiger Web-Anwendungs-Funktionen und -Methoden (für Entwickler).

WEBSERVER

konfiguriertes Default-Trace-Level: **0** (STATUS)

Trace-Level **6** (INTRA): Eingang/Ausgang wichtiger Web-Server-Funktionen und -Methoden (für Entwickler).

WEBSERVER_STATISTIC

konfiguriertes Default-Trace-Level: **0** (STATUS)???Evtl. kommt noch Erläuterung. ???

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**: wie 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): Administrations-Schnittstellen-Trace. Daten, die zur Administrations-Schnittstelle gesendet werden, und XML-Daten, die von der Administrations-Schnittstelle erhalten werden.

Trace-Level **6** (INTRA): User- und Passwort-Informationen.

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)???Evtl. kommt noch Erläuterung. ???

8.1.2 Trace-Profile

8.1.2.1 Profile bei Normal-/Hochlast

Anmerkung: 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'
'1.2.3(normal) SIP Sub. Fax problems'
'1.3(normal) SPE Additional for SIP Sub./Trk.'
'2.1.1(normal) H.323 Trk. General problems'

Übersicht der Profile bei Normal-/Hochlast
'2.1.2(normal) H.323 Trk. Payload problems'
'2.1.3(normal) H.323 Trk. Fax problems'
'2.2.1(normal) HFA Registration'
'2.2.2(normal) HFA General problems'
'2.2.3(normal) HFA Payload problems'
'2.3(normal) SPE Additional for HFA/H323 Trk.'
'3.1(normal) IPDA General problems'
'3.2(normal) IPDA Payload problems'
'3.3(normal) IPDA Fax problems'
'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 Additional for 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 Registration'

- 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 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:
- – H323, Level 9
  – HSA_SYSTEM, Level 1
  – TSA, Level 9

'2.2.3(normal) HFA 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
  – MSC, Level 9
  – SENTA_API, Level 9

'2.3(normal) SPE Additional for 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 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:
- – MPH, Level 3
  – MSC, Level 0

'3.2(normal) IPDA 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
  – MCP, Level 9

– MPH, Level 9
– MSC, Level 0

'3.3(normal) IPDA 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
  – 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

8.1.2.2 Profile bei Schwachlast

Anmerkung: 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. for Sub. and 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 Additional for SIP Sub./Trk.'
'2.1.1(detail) H.323 Trk. General problems'
'2.1.2(detail) H.323 Trk. Payload problems'

Übersicht der Profile bei Schwachlast
'2.1.3(detail) H.323 Trk. Fax problems'
'2.2.1(detail) HFA Registration'
'2.2.2(detail) HFA General problems'
'2.2.3(detail) HFA Payload problems'
'2.3(detail) SPE Additional for HFA/H323 Trk.'
'3.1(detail) IPDA General problems'
'3.2(detail) IPDA Payload problems'
'3.3(detail) IPDA Fax problems'
'4.1(detail) WAML (signaling survivability)'
'4.2(detail) Signaling survivability problemsâ

'1.1.1(detail) SIP Reg. for Sub. and 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 Additional for 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 Registration'

- 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 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:
- – H323, Level 9
  – HSA_SYSTEM, Level 1
  – TSA, Level 9

'2.2.3(detail) HFA 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
  – MSC, Level 9
  – SENTA_API, Level 9

'2.3(detail) SPE Additional for 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 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:
- – ICC, Level 9
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 9

'3.2(detail) IPDA 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
  – MCP, Level 9
  – MPH, Level 9
  – MSC, Level 9

'3.3(detail) IPDA 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
  – 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 problemsâ

- Kategorie: Darf nur bei Schwachlast aktiviert werden!

'4.4(detail) NCUI reboots after TCP timeoutâ

- Kategorie: Darf nur bei Schwachlast aktiviert werden!

8.2 Ereignisse (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

8.2.1 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 5. Zeichen.

Event-Code	Abschnitt
ASSERTION_FAILED_EVENT	8.2.3, 'Reboot-Events'
CCE_GENERAL_ERROR	8.2.49, 'LAN-Signalisierung bezogene Events â“ CCE'
CCE_PSS_STORE_ERROR	8.2.49, 'LAN-Signalisierung bezogene Events â“ CCE'
COMGA_NOK_UPGRADE_REG	8.2.2, 'Status-Events'
EXIT_REBOOT_EVENT	8.2.3, 'Reboot-Events'
FP_EVT_CRITICAL	8.2.3, 'Reboot-Events'
FP_EVT_INDETERMINATE	8.2.2, 'Status-Events'
FP_EVT_MAJOR	8.2.3, 'Reboot-Events'
FP_EVT_MINOR	8.2.2, 'Status-Events'
FP_EVT_SNMP_TRAP	8.2.2, 'Status-Events'
FP_EVT_INFORMATION	8.2.2, 'Status-Events'
FP_EVT_TRACE_START	8.2.2, 'Status-Events'
FP_EVT_TRACE_STOP	8.2.2, 'Status-Events'
FP_EVT_WARNING	8.2.3, 'Reboot-Events'
FW_NOK_UPGRADE_REG	8.2.2, 'Status-Events'
H323_NO_IP	8.2.8, 'H.323-Events'
H323_SNMP_TRAP	8.2.8, 'H.323-Events'
MSG_ADMIN_DIDNT_GET_WRITE_ACCESS	8.2.29, 'OAM-Events'
MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS	8.2.29, 'OAM-Events'
MSG_ADMIN_GOT_WRITE_ACCESS	8.2.29, 'OAM-Events'
MSG_ADMIN_INVALID_LOGIN	8.2.29, 'OAM-Events'
MSG_ADMIN_LOGGED_IN	8.2.29, 'OAM-Events'
MSG_ADMIN_LOGGED_OUT	8.2.29, 'OAM-Events'
MSG_ADMIN_REBOOT	8.2.3, 'Reboot-Events'
MSG_ADMIN_RELEASED_WRITE_ACCESS	8.2.29, 'OAM-Events'
MSG_ADMIN_SESSION_CREATED	8.2.29, 'OAM-Events'
MSG_ADMIN_SESSION_EXPIRED	8.2.29, 'OAM-Events'
MSG_ASC_ERROR	8.2.35, 'Bedeutendere ASC-Events'

Event-Code	Abschnitt
MSG_ASP_ERROR	8.2.36, 'Bedeutendere ASP-Events'
MSG_ASP_INFO	8.2.34, 'Wichtige Plattform-Software-Status-Events'
MSG_ASP_INFO	8.2.37, 'Kleinere ASP-Events'
MSG_ASP_REBOOT	8.2.3, 'Reboot-Events'
MSG_BSD44_ACCEPT_DGW_ERR	8.2.12, 'DGW-Events'
MSG_BSD44_ACCEPT_ERROR	8.2.23, 'VCAPI-Events'
MSG_BSD44_DGW_BIND_FAIL	8.2.12, 'DGW-Events'
MSG_BSD44_DGW_CONNECT_FAIL	8.2.12, 'DGW-Events'
MSG_BSD44_DGW_NO_LIST	8.2.12, 'DGW-Events'
MSG_BSD44_DGW_SOCKET_FAIL	8.2.12, 'DGW-Events'
MSG_BSD44_SELECT_ERROR	8.2.23, 'VCAPI-Events'
MSG_BSD44_VCAPI_NO_LIST	8.2.12, 'DGW-Events'
MSG_CAR_ALIVE_IP_CONNECTION_LOST	8.2.13, 'CAR-Events'
MSG_CAR_ALIVE_IP_CONNECTION_LOST	8.2.13, 'CAR-Events'
MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN	8.2.13, 'CAR-Events'
MSG_CAR_CALL_ADDR_REJECTED	8.2.29, 'OAM-Events'
MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB	8.2.13, 'CAR-Events'
MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS	8.2.13, 'CAR-Events'
MSG_CAR_CODEC_ENTRY_DELETED	8.2.13, 'CAR-Events'
MSG_CAR_CODECS_INCONSISTENT	8.2.13, 'CAR-Events'
MSG_CAR_DB_READ_NODE_TABLE_ERROR	8.2.13, 'CAR-Events'
MSG_CAR_DBF_SERVER_INCONSISTENT	8.2.13, 'CAR-Events'
MSG_CAR_DBFS_POSS_CONFLICT	8.2.13, 'CAR-Events'
MSG_CAR_ERROR_WITH_OAM_INTERFACE	8.2.13, 'CAR-Events'
MSG_CAR_FKT_GET_IPADR_FAILED	8.2.13, 'CAR-Events'
MSG_CAR_GENERAL_ERROR	8.2.13, 'CAR-Events'
MSG_CAR_MALLOC_FAILED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_CAR_NO_FREE_CODEC_TAB_ELE	8.2.13, 'CAR-Events'

Event-Code	Abschnitt
MSG_CAR_NO_MAC_ADDRESS	8.2.13, 'CAR-Events'
MSG_CAR_NO_MEMORY	8.2.13, 'CAR-Events'
MSG_CAR_NODE_INFO_ALREADY_AVAILABLE	8.2.13, 'CAR-Events'
MSG_CAR_PARAM_NOT_FOUND	8.2.13, 'CAR-Events'
MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_NO_MEMORY	8.2.13, 'CAR-Events'
MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_SOH_ERROR	8.2.13, 'CAR-Events'
MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS	8.2.13, 'CAR-Events'
MSG_CAR_START_TCP_LISTENER_FAILED	8.2.13, 'CAR-Events'
MSG_CAR_UNAUTHORIZED_IP_ACCESS	8.2.13, 'CAR-Events'
MSG_CAR_UNEXPECTED_DATA_RECV	8.2.13, 'CAR-Events'
MSG_CAR_UNEXPECTED_MSG_RECV	8.2.13, 'CAR-Events'
MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CAL-LADDRTAB_TOO_BIG	8.2.13, 'CAR-Events'
MSG_CAR_WRONG_EVENT	8.2.13, 'CAR-Events'
MSG_CAR_WRONG_IP_ADDRESS	8.2.13, 'CAR-Events'
MSG_CAR_WRONG_LENGTH	8.2.13, 'CAR-Events'
MSG_CAR_WRONG_NODE_ID	8.2.13, 'CAR-Events'
MSG_CAR_WRONG_SERVICE	8.2.13, 'CAR-Events'
MSG_CAT_H235	8.2.9, 'H.235-Events'
MSG_CAT_H323_REBOOT	8.2.3, 'Reboot-Events'
MSG_CAT_HSA_REBOOT	8.2.2, 'Status-Events'
MSG_CAT_NWRS	8.2.5, 'Routing-Events'
MSG_CLI_LOGGED_IN_FROM_TELNET	8.2.30, 'CLI-Events'
MSG_CLI_LOGGED_IN_FROM_V24	8.2.30, 'CLI-Events'
MSG_CLI_TELNET_ABORTED	8.2.30, 'CLI-Events'
MSG_DELIC_ERROR	8.2.41, 'DELIC-Events'
MSG_DEVM_BINDING_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	8.2.33, 'MAGIC / Device-Manager-Events'

Event-Code	Abschnitt
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CLOSE_LEG_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_LEGS_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_WRONG_LEGS	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CONNECT_WRONG_RES_STATE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_CREATE_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_DEVICEID_OUT_OF_RANGE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_DISCONNECT_LEGS_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_CHNID	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_DEVID	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_INTERROR_RESID	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_LAYER2_SERVICE_TRAP	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_LISTEN_WRONG_RES_STATE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_MSCERROR_RESID	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_OPEN_LEG_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_OPEN_WRONG_RES_STATE	8.2.33, 'MAGIC / Device-Manager-Events'

Event-Code	Abschnitt
MSG_DEVMGR_SCN_TASK_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DEVMGR_UPDATE_LEG_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_DGW_ABORT_SOCK_UNKN	8.2.12, 'DGW-Events'
MSG_DGW_ACCEPT_FAILED	8.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CHN_CONN_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CHN_RUN_OUT	8.2.12, 'DGW-Events'
MSG_DGW_ALLOC_CONF_ERR	8.2.12, 'DGW-Events'
MSG_DGW_ALLOC_DISC_B3	8.2.12, 'DGW-Events'
MSG_DGW_ALLOC_REQ_ERR	8.2.12, 'DGW-Events'
MSG_DGW_BUFAVAIL_SOCK_UNKN	8.2.12, 'DGW-Events'
MSG_DGW_CONF_ALLOC_ERR	8.2.12, 'DGW-Events'
MSG_DGW_CONN_B3_ACT_IND	8.2.12, 'DGW-Events'
MSG_DGW_CONN_COMPL_ALLOC	8.2.12, 'DGW-Events'
MSG_DGW_CONN_OUT_OF_RANGE	8.2.12, 'DGW-Events'
MSG_DGW_CONN_RUN_OUT	8.2.12, 'DGW-Events'
MSG_DGW_CONNECT_FAILED	8.2.12, 'DGW-Events'
MSG_DGW_DATA_B3_ALLOC_ERR	8.2.12, 'DGW-Events'
MSG_DGW_DISC_B3_IND	8.2.12, 'DGW-Events'
MSG_DGW_DISC_B3_NOT_SEND	8.2.12, 'DGW-Events'
MSG_DGW_FREE_ALLOC_ERR	8.2.12, 'DGW-Events'
MSG_DGW_FREE_CHN_ALLOC_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_FREE_NOT_SEND	8.2.12, 'DGW-Events'
MSG_DGW_FREE_UNKNOWN_ID	8.2.12, 'DGW-Events'
MSG_DGW_IND_ALLOC_ERR	8.2.12, 'DGW-Events'
MSG_DGW_INV_DATA_LEN	8.2.12, 'DGW-Events'
MSG_DGW_INV_MSG_LEN	8.2.12, 'DGW-Events'
MSG_DGW_INVALID_LENGTH	8.2.12, 'DGW-Events'
MSG_DGW_LISTENING_ERR	8.2.12, 'DGW-Events'
MSG_DGW_MGR_NOT_READY	8.2.12, 'DGW-Events'

Event-Code	Abschnitt
MSG_DGW_MSG_IGNORED	8.2.12, 'DGW-Events'
MSG_DGW_MSG_RCV_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_NO_PLCI	8.2.12, 'DGW-Events'
MSG_DGW_OPEN_CHN_ALLOC_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_OPEN_CHN_UNKNOWN_ID	8.2.12, 'DGW-Events'
MSG_DGW_OPEN_CHN_WRONG	8.2.12, 'DGW-Events'
MSG_DGW_RCV_ALLOC_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_RCV_FAILED	8.2.12, 'DGW-Events'
MSG_DGW_RCV_SOCK_UNKN	8.2.12, 'DGW-Events'
MSG_DGW_RECEIVE_ERR	8.2.12, 'DGW-Events'
MSG_DGW_SEC_ALLOC_FAIL	8.2.12, 'DGW-Events'
MSG_DGW_SEND_DATA_ERR	8.2.12, 'DGW-Events'
MSG_DGW_SEND_FAILED	8.2.12, 'DGW-Events'
MSG_DGW_SOCKET_BIND_ERR	8.2.12, 'DGW-Events'
MSG_DGW_SOCKET_NOT_OPEN	8.2.12, 'DGW-Events'
MSG_DGW_SOCKET_UNKNOWN	8.2.12, 'DGW-Events'
MSG_DGW_UNH_MSG_CAPI20_MGR	8.2.12, 'DGW-Events'
MSG_DGW_UNHANDLED_EVENT	8.2.12, 'DGW-Events'
MSG_DGW_UNHANDLED_MSG	8.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_ID_CHANNEL	8.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_NOTIFIC	8.2.12, 'DGW-Events'
MSG_DGW_UNKNOWN_PRIMITIVE	8.2.12, 'DGW-Events'
MSG_DGW_WRONG_EVENT_CAPI	8.2.12, 'DGW-Events'
MSG_DGW_WRONG_EVENT_CAPI20	8.2.12, 'DGW-Events'
MSG_DGW_WRONG_STATE	8.2.12, 'DGW-Events'
MSG_DLSC_BOOTSTRAP_OK	8.2.2, 'Status-Events'
MSG_DISP_SENDER_NOT_SET	8.2.29, 'OAM-Events'
MSG_ERH_ADMISSION_ERROR	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_ERROR	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'

Event-Code	Abschnitt
MSG_ERH_INFORMATION	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_NO_LICENSE	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_REGISTRATION_ERROR	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_SECURITY_DENIAL	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_ERH_SUB_OUT_OF_SERVICE	8.2.45, 'Endpunkt-Registrierungs-Handler-Events'
MSG_EXCEPTION_REBOOT	8.2.3, 'Reboot-Events'
MSG_FAXCONV_ERROR	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_FIREWALL_ALARM	8.2.2, 'Status-Events'
MSG_FAXCONV_INFO	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_GSA_SNMP	8.2.11, 'GSA-Events'
MSG_GW_OBJ_ALLOC_FAILED	8.2.3, 'Reboot-Events'
MSG_GW_OBJ_MEMORY_EXHAUSTED	8.2.3, 'Reboot-Events'
MSG_GW_OBJ_MEMORY_INCONSISTENT	8.2.3, 'Reboot-Events'
MSG_GW_SUCCESSFULLY_STARTED	8.2.2, 'Status-Events'
MSG_H323_INFORMATION	8.2.8, 'H.323-Events'
MSG_H323_INVALID_CONFIGURATION	8.2.8, 'H.323-Events'
MSG_H323_INVALID_PARAMETER_VALUE	8.2.8, 'H.323-Events'
MSG_H323_INVALID_POINTER	8.2.8, 'H.323-Events'
MSG_H323_LOGIC_ERROR	8.2.8, 'H.323-Events'
MSG_H323_MISSING_PARAMETER	8.2.8, 'H.323-Events'
MSG_H323_OSCAR_NSD_ERROR	8.2.8, 'H.323-Events'
MSG_H323_PROTOCOL_ERROR	8.2.8, 'H.323-Events'
MSG_H323_SNMP_TRAP	8.2.8, 'H.323-Events'
MSG_H323_STACK_ERROR	8.2.8, 'H.323-Events'
MSG_H323_UNEXPECTED_MESSAGE	8.2.8, 'H.323-Events'
MSG_H323_UNEXPECTED_RETURN_VALUE	8.2.8, 'H.323-Events'
MSG_H323CLIENT_INVALID_ADMIN_MSG	8.2.25, 'H.323-Client-Events'

Event-Code	Abschnitt
MSG_H323CLIENT_INVALID_CLIENTID	8.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_INVALID_PARAM	8.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_MAPS_DIFFER	8.2.25, 'H.323-Client-Events'
MSG_H323CLIENT_NWRS_ENTRY_FAILED	8.2.25, 'H.323-Client-Events'
MSG_HBR_WARNING	8.2.2, 'Status-Events'
MSG_HACKER_ON_SNMP_PORT_TRAP	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_HFAA_INTERNAL_ERROR	8.2.18, 'HFA-Adapter-Events'
MSG_HFAA_INTERNAL_EVENT	8.2.18, 'HFA-Adapter-Events'
MSG_HFAA_MEMORY_ERROR	8.2.18, 'HFA-Adapter-Events'
MSG_HFAA_MESSAGE_ERROR	8.2.18, 'HFA-Adapter-Events'
MSG_HFAA_PARAM_ERROR	8.2.18, 'HFA-Adapter-Events'
MSG_HFAM_HAH_ALLOC_CHAN_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_HAH_ALLOC_CONF_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_ALGORITM_OBJID_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_BIND_REGISOCK_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_CREATE_REGISOCK_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_IPADR_TOO_LONG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_LISTEN_REGISOCK_ERR	8.2.17, 'HFA-Manager-Events'

Event-Code	Abschnitt
MSG_HFAM_LIH_MAX_CON_EXCEED_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_PROTOCOL_LIST_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_RETURNED_SOCKET_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_LIH_UNEXP_CORNET_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_ILLEG_PORTNO_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_NO_LOGONTIMER_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_MON_NO_MON_TIMER_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_ESTAB_NOTREG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_INVAL_PWD_LEN_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_LOGIN_NOTREG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_LOGON_REJECT_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_MISSING_L2INFO_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_RELIN_NOTREG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR	8.2.17, 'HFA-Manager-Events'

Event-Code	Abschnitt
MSG_HFAM_REG_SUBNO_TOO_LONG_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_CORNET_LONGER_28_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR	8.2.17, 'HFA-Manager-Events'
MSG_HIP_ALLOC_DEV_OBJ	8.2.31, 'HIP-Events'
MSG_HIP_ALLOC_MES_SI	8.2.31, 'HIP-Events'
MSG_HIP_NO_CLBLK	8.2.31, 'HIP-Events'
MSG_HIP_NO_CLPOOL_ID	8.2.31, 'HIP-Events'
MSG_HIP_NO_CLUSTER	8.2.31, 'HIP-Events'
MSG_HIP_NO_DEVLOAD	8.2.31, 'HIP-Events'
MSG_HIP_NO_DEVSTART	8.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_CL	8.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_CLBLK	8.2.31, 'HIP-Events'
MSG_HIP_NO_MEM_TO_SI	8.2.31, 'HIP-Events'
MSG_HIP_NO_NETPOOL_INIT	8.2.31, 'HIP-Events'
MSG_HIP_NO_OBJ_INIT	8.2.31, 'HIP-Events'
MSG_HIP_NO_PMBLK	8.2.31, 'HIP-Events'
MSG_HIP_PKTLEN_ZERO	8.2.31, 'HIP-Events'
MSG_HIP_PMBLK_ZERO	8.2.31, 'HIP-Events'
MSG_IP_LINK_FAILURE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK2_FAILURE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK_RESTORE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK2_RESTORE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK_SWITCHOVER	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IP_LINK2_SWITCHOVER	8.2.4, 'Ressourcen-Überwachungs-Events'

Event-Code	Abschnitt
MSG_IP_RTP_QUALITY_FAILURE	8.2.10, 'RTPQM-Events'
MSG_IP_RTP_QUALITY_WARNING	8.2.10, 'RTPQM-Events'
MSG_IPACCSRV_INTERNAL_ERROR	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_LOGON	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MARK_REACHED	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MEMORY_ERROR	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_MESSAGE_ERROR	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_OVERFLOW	8.2.44, 'IP-Accounting-Events'
MSG_IPACCSRV_SOCKET_ERROR	8.2.44, 'IP-Accounting-Events'
MSG_IPF_ON_OFF	8.2.38, 'IP-Filter-Events'
MSG_IPF_PARAMETER	8.2.38, 'IP-Filter-Events'
MSG_IPF_STARTED	8.2.38, 'IP-Filter-Events'
MSG_IPF_STOPPED	8.2.38, 'IP-Filter-Events'
MSG_IPNC_CP_ASYNCH	8.2.26, 'IPNC-Events'
MSG_IPNC_INCONSISTENT_STATE	8.2.26, 'IPNC-Events'
MSG_IPNC_INTERNAL_ERROR	8.2.26, 'IPNC-Events'
MSG_IPNC_MESSAGE_DUMP	8.2.26, 'IPNC-Events'
MSG_IPNC_MESSAGE_ERROR	8.2.26, 'IPNC-Events'
MSG_IPNC_PARAM_ERROR	8.2.26, 'IPNC-Events'
MSG_IPNCA_ERROR	8.2.27, 'IPNCA-Events'
MSG_IPNCV_INTERNAL_ERROR	8.2.2, 'Status-Events'
MSG_IPNCV_MEMORY_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_IPNCV_SIGNALING_ERROR	8.2.46, 'IPNCV-Events'
MSG_IPNCV_STARTUP_ERROR	8.2.2, 'Status-Events'
MSG_IPNCV_STARTUP_SHUTDOWN	8.2.2, 'Status-Events'
MSG_IPSEC_REBOOT	8.2.3, 'Reboot-Events'

Event-Code	Abschnitt
MSG_IPSTACK_INVALID_PARAM	8.2.40, 'IP-Stack-Events'
MSG_IPSTACK_NAT_ERROR	8.2.40, 'IP-Stack-Events'
MSG_IPSTACK_SOH_ERROR	8.2.40, 'IP-Stack-Events'
MSG_ISDN_CMR_ADD_OBJECT_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_DEVICE_PTR_BAD	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_GEN_CALL_REF_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_GENRIC_EVENT	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_INIT_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MAND_FIELDS_MISSING	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MESSAGE_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_DECODE_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_ENCODE_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_SEND_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_MSG_UNEXPECTED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_NEW_OBJECT_FAILED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_OBJECT_NOT_FOUND	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_PROTOCOL_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_SEG_MSG_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_SESSION_NOT_FOUND	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_STATUS_MSG_RECEIVED	8.2.7, 'SCN-Protokoll-Events'

Event-Code	Abschnitt
MSG_ISDN_CMR_TIMER_EXPIRED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_EVENT	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNEXPECTED_VALUE	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNH_STATE_EVENT	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_UNIMPLEMENTED	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_DEVICE_TYPE	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_INTERFACE	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_CMR_WRONG_PROTVAR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_DEVICE_PTR_NOT_FOUND	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_NO_ERROR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_NULL_PTR	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_OVERLOAD_CONDITION	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_IN_USE_BY_O_CALL	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_NOT_AVAILABLE	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_RESOURCE_NOT_IN_SERVICE	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_START_UP	8.2.7, 'SCN-Protokoll-Events'
MSG_ISDN_START_UP_ERROR	8.2.7, 'SCN-Protokoll-Events'

Event-Code	Abschnitt
MSG_LDAP_ENCODE_DECODE_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_GENERAL_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_IP_LINK_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_MEMORY_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_SOCKET_ERROR	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_LDAP_SUCCESSFULLY_STARTED	8.2.2, 'Status-Events'
MSG_LLC_EVENT_INVALID_PARAMETER_VALUE	8.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_MISSING_PARAMETER	8.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_MISSING_RESOURCE	8.2.50, 'Events für LLC-Operation'
MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE	8.2.50, 'Events für LLC-Operation'
MSG_MAF_ETHERNET_HEADER	8.2.39, 'MAC-Filter-Events'
MSG_MAF_NETBUFFER	8.2.39, 'MAC-Filter-Events'
MSG_MAF_NO_OF_RULES	8.2.39, 'MAC-Filter-Events'
MSG_MAF_ON_OFF	8.2.39, 'MAC-Filter-Events'
MSG_MAF_PARAMETER	8.2.39, 'MAC-Filter-Events'
MSG_MAF_STARTED	8.2.39, 'MAC-Filter-Events'
MSG_MAF_STOPPED	8.2.39, 'MAC-Filter-Events'
MSG_MAND_PARAM_MISSING	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_MIKEY_REBOOT	8.2.3, 'Reboot-Events'
MSG_MPH_INFO	8.2.28, 'MPH-Events'
MSG_MSP_FAX_OVERLONG_PKT	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_MSP_HDLC_ERROR	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_MSP_HDLC_INFO	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'

Event-Code	Abschnitt
MSG_NU_CAR_FAILED	8.2.15, 'NU-Events'
MSG_NU_CAR_RESP_INVALID	8.2.15, 'NU-Events'
MSG_NU_DEV_TAB_NOT_FOUND	8.2.15, 'NU-Events'
MSG_NU_EVENT_EXCEPTION	8.2.15, 'NU-Events'
MSG_NU_FREE_CHN_COMF_TOO_LATE	8.2.15, 'NU-Events'
MSG_NU_FREE_CHN_UNEXPECTED	8.2.15, 'NU-Events'
MSG_NU_GENERAL_ERROR	8.2.15, 'NU-Events'
MSG_NU_INTERNAL_ERROR	8.2.15, 'NU-Events'
MSG_NU_INVALID_CIDL	8.2.15, 'NU-Events'
MSG_NU_IP_ERROR	8.2.15, 'NU-Events'
MSG_NU_NO_FREE_TRANSACTION	8.2.15, 'NU-Events'
MSG_NU_NO_PORT_DATA	8.2.15, 'NU-Events'
MSG_NU_SOH_RESP_INVALID	8.2.15, 'NU-Events'
MSG_NU_SUPERFLUOS_MSG	8.2.15, 'NU-Events'
MSG_NU_TCP_LISTENER_FAILED	8.2.15, 'NU-Events'
MSG_NU_TOO_MUCH_DIGITS	8.2.15, 'NU-Events'
MSG_NU_TRANSPCONT_MISSING	8.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_MSG	8.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_SETUP	8.2.15, 'NU-Events'
MSG_NU_UNEXPECTED_TIMER	8.2.15, 'NU-Events'
MSG_NU_UNKNOWN_MESSAGE	8.2.15, 'NU-Events'
MSG_NU_WRONG_CALL_REF	8.2.15, 'NU-Events'
MSG_NULC_INTERNAL_ERROR	8.2.16, 'NU-Leg-Kontroll-Events'
MSG_NULC_INTERNAL_EVENT	8.2.16, 'NU-Leg-Kontroll-Events'
MSG_NULC_MEMORY_ERROR	8.2.16, 'NU-Leg-Kontroll-Events'
MSG_NULC_MESSAGE_ERROR	8.2.16, 'NU-Leg-Kontroll-Events'
MSG_NULC_PARAM_ERROR	8.2.16, 'NU-Leg-Kontroll-Events'
MSG_NWRS_DEVICE_NOT_FOUND	8.2.5, 'Routing-Events'

Event-Code	Abschnitt
MSG_NWRS_DEVICE_TABLE_NOT_FOUND	8.2.5, 'Routing-Events'
MSG_NWRS_DPLN_ENTRY_INVALID	8.2.5, 'Routing-Events'
MSG_NWRS_DPLN_NOT_FOUND	8.2.5, 'Routing-Events'
MSG_NWRS_EMPTY_FIELD_ECHOED	8.2.5, 'Routing-Events'
MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE	8.2.5, 'Routing-Events'
MSG_NWRS_ODR_COMMAND_UNKNOWN	8.2.5, 'Routing-Events'
MSG_NWRS_ODR_NOT_FOUND	8.2.5, 'Routing-Events'
MSG_NWRS_ROUTE_NOT_FOUND	8.2.5, 'Routing-Events'
MSG_NWRS_UNKNOWN_FIELD_ECHOED	8.2.5, 'Routing-Events'
MSG_NWRS_UNSPEC_ERROR	8.2.5, 'Routing-Events'
MSG_OAM_DMA_RAM_THRESHOLD_REACHED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_OVERLOAD_REACHED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_OVERLOAD_CLEARED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_FAN_OUT_OF_SERVICE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_INTERNAL_EVENT	8.2.29, 'OAM-Events'
MSG_OAM_PRIO_INCREASED	8.2.29, 'OAM-Events'
MSG_OAM_PRIO_SWITCHED_BACK	8.2.29, 'OAM-Events'
MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_PUT_TO_QUEUE_FAILED	8.2.29, 'OAM-Events'
MSG_OAM_QUEUE_BLOCKED	8.2.29, 'OAM-Events'
MSG_OAM_QUEUE_FULL	8.2.29, 'OAM-Events'
MSG_OAM_RAM_THRESHOLD_REACHED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_THRESHOLD_REACHED	8.2.4, 'Ressourcen-Überwachungs-Events'
MSG_OAM_TIMESYNC	8.2.29, 'OAM-Events'
MSG_OAM_TIMESYNC_FAILED	8.2.29, 'OAM-Events'

Event-Code	Abschnitt
MSG_OS_EXCEPTION_ERROR	8.2.3, 'Reboot-Events'
MSG_ERH_NO_LICENSE	8.2.48, 'Fehler-Events'
MSG_OSF_PCS_EXCEPTION	8.2.3, 'Reboot-Events'
MSG_PPP_STACK_PROC	8.2.21, 'PPP-Stack-Events'
MSG_PPP_STACK_REBOOT	8.2.3, 'Reboot-Events'
MSG_PS_INVALID_STREAM_FROM_ADDRESS	8.2.2, 'Status-Events'
MSG_PS_INVALID_STREAM_FROM_PORT	8.2.2, 'Status-Events'
MSG_PPTP_STACK_REBOOT	8.2.3, 'Reboot-Events'
MSG_PPPM_ERR_CONFIG	8.2.20, 'PPP-Manager-Events'
MSG_PPPM_ERR_OPERATION	8.2.20, 'PPP-Manager-Events'
MSG_REG_ERROR_FROM_SOH	8.2.14, 'REG-Events'
MSG_REG_GLOBAL_ERROR	8.2.14, 'REG-Events'
MSG_REG_NIL_PTR_FROM_SOH	8.2.14, 'REG-Events'
MSG_REG_NO_MEMORY	8.2.14, 'REG-Events'
MSG_REG_NO_REGISTRATION_POSSIBLE	8.2.14, 'REG-Events'
MSG_REG_REQUEST_WITHIN_REGISTRATION	8.2.14, 'REG-Events'
MSG_REG_SOH_SEND_DATA_FAILED	8.2.14, 'REG-Events'
MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH	8.2.14, 'REG-Events'
MSG_RESTORE_CFG_REBOOT	8.2.3, 'Reboot-Events'
MSG_SCN_ADD_PARAMETER_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_BIND_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_DEV_NOT_IN_DEVLIST	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_ERROR_12_MSG	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_GET_ADMMSG_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_GET_LDAPMSG_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'

Event-Code	Abschnitt
MSG_SCN_OPEN_STREAM_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_OPERATION_ON_STREAM_FAILED	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_POLL_FD	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_UNEXPECTED_L2_MSG	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SCN_UNEXPECTED_POLL_EVENT	8.2.33, 'MAGIC / Device-Manager-Events'
MSG_SDR_INIT	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SDR_UNEXPECTED_EVENT	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SI_L2STUB_COUDNT_OPEN_STREAM	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_ERROR_INIT_DRIVER	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_NO_ALLOC	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_NO_CLONE	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_OPEN_OTHER_STREAM_NOT_POSSIBLE	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_PORT_NOT_OPEN	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_STREAM_ALREADY_OPEN	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_UNEXPECTED_DB_TYPE	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SI_L2STUB_UNKNOWN_SOURCE_PID	8.2.32, 'SI-Events (Systemschnittstellen-Events)'
MSG_SIP_FM_INTERNAL_ERROR	8.2.2, 'Status-Events'
MSG_SIP_FM_MSG_INTERNAL_ERROR	8.2.2, 'Status-Events'
MSG_SIP_FM_MSG_NOT_PROCESSED	8.2.2, 'Status-Events'
MSG_SIP_FM_STARTUP_FAILURE	8.2.2, 'Status-Events'
MSG_SNCP_ADD_OBJECT_FAILED	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'

Event-Code	Abschnitt
MSG_SNCP_CHANNEL_ID_MISSING	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_CREATE_OBJECT	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_DELETE_OBJECT	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_SET_FORW_ENC	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_COULD_NOT_SET_REV_ENC	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_DEVICE_ID_MISSING	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_ERROR	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_NEITHER_ENC_COULD_BE_SET	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_NO_RESOURCE_ID	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNCP_UNANTICIPATED_MESSAGE	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SNMP_TRAP_COLLECTOR_START_ERROR	8.2.3, 'Reboot-Events'
MSG_SPE_CERT_MISSING	8.2.22, 'SPE-Events'
MSG_SPE_CERT_AVAIL	8.2.22, 'SPE-Events'
MSG_SPE_CERT_UPDATED	8.2.22, 'SPE-Events'
MSG_SPE_CERT_EXPIRED	8.2.22, 'SPE-Events'
MSG_SPE_CERT_TIMEREMAINING	8.2.22, 'SPE-Events'
MSG_SPE_CRL_EXPIRED	8.2.22, 'SPE-Events'
MSG_SPE_CRL_UPDATED	8.2.22, 'SPE-Events'
MSG_SPE_ALL_CRLS_UPTODATE	8.2.22, 'SPE-Events'
MSG_SPL_ADD_OBJECT_FAILED	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_ERROR	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_FMSEM_ERROR	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_MISSING_CS_ID	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'

Event-Code	Abschnitt
MSG_SPL_SESSION_NOT_FOUND	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SPL_UNANTICIPATED_MESSAGE	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_BAD_NWRS_RESULT	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_INVALID_PARAM	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_NO_CSID	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	8.2.3, 'Reboot-Events'
MSG_SSM_SESSION_CREATION_FAILED	8.2.3, 'Reboot-Events'
MSG_SSM_UNSPEC_ERROR	8.2.6, 'Anrufkontroll- und Leistungsmerkmal-Events'
MSG_SYSTEM_REBOOT	8.2.3, 'Reboot-Events'
MSG_STRC_STOP	8.2.2, 'Status-Events'
MSG_STRC_START	8.2.2, 'Status-Events'
MSG_T90_ERROR	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_T90_INFO	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_TESTLW_ERROR	8.2.42, 'Test-Loadware-Events'
MSG_TESTLW_INFO	8.2.42, 'Test-Loadware-Events'
MSG_TLS_MUTEX_BLOCKED	8.2.29, 'OAM-Events'
MSG_TLS_POOL_SIZE_EXCEEDED	8.2.3, 'Reboot-Events'
MSG_VCAPI_ACCEPT_ERROR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_ADD_OBJECT_FAILED	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_BUF_NOT_CREATED	8.2.23, 'VCAPI-Events'
MSG_VCAPI_CONF_ALLOC_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_CONF_WITHOUT_REQ	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_CONV_H2N_ERROR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_CONV_H2N_FAILED	8.2.23, 'VCAPI-Events'

Event-Code	Abschnitt
MSG_VCAPI_CONV_N2H_FAILED	8.2.23, 'VCAPI-Events'
MSG_VCAPI_COULD_NOT_CREATE_OBJECT	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_DELETE_OBJECT	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_CSID	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_OBJECT	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_FIND_PLCI	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_COULD_NOT_STORE_REQ	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_CSID_MISSING	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_DATA_B3_ALLOC_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_DATA_NOT_STORED	8.2.23, 'VCAPI-Events'
MSG_VCAPI_DISP_NOT_READY	8.2.23, 'VCAPI-Events'
MSG_VCAPI_ILLEGAL_LINK_NUMBER	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_ILLEGAL_PARTNER_NUMBER	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_IND_ALLOC_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_LINK_TABLE_FULL	8.2.23, 'VCAPI-Events'
MSG_VCAPI_LISTENING_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_MSG_NOT_SEND	8.2.23, 'VCAPI-Events'
MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_NO_ALLOC_EXTENDED	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_ALLOC_MSG	8.2.23, 'VCAPI-Events'

Event-Code	Abschnitt
MSG_VCAPI_NO_ALLOC_SINGLE	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_CAPI_DATA	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_CLIENT	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_LIST_SOCKET	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_LNK_CONN	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_NEW_BUF	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI_AVAILABLE	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_NO_PLCI_DATA_B3	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_PLCI_DISCONNECT	8.2.23, 'VCAPI-Events'
MSG_VCAPI_NO_RCV_BUFFER	8.2.23, 'VCAPI-Events'
MSG_VCAPI_PLCI_NOT_FOUND	8.2.23, 'VCAPI-Events'
MSG_VCAPI_RCV_LEN_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_RECEIVE_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_SERVER_ERROR	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_SOCK_NOT_AVAIL	8.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_BIND_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_NOT_OPEN	8.2.23, 'VCAPI-Events'
MSG_VCAPI_SOCKET_RCV_ERR	8.2.23, 'VCAPI-Events'
MSG_VCAPI_TOO_MANY_CLIENTS	8.2.23, 'VCAPI-Events'
MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNANTICIPATED_MESSAGE	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE	8.2.24, 'VCAPI-Anwendungs-Events'
MSG_VCAPI_UNKNOWN_MSG_N2H	8.2.23, 'VCAPI-Events'
MSG_VCAPI_UNKNOWN_NTFY	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_BUF_LEN	8.2.23, 'VCAPI-Events'

Event-Code	Abschnitt
MSG_VCAPI_WRONG_CONV_H2N	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_CONV_N2H	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_EVENT_CAPI	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_EVENT_SRV	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_LENGTH_MSG	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_LINKNUM	8.2.23, 'VCAPI-Events'
MSG_VCAPI_WRONG_MSG_LENGTH	8.2.23, 'VCAPI-Events'
MSG_WEBSERVER_INTERNAL_ERROR	8.2.29, 'OAM-Events'
MSG_WEBSERVER_MAJOR_ERROR	8.2.3, 'Reboot-Events'
MSG_X25_ERROR	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X25_INFO	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X75_ERROR	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_X75_INFO	8.2.43, 'Fax-Konverter-, HDLC- und X.25-Events'
MSG_XMLUTILS_ERROR	8.2.47, 'XMLUTILS-Events'
QDC_ERROR_IN_CLIENT	8.2.52, 'QDC CGWA releated Events'
QDC_ ERROR_IN_COMMON_CLIENT	8.2.51, 'Client releated Events'
QDC_INVALID_CONFIGURATION	8.2.52, 'QDC CGWA releated Events'
QDC_MSG_QUEUE_ERROR	8.2.51, 'Client releated Events'
QDC_PERSYSTENCY_ERROR	8.2.52, 'QDC CGWA releated Events'
QDC_SIGNALLING_DATA_ERROR	8.2.51, 'Client releated Events'
QDC_SYSTEM_ERROR	8.2.51, 'Client releated Events'
QDC_VOIPSD_ERROR	8.2.53, 'QDC VoIPSD Fehlerberichts-Events'
SENTA_NOK_UPGRADE_REG	8.2.2, 'Status-Events'

Event-Code	Abschnitt
SIP_INFORMATION	8.2.54, 'SIP bezogene Events'
SIP_INVALID_PARAMETER_VALUE	8.2.54, 'SIP bezogene Events'
SIP_INVALID_POINTER	8.2.54, 'SIP bezogene Events'
SIP_REBOOT	8.2.3, 'Reboot-Events'
SIP_UNEXPECTED_RETURN_VALUE	8.2.54, 'SIP bezogene Events'

8.2.2 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.???Informationen notwendig. ???

MSG_FIREWALL_ALARM

Alarm an der Firewall.???Informationen notwendig. ???

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: **Major**

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: IPNCV Internal 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 â“ 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 â“ SNMP-Trap wird erzeugt.

FP_EVT_MINOR

`EventText: %x %c #%d/%d %x-%x %s`

Typ: **Minor**

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.???noch Informationen nötig.???

MSG_PS_INVALID_STREAM_FROM_PORT

Ungültige Daten von einem bestimmten Port.???noch Informationen nötig.???

MSG_SIP_FM_MSG_INTERNAL_ERROR

`EventText: %p`

Typ: **Major**

Softwarefehler innerhalb von SIP_FM_MSG

MSG_SIP_FM_STARTUP_FAILURE

`EventText: SIP_FM startup failed: %s`

Typ: **Major**

Softwarefehler während SIP_FM-Start

MSG_SIP_FM_INTERNAL_ERROR

`EventText: %p`

Typ: **Major**

Softwarefehler innerhalb von SIP_FM

MSG_SIP_FM_MSG_NOT_PROCESSED

`EventText: SIP_FM received an illegal message: %d`

Typ: **Major**

SIP_FM konnte keine Erhalten-Meldung absetzen.

MSG_STRC_STOP

STRC gestoppt.???mehr Informationen nötig! ???

MSG_STRC_START

STRC gestartet.???mehr Informationen nötig! ???

MSG_HBR_WARNING

Warnung von Backup- und Restore.???mehr Informationen nötig! ???

SENTA_NOK_UPGRADE_REG

Laden der SENTA-Firmware via HTTP

8.2.3 Reboot-Events

MSG_CAT_H323_REBOOT

Der H.323-Stack-Adapter hat keine internen Ressourcen mehr und bewirkt einen Neustart. Der Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.??? mehr Informationen nötig! ???

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 ausgeführt. 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 ausgeführt.???mehr Informationen nötig! ???

MSG_WEBSERVER_MAJOR_ERROR

```
EventText: %p
```

Typ: **Major**

Interner Fehler beim Webserver. Da weitere Aktivitäten des Webservers beeinflusst würden, wird ein Neustart erzwungen. Der Neustart wird ausgeführt.

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 partion 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 partion 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 ...`

Das Reservieren 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: maximal number of elements exceeded`

Typ: **Major**

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: **Major**

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: **Major**

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 ausgeführt. Ein SNMP-Trap wird erzeugt.???mehr Informationen nötig! ???

MSG_DELIC_ERROR

Ein DELIC-Fehler ist aufgetreten. Der Neustart wird ausgeführt. Ein SNMP-Trap wird erzeugt.???mehr Informationen nötig! ???

MSG_IPSEC_REBOOT

Der Neustart wird ausgeführt.???mehr Informationen nötig! ???

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: **major**

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 ausgeführt.

MSG_MIKEY_REBOOT

Der Neustart wird ausgeführt.???mehr Informationen nötig! ???

8.2.4 Ressourcen-Überwachungs-Events

MSG_IP_LINK_FAILURE

`EventText: IP Link [still] out of order`

Typ bei diesem Log-Eintrag: **Warning**

Eine IP-Netzwerkverbindung ist nicht oder immer noch nicht möglich. Ein SMNP-Trap wird erzeugt. Überprüfen Sie die Steckerverbindungen und Kabel!

`EventText: IP Link no longer out of order`

Typ bei diesem Log-Eintrag: **Cleared**

Die IP-Netzwerkverbindung ist wieder verfügbar. Ein SMNP-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 bei diesem 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 SMNP-Trap wird erzeugt.

```
EventText: High WaterMark 'XXX' no longer reached:
           Configured: xxx Current: xxx
```

Typ bei diesem Log-Eintrag: **Cleared**

Das Problem mit der Systemspeichergrenze besteht nicht mehr. Ein niedrigeres Anrufaufkommen kann die Ursache für die geringere Speicherauslastung sein. Ein SMNP-Trap wird erzeugt.

MSG_OAM_DMA_RAM_THRESHOLD_REACHED

```
EventText: High WaterMark 'XXX' [still] reached:
           Configured: xxx Current: xxx
```

Typ bei diesem 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 SMNP-Trap wird erzeugt.

```
EventText: High WaterMark 'XXX' no longer reached:
           Configured: xxx Current: xxx
```

Typ bei diesem Log-Eintrag: **Cleared**

Das Problem mit der DMA-Speichergrenze besteht nicht mehr. Ein niedrigeres Anrufaufkommen kann die Ursache für die geringere Speicherauslastung sein. Ein SMNP-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 bei diesem 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 SMNP-Trap wird erzeugt.

```
EventText: High/Low WaterMark 'XXX' no longer reached:
           Configured: xxx Current: xxx
```

Typ bei diesem Log-Eintrag: **Cleared**

Das Problem mit dem Grenzwert besteht nicht mehr. Ein SMNP-Trap wird erzeugt.

MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE

```
EventText: PSU or RPS [still] out of Service
```

Typ bei diesem Log-Eintrag: **Warning**

Bei PSU oder RPS gibt es (immer noch) ein Problem. Ein SMNP-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 bei diesem Log-Eintrag: **Cleared**

Das Problem mit PSU oder RPS besteht nicht mehr. Ein SMNP-Trap wird erzeugt.

MSG_OAM_FAN_OUT_OF_SERVICE

```
EventText: Fan [still] out of Service
```

Typ bei diesem Log-Eintrag: **Warning**

Beim Lüfter gibt es (immer noch) ein Problem. Ein SMNP-Trap wird erzeugt. Überprüfen Sie den Lüfter und tauschen Sie ihn gegebenenfalls aus!

```
EventText: Fan no longer out of Service
```

Typ bei diesem Log-Eintrag: **Cleared**

Das Problem mit dem Lüfter besteht nicht mehr. Ein SMNP-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: **Major**

Die Reservierung von Speicher schlug fehl.

MSG_IPNCV_MEMORY_ERROR

`EventText: IPNCV Memory: %s`

Typ: **Major**

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: **Major**

Nicht genügend Speicher zum Senden/Empfangen einer Meldung.

MSG_LDAP_ENCODE_DECODE_ERROR

`EventText: Unable to Encode/Decode LDAP Msg`

Typ: **Major**

Die BER-Kodierung oder -Dekodierung einer LDAP-ASN.1-Meldung schlug fehl.

MSG_LDAP_SOCKET_ERROR

`EventText: LDAP Socket Failure`

Typ: **Major**

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.

8.2.5 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: **Minor**

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: **Major**

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: **Minor**

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: **Minor**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

Ein Rufnummernplan mit der angegebenen ID konnte nicht gefunden werden.

MSG_NWRS_UNSPEC_ERROR

`EventText:` %p

Typ: **Major**

Inkonsistenter Software-Zustand, z. B. durch ungültige Daten.

8.2.6 Anrufkontroll- und Leistungsmerkmal-Events

MSG_SDR_INIT

`EventText:` SDR init %p

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

SCN-Payload-Objekt konnte nicht erzeugt 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: **Major**

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: **Major**

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: **Major**

Es war keine Kodierung möglich.

MSG_SNCP_ADD_OBJECT_FAILED

`EventText:` SCN Payload: Could not add SCN Payload Object - EXCEP: %n %e

Typ: **Major**

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: **Major**

Es konnte kein Session-Objekt gefunden werden.

MSG_SPL_ADD_OBJECT_FAILED

`EventText:` Session Payload: Object could not be added - EXCEP: %n%e

Typ: **Major**

Es konnte kein Objekt hinzugefügt werden.

MSG_SPL_MISSING_CS_ID

`EventText:` Session Payload: Missing Call and Session ID - EXCEP: %n%e

Typ: **Major**

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: **Major**

Anruf- und Session-ID fehlen.

MSG_SSM_INVALID_PARAM

`EventText:` Invalid parameter %s, value %x

Typ: **Major**

Ein Parameter enthielt einen ungültigen Wert.

MSG_SSM_UNSPEC_ERROR

`EventText: %p`

Typ: **Major**

Inkonsistenter Software-Zustand, z. B. durch ungültige Daten.

MSG_SSM_BAD_NWRS_RESULT

`EventText:` Bad result from NWRS

Typ: **Major**

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: **Major**

Eine CCP-Meldung konnte nicht aus der Meldungs-Basis erstellt werden, weil ein Pflichtparameter fehlte.

8.2.7 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 Versenden der Meldung schlug fehl.

MSG_ISDN_CMR_SEG_MSG_ERROR

`EventText: %pSegmented message error`

Typ: **Minor**

Fehler bei segmentierter Nachricht.

MSG_ISDN_CMR_UNEXPECTED_ERROR

`EventText: %pUnexpected error`

Typ: **Minor**

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: **Minor**

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: **Minor**

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.

8.2.8 H.323-Events

H323_NO_IP

n. zutr.??? Informationen Nötig.???

H323_SNMP_TRAP

n. zutr.??? Informationen Nötig.???

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).

8.2.9 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.

8.2.10 RTPQM-Events

MSG_IP_RTP_QUALITY_FAILURE

`EventText: ...`

Typ bei diesem Log-Eintrag: **Major**

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 bei diesem 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: **Major**

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!

8.2.11 GSA-Events

MSG_GSA_SNMP

`EventText: %p`

Typ: **Critical**

Kritischer Fehler für GSA, der einen SNMP-Trap generiert.

8.2.12 DGW-Events

MSG_BSD44_VCAPI_NO_LIST

`EventText: No listening socket for VCAPI`

Typ: **Major**

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: **Major**

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: **Major**

Es ist nicht möglich, eine neue Verbindung für DATAGW herzustellen.

MSG_BSD44_DGW_SOCKET_FAIL

`EventText: DGW socket() failed`

Typ: **Minor**

Ein Client kann keinen Socket empfangen.

MSG_BSD44_DGW_BIND_FAIL

`EventText: DGW bind() failed`

Typ: **Minor**

Ein Client kann keinen Socket binden.

MSG_BSD44_DGW_CONNECT_FAIL

`EventText: DGW connect() failed`

Typ: **Minor**

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: **Minor**

Die Verbindungs-ID hat die maximal erlaubte Anzahl von Kanälen überschritten.

MSG_DGW_WRONG_STATE

`EventText: dg_capi_HandleCapi20Msg: id=%d wrong state!`

Typ: **Minor**

Falscher Status für den DATAGW-Dispatcher.

MSG_DGW_MSG_IGNORED

`EventText: %s from CAPI_PAYLOAD_IF ignored!`

Typ: **Minor**

Meldung ignoriert, da sich der DGW-Dispatcher im falschen Status befindet.

MSG_DGW_CONN_B3_ACT_IND

`EventText: ALLOC error: no more buffers`

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

Unbekannte Meldung von CAPI_PAYLOAD_IF an DGW-Dispatcher.

MSG_DGW_DATA_B3_ALLOC_ERR

`EventText: DATAB3_REQ:ALLOC ERROR: returncode %x`

Typ: **Major**

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: **Minor**

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: **Minor**

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: **Major**

Es konnte kein Speicher reserviert werden, um die Meldung DISCONNEC-T_B3_REQ zu senden. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_UNKNOWN_PRIMITIVE

`EventText: unknown capi primitive: %x`

Typ: **Major**

Unbekannte Meldung von CAPI_PAYLOAD_IF an DGW-Dispatcher.

MSG_DGW_RECEIVE_ERR

`EventText: Error while receiving message for DATAGW-Dispatcher:Returncode %x`

Typ: **Major**

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: **Major**

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: **Major**

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: **Minor**

Zu viele Verbindungen.

MSG_DGW_ALLOC_CHN_CONN_FAIL

`EventText: ALLOC_CHANNEL_REQ:connect failed`

Typ: **Major**

Es konnte keine neue Verbindung zum Server hergestellt werden.

MSG_DGW_OPEN_CHN_UNKNOWN_ID

`EventText: AOPEN_CHANNEL_REQ: unknown id`

Typ: **Minor**

Über die Channel-ID konnte die Verbindungs-ID nicht gefunden werden.

MSG_DGW_OPEN_CHN_WRONG

`EventText: OPEN_CHANNEL_REQ:dreadful!: wrong state`

Typ: **Minor**

Falscher Zustand für die Meldung OPEN_CHANNEL_REQ.

MSG_DGW_OPEN_CHN_ALLOC_FAIL

`EventText: OPEN_CHANNEL_REQ:Alloc failed`

Typ: **Major**

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: **Major**

FREE_CHANNEL_REQ mit falscher ID.

MSG_DGW_FREE_CHN_ALLOC_FAIL

`EventText: FREE_CHANNEL_REQ : Alloc failed`

Typ: **Major**

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: **Major**

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: **Minor**

Über die Channel-ID kann die Verbindungs-ID nicht gefunden werden.

MSG_DGW_FREE_NOT_SEND

`EventText: Alloc error: DGW_FREE_REQUEST not sent`

Typ: **Major**

Es konnte kein Speicher reserviert werden. DGW_FREE_REQUEST wurde nicht gesendet. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_DISC_B3_NOT_SEND

`EventText: Alloc error: DISCONNECT_B3_REQUEST not sent`

Typ: **Major**

Es konnte kein Speicher reserviert werden. DISCONNECT_B3_REQUEST wurde nicht gesendet. Das Gateway führt einen automatischen Neustart durch.

MSG_DGW_SOCKET_UNKNOWN

`EventText: SO_NTFY_CONN_COMPLETE: unknown socket!`

Typ: **Minor**

SO_NTFY_CONN_COMPLETE: unbekannter Socket. Die Verbindung wird beendet.

MSG_DGW_CONNECT_FAILED

`EventText: SO_NTFY_CONN_COMPLETE: error! ret= %d!`

Typ: **Major**

SO_NTFY_CONN_COMPLETE: Verbindungsfehler.

MSG_DGW_CONN_COMPL_ALLOC

`EventText: SO_NTFY_CONN_COMPLETE: Alloc failed`

Typ: **Major**

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: **Minor**

Senden nicht möglich wegen unbekanntem Socket.

MSG_DGW_RCV_SOCK_UNKN

`EventText: SO_NTFY_RCV_SDATA: unknown socket`

Typ: **Minor**

Daten können nicht empfangen werden wegen unbekanntem Socket.

MSG_DGW_ABORT_SOCK_UNKN

`EventText: SO_NTFY_ABORT: unknown socket`

Typ: **Minor**

Verbindung kann nicht geschlossen werden wegen unbekanntem Socket.

MSG_DGW_UNKNOWN_NOTIFIC

`EventText: Unknown notification 0x%x`

Typ: **Minor**

Unbekannte Benachrichtigung.

MSG_DGW_RCV_FAILED

`EventText: recv() failed, id=%d`

Typ: **Minor**

Daten werden nicht ordnungsgemäß empfangen.

MSG_DGW_INV_MSG_LEN

`EventText: invalid message lenght: %d`

Typ: **Minor**

Meldung mit falscher Länge von entfernter Stelle empfangen.

MSG_DGW_RCV_ALLOC_FAIL

`EventText: FATAL: allocb() failed, id=%d`

Typ: **Major**

Es ist nicht möglich, Speicher für den Empfangspuffer zu reservieren.

MSG_DGW_MSG_RCV_FAIL

`EventText: recv() failed, id=%d`

Typ: **Minor**

Es ist nicht möglich, eine Meldung zu empfangen.

MSG_DGW_INVALID_LENGTH

`EventText: invalid lenght:%d %s`

Typ: **Minor**

Falsche Länge von entfernter Stelle empfangen.

MSG_DGW_INV_DATA_LEN

`EventText: invalid data lenght:%d`

Typ: **Minor**

Falsche Datenlänge von entfernter Stelle empfangen.

MSG_DGW_SEND_FAILED

`EventText: send() failed, id=%d`

Typ: **Minor**

Es ist nicht möglich, eine Meldung an die entfernte Stelle zu senden.

MSG_DGW_SEND_DATA_ERR

`EventText: send() data failed, id=%d`

Typ: **Minor**

Es ist nicht möglich, Daten an die entfernte Stelle zu senden.

MSG_DGW_SOCKET_NOT_OPEN

`EventText: DGW-Socket not opened`

Typ: **Major**

DGW-Socket wurde nicht geöffnet. Es sind keine Verbindungen möglich.

MSG_DGW_SOCKET_BIND_ERR

`EventText: bind error for DGW socket %d`

Typ: **Major**

Bindungs-Fehler bei DGW-Socket. Es sind keine Verbindungen möglich.

MSG_DGW_LISTENING_ERR

`EventText: listening error for DGW socket %d`

Typ: **Major**

Listening-Fehler bei DGW-Socket. Es sind keine Verbindungen möglich.

MSG_DGW_ACCEPT_FAILED

`EventText: so_accept() failed`

Typ: **Minor**

Es werden keine neuen Verbindungen akzeptiert.

8.2.13 CAR-Events

MSG_CAR_GENERAL_ERROR

`EventText: CAR : General error : %s`

Typ: **Minor**

Im Subsystem CAR trat ein allgemeiner Fehler auf.

MSG_CAR_NO_MEMORY

`EventText: CAR : no more memory available`

Typ: **Minor**

`EventText:` CAR: es ist kein Speicher verfügbar.

MSG_CAR_FKT_GET_IPADR_FAILED

`EventText: CAR : car_fkt_get_ipadr result unsuccessful due to lack of memory (mat_allocb)`

Typ: **Minor**

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_data` 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: **Minor**

CAR: SOH: Das Staten des des Update-Requests schlug fehl wegen Speichermangel.

MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CALLADDRTAB_TOO_BIG

`EventText: CAR : SOH : update data : number of CallAddressEntries = %d too big`

Typ: **Minor**

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: **Major**

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: **Major**

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: **Major**

`EventText:` CAR: Alive: IP-Verbindung verloren.

MSG_CAR_ALIVE_IP_CONNECTION_LOST

`EventText: CAR : Alive : ip connection %d.%d.%d.%d lost`

Typ: **Major**

CAR: Alive: IP-Verbindung verloren.

MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN

`EventText: CAR: Alive : ip connection %d.%d.%d.%d ok again`

Typ: **Information**

CAR: Alive: IP-Verbindung steht wieder.

MSG_CAR_ERROR_WITH_OAM_INTERFACE

`EventText: CAR : An error occurred with the OAM interface RC = %d`

Typ: **Minor**

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: **Minor**

Kein freies Tabellenelement für CODECs gefunden.

MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB

`EventText: Cannot arrange node table %d`

Typ: **Major**

Knotentabelle kann nicht angeordnet werden.

MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS

`EventText: Cannot sort MAC addresses %s`

Typ: **Minor**

MAC-Adressen können nicht sortiert werden.

MSG_CAR_CODECS_INCONSISTENT

`EventText: HSA CODEC tables inconsistent %s`

Typ: **Major**

Die HSA-CODEC-Tabellen sind inkonsistent.

MSG_CAR_WRONG_NODE_ID

`EventText: Wrong node id %d`

Typ: **Major**

Falsche Knotenidentifikation.

MSG_CAR_WRONG_SERVICE

`EventText: Wrong service %d`

Typ: **Minor**

Falscher Service.

MSG_CAR_NODE_INFO_ALREADY_AVAILABLE

`EventText: Node info already available for %d`

Typ: **Minor**

Die Knoteninformationen für den angegebenen Knoten sind bereits verfügbar.

MSG_CAR_DBF_SERVER_INCONSISTENT

`EventText: DB feature server inconsistent %s`

Typ: **Major**

Der DB-Feature-Server befindet sich in einem inkonsistenten Zustand.

MSG_CAR_UNEXPECTED_MSG_RECV

`EventText: Unexpected message received %s`

Typ: **Minor**

Eine unerwartete Meldung wurde empfangen.

MSG_CAR_UNEXPECTED_DATA_RECV

`EventText: Unexpected data received %s`

Typ: **Minor**

Es wurden unerwartete Daten empfangen.

MSG_CAR_PARAM_NOT_FOUND

`EventText: Parameter not found %s`

Typ: **Major**

Ein Parameter wurde nicht gefunden.

MSG_CAR_WRONG_EVENT

`EventText: Wrong event received %x`

Typ: **Major**

Ein falsches Ereignis wurde empfangen.

MSG_CAR_WRONG_LENGTH

`EventText: Wrong length %d`

Typ: **Minor**

Falsche Länge.

MSG_CAR_WRONG_IP_ADDRESS

`EventText: Wrong IP address %d.%d.%d.%d`

Typ: **Major**

Falsche IP-Adresse.

MSG_CAR_UNAUTHORIZED_IP_ACCESS

`EventText: Unauthorised access from %d.%d.%d.%d`

Typ: **Minor**

Nicht authorisierter Zugriff von der angegebenen IP-Adresse aus.

MSG_CAR_NO_MAC_ADDRESS

`EventText: No MAC address found`

Typ: **Major**

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: **Major**

HSA CODEC Zugang gelöscht.

8.2.14 REG-Events

MSG_REG_GLOBAL_ERROR

`EventText: REG : Global error : %s`

Typ: **Minor**

REG: Allgemeiner Fehler.

MSG_REG_NO_MEMORY

`EventText: REG : No more memory available`

Typ: **Minor**

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: es konnten keine Daten gesendet werden: die Routine `soh_api_send_tcp_data` gab einen ungültigen Wert zurück.

MSG_REG_REQUEST_WITHIN_REGISTRATION

`EventText: REG : REG request within registration`

Typ: **Minor**

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: **Minor**

REG: SOH: Unbekanntes Ereignis von SOH.

MSG_REG_NO_REGISTRATION_POSSIBLE

`EventText: REG : No registration possible (no response)`

Typ: **Major**

REG: Keine Registrierung möglich (keine Antwort).

8.2.15 NU-Events

MSG_NU_GENERAL_ERROR

`EventText: General error %s`

Typ: **Warnung**

Nur als ein temporärer Dummy.

MSG_NU_TRANSPCONT_MISSING

`EventText: Transport container missing`

Typ: **Major**

Der Transport-Container fehlt.

MSG_NU_NO_FREE_TRANSACTION

`EventText: No free transaction store found in %s`

Typ: **Warnung**

In einer Funktion wurde kein freier Transaktionsspeicher gefunden.

MSG_NU_INVALID_CIDL

`EventText: NCIDL invalid`

Typ: **Major**

Die in der Meldung gesendete CIDL ist ungültig.

MSG_NU_CAR_FAILED

`EventText: Call to CAR function failed`

Typ: **Major**

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: **Major**

Ungültige Antwort von CAR.

MSG_NU_UNEXPECTED_MSG

`EventText: Unexpected message: State:%d, Event:0x%x, Msgtype:0x%x`

Typ: **Major**

Unerwartete Meldung in einem bestimmten NU-Status.

MSG_NU_UNEXPECTED_TIMER

`EventText: Timer unexpected: State: %d, Subind:0x%x`

Typ: **Minor**

Unerwartetes Timer-Ereignis in einem bestimmten NU-Status.

MSG_NU_FREE_CHN_UNEXPECTED

`EventText: Free channel unexpected: State: %d`

Typ: **Major**

Unerwartet freier Kanal in einem bestimmten NU-Status.

MSG_NU_FREE_CHN_COMF_TOO_LATE

`EventText: Free channel confirmation too late State: %d`

Typ: **Major**

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: **Minor**

In einem bestimmten NU-Zustand ist eine Ereignisausnahme aufgetreten.

MSG_NU_WRONG_CALL_REF

`EventText: Wrong Call Reference. Event: 0x%x`

Typ: **Major**

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: **Major**

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: **Minor**

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: **Minor**

IP-Fehler.

MSG_NU_UNKNOWN_MESSAGE

`EventText: Unknown message: Event:0x%x, Channel:%d`

Typ: **Minor**

An NU gesendete unbekannte Meldung.

MSG_NU_INTERNAL_ERROR

```
EventText: NU internal error: %s
```

Typ: **Minor**

Interner NU-Software-Fehler.

MSG_NU_TOO_MUCH_DIGITS

```
EventText: Too much digits send at a time
```

Typ: **Minor**

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: **Minor**

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: **Major**

Der Zugriff auf die Gerätetabelle ist nicht in Ordnung.

8.2.16 NU-Leg-Kontroll-Events

MSG_NULC_MESSAGE_ERROR

```
EventText: Unexpected message ID or eventcode (%x)
           %x = message type
```

Typ: **Warnung**

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: **Major**

Ein Pflicht-Parameter fehlt oder hat keinen gültigen Wert.

MSG_NULC_MEMORY_ERROR

`EventText: EventText: Canâ##t access/allocate memory`

Typ: **Major**

Die Anwendung erhielt den angeforderten Speicher nicht, oder irgendeine andere Operation gab einen Nullzeiger zurück.

MSG_NULC_INTERNAL_ERROR

`EventText: %s`

Typ: **Major**

Interner Fehler bei NU-Leg-Kontrolle.

MSG_NULC_INTERNAL_EVENT

`EventText: %s`

Typ: **Information**

Die Anwendung wurde erfolgreich gestartet oder beendet.

8.2.17 HFA-Manager-Events

MSG_HFAM_HAH_ALLOC_CHAN_ERR

`EventText: tried to allocate channel for client that is not in idle state`

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

Ungültige Portnummer mit Event-Code. Überprüfen Sie das System!

MSG_HFAM_MAIN_NO_LOGONTIMER_ERR

`EventText: No logon timer started for that client`

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

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: keine Daten -> ignorieren
```

Typ: **Minor**

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: **Minor**

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: **Minor**

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: **Major**

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: **Major**

Kundennummer war zu lang und wurde abgeschnitten. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_ALGORITM_OBJID_ERR

```
EventText: SubNo too long, cut !
```

Typ: **Major**

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: **Major**

Die Protokoll-Liste enthält zu viele Elemente. Überprüfen Sie das Client-Setup!

MSG_HFAM_LIH_RETURNED_SOCKET_ERR

`EventText: returned socket error`

Typ: **Major**

Zurück gegebener Socket-Fehler. LAN-seitiger Fehler.

MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR

`EventText: timeslot is valid`

Typ: **Major**

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: **Major**

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: **Major**

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: **Minor**

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: **Minor**

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: **Major**

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: **Minor**

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: **Minor**

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: **Minor**

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: **Minor**

`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: **Minor**

Ungültige Passwortlänge zu <Unternummer>, kein Hash. Überprüfen Sie das Client-Setup oder WBM!

8.2.18 HFA-Adapter-Events

MSG_HFAA_MESSAGE_ERROR

`EventText: Unexpected message ID or eventcode (%x)`

Typ: **Warning**

Unerwartete oder unbekannte Meldung empfangen.

MSG_HFAA_PARAM_ERROR

`EventText: Missing/not valid parameter %s in message %s`

Typ: **Major**

Ein Pflicht-Parameter fehlt oder enthält einen ungültigen Wert.

MSG_HFAA_MEMORY_ERROR

`EventText: Canâ##t access to/allocate memory`

Typ: **Major**

Die Anwendung erhält nicht den angeforderten Speicher, oder ein Konstruktor gibt einen Nullzeiger zurück.

MSG_HFAA_INTERNAL_ERROR

`EventText: %s`

Typ: **Major**

Ein interner Fehler im HFA-Adapter.

MSG_HFAA_INTERNAL_EVENT

`EventText: %s`

Typ: **Information**

Die Anwendung wurde erfolgreich gestartet oder beendet.

8.2.19 PPP-Anruf-Kontroll-Events

Derzeit keine implementiert.

8.2.20 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!

8.2.21 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!

8.2.22 SPE-Events

MSG_SPE_CERT_MISSING

Zertifikat für Signaling- und Payload-Encryption ist nicht vorhanden.??? Mehr Informationen nötig. ???

MSG_SPE_CERT_AVAIL

Zertifikat für Signaling- und Payload-Encryption ist verfügbar.??? mehr Informationen nötig. ???

MSG_SPE_CERT_UPDATED

Zertifikat für Signaling- und Payload-Encryption wurde aktualisiert.??? mehr Informationen nötig. ???

MSG_SPE_CERT_EXPIRED

Zertifikat für Signaling- und Payload-Encryption ist abgelaufen.??? mehr Informationen nötig. ???

MSG_SPE_CERT_TIMEREMAINING

Zertifikat für Signaling- und Payload-Encryption, verbleibende Zeit

MSG_SPE_CRL_EXPIRED

Zertifikatssperrliste für SPE ist abgelaufen.??? mehr Informationen nötig. ???

MSG_SPE_CRL_UPDATED

Zertifikatssperrliste für SPE wurde aktualisiert.??? mehr Informationen nötig. ???

MSG_SPE_ALL_CRLS_UPTODATE

Alle Zertifikatssperrlisten für SPE sind aktuell.??? Mehr Informationen nötig. ???

8.2.23 VCAPI-Events

MSG_BSD44_SELECT_ERROR

`EventText: Select error for VCAPI & DATAGW Dispatcher`

Typ: **Major**

Sockets für VCAPI- und DATAGW-Clients arbeiten nicht mehr.

MSG_BSD44_ACCEPT_ERROR

`EventText: Accept error for VCAPI Dispatcher`

Typ: **Major**

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: **Minor**

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: **Minor**

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: **Major**

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: **Major**

PLCI in `VS_Plci_Link` Tabelle nicht gefunden (benötigt, um `message_nbr` zu finden).

MSG_VCAPI_CONV_H2N_ERROR

`EventText: Conversion error:%d`

Typ: **Minor**

Die Meldung zum Client wurde nicht korrekt konvertiert.

MSG_VCAPI_CONV_H2N_FAILED

`EventText: Conversion for %s returns %d,expected %d`

Typ: **Minor**

Die Konvertierung liefert einen falschen Wert zurück.

MSG_VCAPI_WRONG_CONV_H2N

`EventText: Wrong conversion for %s`

Typ: **Minor**

Die Nachricht wurde nicht konvertiert (falsche Nachricht).

MSG_VCAPI_WRONG_MSG_LENGTH

`EventText: Wrong message length %d`

Typ: **Minor**

Die Gesamtlänge der CAPI-Nachricht stimmt nicht.

MSG_VCAPI_CONV_N2H_FAILED

`EventText: Conversion for %s returns %d,expected %d)`

Typ: **Minor**

Die Konvertierung gibt einen falschen Wert zurück.

MSG_VCAPI_WRONG_CONV_N2H

`EventText: Wrong conversion for %s`

Typ: **Minor**

Die Nachricht wurde nicht konvertiert (falsche Nachricht).

MSG_VCAPI_UNKNOWN_MSG_N2H

`EventText: unknown msg %s`

Typ: **Minor**

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: **Major**

Es ist nicht möglich, eine neue Verbindung für VCAPI zu errichten.

MSG_VCAPI_DISP_NOT_READY

`EventText: VCAPI-Dispatcher not ready`

Typ: **Major**

Der VCAPI-Server hat keine Meldung `VCAPI_EVENT_START_OPERATION_REQ` an den Dispatcher gesendet.

MSG_VCAPI_NO_CLIENT

`EventText: no client address`

Typ: **Minor**

Keine Client-Adresse.

MSG_VCAPI_WRONG_BUF_LEN

`EventText: Wrong buffer length %d`

Typ: **Minor**

Die Puffergröße befindet sich nicht innerhalb der Grenzen der Meldung.

MSG_VCAPI_NO_RCV_BUFFER

`EventText: rcvBufPP=0x%x null`

Typ: **Minor**

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: **Minor**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

Der Socket konnte nicht geöffnet werden (Verbindungen mit Clients sind nicht möglich).

MSG_VCAPI_SOCKET_BIND_ERR

`EventText: bind error for socket %d`

Typ: **Major**

Bindungs-Fehler beim VCAPI-Socket (Verbindungen mit Clients sind nicht möglich).

MSG_VCAPI_LISTENING_ERR

`EventText: listening error for socket %d`

Typ: **Major**

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: **Minor**

Fehler beim Empfangen einer Meldung für den VCAPI-Dispatcher.

MSG_VCAPI_NO_ALLOC_MSG

`EventText: Not possible to allocate a buffer`

Typ: **Major**

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: **Minor**

Beim Empfangen einer Meldung von `CAPI_PAYLOAD_IF` wurde PLCI in der Tabelle `VS_Plci_Link` nicht gefunden .

MSG_VCAPI_IND_ALLOC_ERR

`EventText: Not possible to allocate a buffer for CMT_DATA_IND`

Typ: **Major**

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: **Major**

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: **Minor**

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: **Major**

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: **Minor**

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: **Major**

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: **Minor**

Der verbundene Socket wurde nicht in der Verbindungstabelle gespeichert. Es können keine Daten empfangen werden.

MSG_VCAPI_UNKNOWN_NTFY

EventText: Unknown notification. Used value:%d

Typ: **Warning**

Unbekannte Benachrichtigung.

MSG_VCAPI_NO_LNK_CONN

`EventText: Link number not found in connection table`

Typ: **Minor**

Die Linknummer wurde in der Verbindungstabelle nicht gefunden.

8.2.24 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 haben einem `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: **Major**

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: **Major**

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: **Major**

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.

8.2.25 H.323-Client-Events

MSG_H323CLIENT_INVALID_CLIENTID

`EventText: invalid Peer ID: %d`

Typ: **Major**

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: **Minor**

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: **Major**

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: **Major**

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: **Major**

Software-Fehler: ungültiger Parameter. Das Trace-Profil H323Client-Internal wird gestoppt.

8.2.26 IPNC-Events

MSG_IPNC_MESSAGE_ERROR

`EventText: message error: %s`

Typ: **Major**

Eine unerwartete Meldung wurde empfangen und ignoriert. Das Trace-Profil IPNC-Std wird gestoppt.

MSG_IPNC_MESSAGE_DUMP

```
EventText: message error: %s% M
```

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

Asynchronie zwischen den Zuständen von CP und IPNC entdeckt. Das Trace-Profil IPNC-Std wird gestoppt.

8.2.27 IPNCA-Events

MSG_IPNCA_ERROR

```
EventText: IPNC Adapter: (some) Error description ('IPNC
Adapter: %sâ##)
```

Typ: **Minor**

Ein kleinerer Fehler ist aufgetreten.

8.2.28 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.

8.2.29 OAM-Events

MSG_TLS_MUTEX_BLOCKED

`EventText: Mutex blocked`

Typ: **Major**

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 ein gültiges Verhalten.

MSG_OAM_QUEUE_FULL

`EventText: POAM Msg Queue (%s) full. Remove Messages`

Typ: **Major**

Die Warteschlange von OAM-Tasks (Trace, Event, OAM) ist voll. Alle Meldungen werden gelöscht. Siehe hierzu auch Abschnitt 7.4.1.4, "Überlastung der Baugruppe durch Trace-Informationen".

MSG_OAM_PUT_TO_QUEUE_FAILED

`EventText: Put to OAM Msg Queue (%s) failed. Remove Message`

Typ: **Major**

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: **Major**

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 V8 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 Schreibberechtiung erhalten. Damit kann er die Gateway-Konfiguration ändern.

MSG_ADMIN_DIDNT_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: **Minor**

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.

8.2.30 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.

8.2.31 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 initialisation 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**

Die Länge eines Pakets von MUX ist gleich 0. Informieren Sie den IP-Verantwortlichen über diese Meldung!

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**

Die Länge eines Pakets von MUX ist gleich 0. Informieren Sie den IP/MUX-Verantwortlichen!

8.2.32 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 coudnÂ´t be opened for device %X`

Typ: **Warning**

Fehler beim Vxworks-Costream zum Ã–ffnen 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 Initialising 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)â##`

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.

8.2.33 MAGIC / Device-Manager-Events

8.2.33.1 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: **Major**

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: **Major**

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 â##%uâ## will be taken
out of service
```

Typ: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

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: **Major**

`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 beim nachfolgenden Event-Text: **Minor**

`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: **Major**

`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.

8.2.33.2 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.

8.2.33.3 Layer2-Kommunications-Meldungen

MSG_SCN_ERROR_12_MSG

`EventText: L2 Error: %d Primitive: %d received on Device: %d`

Typ: **Major**

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: **Major**

Das Hinzufügen eines Parameters schlug fehl.

MSG_SCN_DEV_NOT_IN_DEVLIST

`EventText: Device %d not in devicelist of SCN_TASK`

Typ: **Major**

Das angegebene Device wurde in der Device-Liste nicht gefunden.

MSG_SCN_GET_ADMMSG_FAILED

`EventText: Reading message from admin stream failed`

Typ: **Major**

Vom Admin-Stream kann eine Meldung nicht gelesen werden.

MSG_SCN_GET_LDAPMSG_FAILED

`EventText: Reading message for device %d failed`

Typ: **Major**

Vom angegebenen Device kann eine Meldung nicht gelesen werden.

MSG_SCN_UNEXPECTED_L2_MSG

`EventText: Unexpected layer2 message on device %d`

Typ: **Major**

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: **Major**

Eine Operation am angegebenen Stream schlug fehl.

MSG_SCN_POLL_FD

`EventText: Poll returned unexpected value -1`

Typ: **Major**

Das Polling schlug fehl.

MSG_SCN_OPEN_STREAM_FAILED

`EventText: Open stream failed on device %d`

Typ: **Major**

Das Ã–ffnen eines Kommunikationspfads zu Layer2 schlug fehl. Starten Sie das System neu!

MSG_SCN_UNEXPECTED_POLL_EVENT

`EventText: Unexpected poll event on device %u`

Typ: **Major**

Für das angegebene Device wurde unerwarteter Event erhalten.

MSG_SCN_BIND_FAILED

`EventText: Bind for device: %d failed`

Typ: **Major**

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-Text: **Information**

`EventText: DEVMGR DevId: %d Layer2 In-Service`

Layer2 ist bereit. Verbindungen zu diesem Device sind möglich. Ein SNMP-Trap wird erzeugt.

8.2.34 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 module #<nr> done`

Diese Meldung erscheint beim Starten und markiert den erfolgreichen Abschluss des Boot-Vorgangs des DSP-Moduls.

8.2.35 Bedeutendere ASC-Events

MSG_ASC_ERROR

`EventText: DSP channel not initialized`

Typ: **Indeterminate**

Möglicherweise ein Konfigurationsproblem. Verifizieren Sie die ASC-Konfiguration im Gateway.

8.2.36 Bedeutendere ASP-Events

MSG_ASP_ERROR

Typ bei den nachfolgenden Event-Texten: **Critical**

`EventText: Hardware Configuration 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.

8.2.37 Kleinere 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!

8.2.38 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: **Ciritical**

Beim Lesen der angegebenen Filterregel war es nicht möglich, den angegebenen Parameter zu lesen.

8.2.39 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: **Ciritical**

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: **Ciritical**

Die Anzahl der eingegebenen Regeln ist größer als das vordefinierte Maximum.

MSG_MAF_NETBUFFER

`EventText: IP packet seems to be corrupt`

Typ: **Ciritical**

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: **Ciritical**

Ein Fehler trat auf beim Versuch, auf den Ethernet-Header eines IP-Pakets zuzugreifen.

8.2.40 IP-Stack-Events

MSG_IPSTACK_NAT_ERROR

`EventText: CNAT Error: %s`

Typ: **Ciritical**

Ein kritischer Fehler trat auf bei der Netzwerk-Adressübersetzung (NAT).

MSG_IPSTACK_SOH_ERROR

`EventText: Error occurred in Socket Handler`

Typ: **Ciritical**

Beim Socket-Handler trat ein Fehler auf.

MSG_IPSTACK_INVALID_PARAM

`EventText: IP-Stack invalid parameter %s, value %s`

Typ: **Minor**

Der IP-Stack hat einen ungültigen Parameter empfangen.

8.2.41 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.

8.2.42 Test-Loadware-Events

MSG_TESTLW_INFO

`EventText: Info: %p`

Typ: **Information**

Information über TESTLW-Funktionen (erfolgreiche Initialisierung usw.).

MSG_TESTLW_ERROR

`EventText: Error: %p`

Typ: **Major**

Fehler bei Initialisierung, wegen Empfang einer unbekannten Meldung, bei Speicher- und Timer-Fehlern.

8.2.43 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: Error: %p`

Typ bei den nachfolgendem Fehlern: **Warning**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern.

Typ bei den nachfolgendem Fehlern: **Major**

Fehler beim Ã–ffnen 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: 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: 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: 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: Error: %p`

Typ: **Warning/Major**

Fehler bei der Initialisierung, beim Empfang unbekannter Meldungen oder bei Speicherfehlern und Fehlern beim Ã–ffnen des HDLC-Treibers.

8.2.44 IP-Accounting-Events

MSG_IPACCSRV_SOCKET_ERROR

`EventText: Socket Error: %d (%s)`

Typ: **Major**

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: **Major**

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: **Major**

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 IP-Counting-Tabelle wurde überschritten. 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!

8.2.45 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 und ERH_CONFIGURATION und Trace-Level 6, um weitere Informationen zu gewinnen. Häufig 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. zutr???noch Informationen nötig.???

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.

8.2.46 IPNCV-Events

MSG_IPNCV_SIGNALING_ERROR

`EventText: IPNCV Signaling Error: %s`

Typ: **Warning**

Software-Fehler: ungültige interne Daten entdeckt.

8.2.47 XMLUTILS-Events

MSG_XMLUTILS_ERROR

`EventText: %d`

Typ: **Major**

In der XMLUTILS-Komponente ist ein Fehler aufgetreten.

8.2.48 Fehler-Events

MSG_OSF_PCS_ERROR

`EventText: %p`

Typ: **Major**

OSF hat einen bedeutenden Fehler entdeckt.

8.2.49 LAN-Signalisierung bezogene Events â“ 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).

8.2.50 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.

8.2.51 Client releated 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: **Major**

QDC-Meldungsspeicher ist voll. Meldungen können verloren gehen.

QDC_SYSTEM_ERROR

`EventText: QDC software failure`

Typ: **Major**

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.

8.2.52 QDC CGWA releated 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.

8.2.53 QDC VoIPSD Fehlerberichts-Events

QDC_VOIPSD_ERROR

`EventText: Error in secure data handling: %s`

Typ: **Information**

Eine der Komponenten meldet einen Fehler bei der 'sicherenâ Datenübertragung: %s

8.2.54 SIP bezogene 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.

9 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.

9.1 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 auf UNIX basierende Betriebssysteme werden in der RFC 1147 ausführlich beschrieben. Spezielle Parameter können der Hilfe des jeweiligen Betriebssystems entnommen werden und in der Regel durch Eingabe von `<Befehl> -?` abgerufen werden.

9.1.1 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.

9.1.2 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 erhalten....... ...:  Di., 17.08.1999 08:43:30

Lease läuft ab....... ...:  Di., 19.01.2038 04:14:07
```

9.1.3 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
Address: 192.168.0.1
Name: localhost
Address : 127.0.0.1
```

Der Host 'localhost' besitzt die IP-Adresse 127.0.0.1.

9.1.4 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
```

9.1.5 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-Betriebsysteme:

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        Zustand
....
....
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	Zustand
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	Zustand
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.

9.1.6 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.

9.1.7 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. Der Standardwert 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. Der Standardwert ist 100.
`-w <Zeitüber-schreitung>`	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.

9.1.8 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
`delete`	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 die Routen über den `route` Befehl nur statisch 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	Subnet-Mask	Gateway-Adresse	Schnittstelle	Anzahl
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
192.168.128.255	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.

9.1.9 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.
```

9.1.10 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

9.1.11 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
```

9.2 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:

Tabelle 3: Netzwerkklassen und Standardnetzwerkmasken

Class	Subnet Mask
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.

Tabelle 4: Beispiel einer Class C Standardnetzwerkmaske

	Netzwerk			Host
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Subnet-Mask	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.

Tabelle 5: 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.

Tabelle 6: Beispiel des Binärformats einer Subnetzmaske

Class C	**Netzwerk**			**Host**
Bytes	1. Byte	2. Byte	3. Byte	4. Byte
Subnet-Mask	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
Subnet-Mask	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.

Tabelle 7: Berechnung neu entstandener Subnetze

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
0000 0000	0	192.168.1.0	192.168.1.63	1â“62

4. Byte	Dezimal	Neue Netzwerke	Broadcast Adresse	Hostadressen
0100 0000	64	192.168.1.64	192.168.1.127	65â“126
1000 0000	128	192.168.1.128	192.168.1.191	129â“190
1100 0000	192	192.168.1.192	192.168.1.255	193â“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 â“ rein rechnerisch â“ 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.

Tabelle 8: Hostanteil in einem Netzwerkanteil

	Netzwerk			Host	Netzwerk
Bytes	1. Byte	2. Byte	3. Byte	4. Byte	
Subnet-Mask	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.

Tabelle 9: Netzwerkadressen in Abhängigkeit der letzten beiden Bit-Stellen

4. Byte	Dezimal	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.

Tabelle 10: 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.

Tabelle 11: Übersicht der meistgenutzten Masken der Klasse C

Subnet Mask	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
255.255.255.0	1	253	0	255	1 â“ 254
255.255.255.128	2	126	0	127	1 â“ 126
			128	255	129 â“ 254
255.255.255.192	4	62	0	63	1 â“ 62
			64	127	65 â“ 126
			128	191	129 â“ 190
			192	255	193 â“ 254

Subnet Mask	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
255.255.255.224	8	30	0	31	1 â“ 30
			32	63	33 â“ 62
			64	95	65 â“ 94
			96	127	97 â“ 126
			128	159	129 â“ 158
			160	191	161 â“ 190
			192	223	193 â“ 222
			224	255	225 â“ 254
255.255.255.240	16	16	0	15	1 â“ 14
			16	31	17 â“ 30
			32	47	33 â“ 46
			48	63	47 â“ 62
			64	79	65 â“ 78
			80	95	81 â“ 94
			96	111	97 â“ 110
			112	127	113 â“ 126
			128	143	129 â“ 142
			144	159	145 â“ 158
			160	175	161 â“ 174
			176	191	177 â“ 190
			192	207	193 â“ 206
			208	223	209 â“ 222
			224	239	225 â“ 238

Subnet Mask	Anzahl Netze	Hosts pro Subnet	Subnet	Broadcast Adr.	Hosts
			240	255	241 â“ 254

Beispiel:

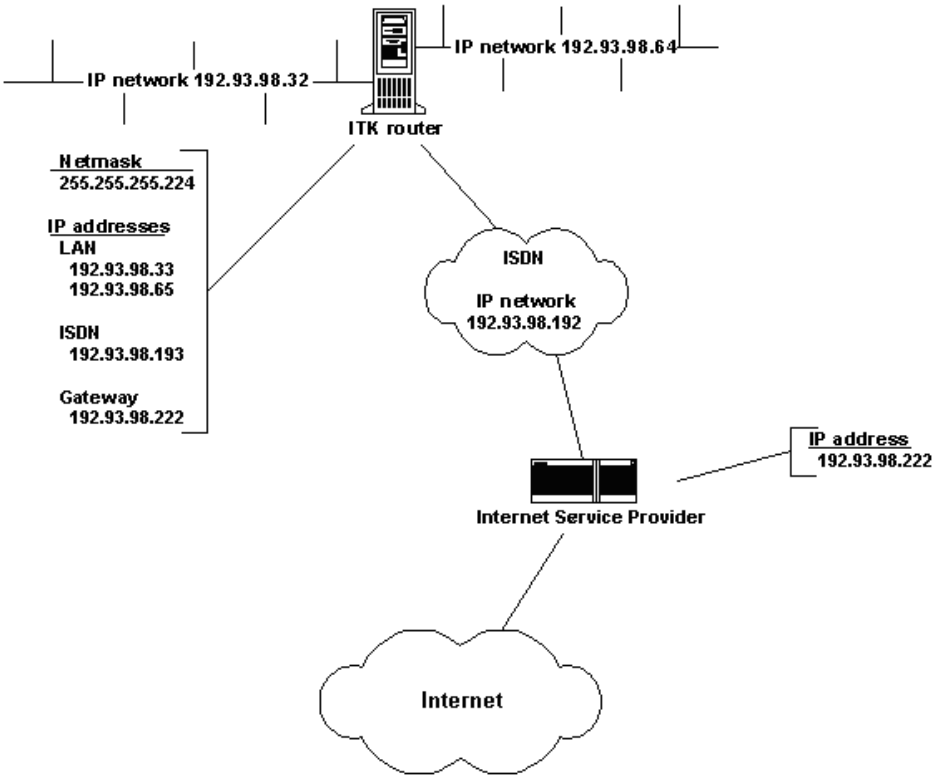
Ein LAN mit zwei Ethernet-Netzwerken soll über einen ISDN-Zugang an das Internet angeschlossen werden. Alle Stationen im lokalen Ethernet sollen Zugriff auf das Internet haben und auch aus dem Internet heraus direkt erreichbar sein. Legt man entsprechende Strukturen einer Class C-Adresse zugrunde, so 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.

9.3 Portnummern

9.3.1 Portnummern auf OpenScape 4000 V8

Tabelle 12: Portnummern auf OpenScape 4000 V8

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	1500	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		

9.4 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)

10 Anhang: Internet-Verweise

Die nachfolgenden Internet-Quellen bieten Original- oder Detail-Informationen zu technischen Standards, die im HG 3500/3575 zum Einsatz kommen.

10.1 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

10.2 Sonstige Quellen

http://www.protocols.com/pbook/VoIP.htm

1) Voice Over IP Reference Page

http://de.wikipedia.org/wiki/Voice_over_IP

Wikipedia-Artikel zu 'Voice over IP'.

11 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 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 â“ 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 â“ Telecommunication Standardization Sector) niedergelegt.

HFA

HiPath

HiPath (von 'Highly Integrated Pathwork') ist eine innovative Strategie zur Implementierung eines umfassenden IP-Migrationskonzepts, das die

Integration von Multimedia-Kommunikation in bestehenden IP-basierten Unternehmensnetzwerken vereinfacht.

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 â“ 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. HG 3500/3575 Das 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.

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.

MIB

Abkürzung für 'Management Information Base'. Eine MIB fasst Informationen und Parameter eines Netzwerkgeräts zusammen. Sie ist für die Verwaltung über SNMP erforderlich.

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 Firstâ.

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.

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.

PSTN

Abkürzung für 'Public Switched Telephone Network'. PSTN ist das weltweite öffentliche Telefonnetz.

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.

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.

QSIG

QSIG ist ein Protokoll für das Vernetzen von Knoten, das von der ITU-T (International Telecommunication Union â“ Telecommunication Standardization Sector) adaptiert wurde. Mithilfe von QSIG können Nebenstellenanlagen verschiedener Hersteller verbunden werden.

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

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.