A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000

HG 3500 on STMIX or STMIY V10

Administration Documentation
04/2025

A31003-H31A0-M102-07-76A9

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.

Contents

1 Introduction....9
1.1 Target Audience....9
1.2 Contents of this Manual....9
1.3 Note for Internet Explorer....9
1.4 Conventions Used....10

2 Preparing the Board....11

3 USB Access....12

4 WBM....13
4.1 Preparing for Configuration....14
4.2 Starting and Finishing WBM....14
4.2.1 Starting via OpenScape 4000 Assistant....14
4.2.2 Starting via Web Browser....15
4.2.3 Finishing a WBM Session....15
4.3 WBM Application Interface....15
4.3.1 Modules....16
4.3.1.1 *Configuration*....16
4.3.1.2 Maintenance....17
4.3.1.3 Help....17
4.3.1.4 Logoff....17
4.3.2 Icons in the WBM Window's Status Area....17
4.3.3 Icons in the WBM Tree Representations....18
4.3.4 Dialogs and Dialog Elements....19
4.4 OpenScape 4000 Manager....20

5 HFA WBM - Configuration....21
5.1 Configuration....21
5.2 Basic Settings....21
5.2.1 Gateway....21
5.3 Security....22
5.3.1 Security Options....22
5.3.2 TLS Configuration for HTTPS....23
5.4 SPE....23
5.4.1 Import Keycert (STMIX/STMIY - HFA only)....24
5.4.2 Show Keycert....25
5.4.3 Delete Keycert....25
5.4.4 SPE CA Certs....26
5.4.5 SPE Security Setup for HFA....26
5.5 Network Interfaces....28
5.6 Miscellaneous....28
5.6.1 NGS....28
5.6.2 QoS-Data-Collection....29
5.7 SIP Functions....32

6 SIP/IPDA WBM - Configuration....33
6.1 Configuration....33
6.2 Basic Settings....33
6.2.1 System....33
6.2.1.1 Partnumber....34
6.2.1.2 Software Build....34

6.2.2 Gateway....34
6.2.3 Quality of Service....36
6.2.4 Timezone Settings....37
6.3 Statistics....37
6.3.1 Call Statistics....37
6.3.1.1 Delete Statistics....37
6.3.1.2 Call Statistics (1 h)....38
6.3.1.3 Call Statistics (24 h)....38
6.3.1.4 Call Statistics (Total)....38
6.3.1.5 Call Statistics (Maximum Parallel)....39
6.3.1.6 LAN Call Statistics....39
6.3.1.7 PBX Call Statistics....39
6.3.1.8 Current Connections....40
6.4 Security....40
6.4.1 User Accounts....40
6.4.2 Signaling and Payload Encryption (SPE)....41
6.4.2.1 SPE Security Setup for SIP....41
6.4.2.2 SPE Certificate....45
6.4.2.3 SPE CA Certificate(s)....46
6.4.3 TLS Ciphers for SIP....48
6.5 Network & Routing....48
6.6 Routing....49
6.6.1 IP Routing....49
6.6.2 Static Routes....49
6.6.2.1 Add Static Route....50
6.6.3 Default Router....51
6.6.4 DNS Server....51
6.6.4.1 ICMP Request....52
6.6.4.2 Ping....52
6.6.4.3 Traceroute....52
6.6.5 Dialing Parameters....53
6.6.5.1 Edit General Dialing Parameters....53
6.6.5.2 Configured Subscribers....54
6.6.5.3 Configured IP Addresses....55
6.7 Voice Gateway....55
6.7.1 H.323 Parameters....55
6.7.2 SIP Parameters (not for HG3575)....56
6.7.3 Codec Parameters....57
6.7.4 IP Networking Mode....59
6.7.5 SIP Trunk Profile Parameter (not for HG3575)....60
6.7.6 SIP Trunk Profiles....60
6.7.7 Hunt Group....61
6.7.7.1 Add....62
6.7.8 Destination Codec Parameters....62
6.7.8.1 Add Destination Codec Parameters....62
6.7.8.2 DARs for MLPP....63
6.7.9 Clients....63
6.7.9.1 UFIP SIP....63
6.7.9.2 Classic SIP....65
6.7.10 CICA....65
6.7.11 ISDN Classmarks....65
6.8 Payload....66
6.8.1 Payload Parameters....66
6.8.2 Fax/Modem Tone Handling....66
6.9 HFA Functions....67

7 HFA WBM - Maintenance....68
7.1 Maintenance....68
7.2 SW-Update....68
7.2.1 Show SW-Version....68
7.2.2 LW Update....69
7.2.3 LW Activation....70
7.2.4 OS Update....71
7.2.4.1 OS Update Settings....71
7.2.4.2 OS Update Actions....71
7.3 Backup/Restore....72
7.3.1 Export Config....72
7.3.2 Export Sec Config....73
7.3.3 Import Config....73
7.3.4 Import Sec Config....74
7.3.5 Import of classic STMI backup data to STMIX/STMIY....74
7.3.6 Factory Reset....75
7.4 Logs....76
7.4.1 Export Logs....76
7.4.2 Delete Logs....77
7.4.3 Trace Profiles....77
7.5 Secure Trace....79
7.5.1 Import Certificate....80
7.5.2 Show Certificate....81
7.5.3 State....81
7.5.4 Start Trace....82
7.5.5 Stop Trace....83
7.6 DLS Client....83
7.6.1 DLS Settings....84
7.6.2 Enter PIN....85
7.6.3 Reset Bootstrapping....86
7.6.4 Contact DLS....86
7.6.4.1 DLSC Keycert....86
7.6.4.2 1.DLSC Keycert....87
7.6.5 DLSC CA Certs....87
7.6.5.1 "1. DLSS CA Cert", "2. DLSC CA Cert"....87
7.7 Diagnostic....88
7.7.1 Diagnostic Functions....88
7.7.2 Diagnostic Files....90
7.8 Status Information....90
7.8.1 System Information....90
7.8.1.1 Show Thread Health....90
7.8.2 SoftGate Connection Control....91
7.8.2.1 Show All Connections....91
7.9 Reboot OS....91
7.9.1 Reboot OS....91

8 SIP/IPDA WBM - Maintenance....93
8.1 Maintenance....93
8.2 Config & Update....93
8.2.1 Configuration....93
8.2.2 Configuration Data....93
8.2.2.1 Load from Gateway....94
8.2.2.2 Load to Gateway....95
8.2.3 SSL Data....96
8.2.3.1 Load from Gateway....96
8.2.3.2 Load to Gateway....97

8.2.4 Reset Configuration to Factory Default..... 97
8.3 Job List..... 98
8.4 Traces & Events..... 98
8.4.1 Traces..... 98
8.4.1.1 Load All Logs..... 99
8.4.1.2 Delete All Logs..... 99
8.4.1.3 Trace Configuration..... 100
8.4.1.4 Load Trace Log..... 101
8.4.1.5 Clear Trace Log..... 101
8.4.1.6 Trace Profiles..... 101
8.4.1.7 Stop All Trace Profiles..... 102
8.4.1.8 Trace Components..... 103
8.4.1.9 Display Started Trace Components..... 103
8.4.1.10 Stop All Trace Components..... 104
8.4.1.11 Secure Trace..... 104
8.4.1.12 Secure Trace Options..... 105
8.4.1.13 Start Secure Trace..... 106
8.4.1.14 Stop Secure Trace..... 107
8.4.1.15 Import Secure Trace Certificates (PEM or Binary)..... 107
8.4.1.16 M5T Trace Components..... 107
8.4.1.17 M5T Syslog Trace..... 108
8.4.1.18 Service Center..... 109
8.4.2 Events..... 109
8.4.2.1 Event Configuration..... 109
8.4.2.2 E-Mail..... 110
8.4.2.3 Reaction Table..... 111
8.4.3 Admin Log..... 112
8.4.3.1 Configuration..... 112
8.4.3.2 Load Admin Log Data..... 112
8.5 Appl. Diagnostics..... 113

9 Appendix: Traces and Events..... 114
9.1 Traces..... 114
9.1.1 Trace Components..... 114
9.1.2 Trace Profiles..... 141
9.1.2.1 Profiles under Normal/Heavy Load..... 141
9.1.2.2 Profiles under Light Load..... 146
9.2 Events..... 152
9.2.1 Overview: Event Codes..... 153
9.2.2 Status Events..... 177
9.2.3 Reboot Events..... 180
9.2.4 Resource Monitoring Events..... 183
9.2.5 Routing Events..... 186
9.2.6 Call Control and Feature Events..... 188
9.2.7 SCN Protocol Events..... 191
9.2.8 H.323 Events..... 196
9.2.9 H.235 Events..... 198
9.2.10 RTPQM Events..... 198
9.2.11 GSA Events..... 198
9.2.12 DGW Events..... 199
9.2.13 CAR Events..... 206
9.2.14 REG Events..... 210
9.2.15 NU Events..... 211
9.2.16 NU Leg Control Events..... 214
9.2.17 HFA Manager Events..... 214
9.2.18 HFA Adapter Events..... 219

9.2.19 PPP Call Control Events....219
9.2.20 PPP MANAGER Events....219
9.2.21 PPP Stack Events....220
9.2.22 SPE Events....220
9.2.23 VCAPI Events....220
9.2.24 VCAPI Application Events....226
9.2.25 H.323 Client Events....229
9.2.26 IPNC Events....230
9.2.27 IPNCA Events....231
9.2.28 MPH Events....231
9.2.29 OAM Events....231
9.2.30 CLI Events....234
9.2.31 HIP Events....234
9.2.32 SI Events (System Interface Events)....236
9.2.33 MAGIC/Device Manager Events....238
9.2.33.1 Startup and Internal Messages....238
9.2.33.2 LEG Management Messages....242
9.2.33.3 Layer2 Communication Messages....244
9.2.34 Important Platform Software Status Events....245
9.2.35 Major ASC Events....246
9.2.36 Major ASP Events....246
9.2.37 Minor ASP Events....246
9.2.38 IP Filter Events....246
9.2.39 MAC Filter Events....247
9.2.40 IP Stack Events....248
9.2.41 DELIC Events....248
9.2.42 Test Loadware Events....248
9.2.43 Fax Converter, HDLC and X.25 Events....249
9.2.44 IP Accounting Events....250
9.2.45 Endpoint Registration Handler (ERH) Trace Events....251
9.2.46 IPNCV Events....252
9.2.47 XMLUTILS Events....252
9.2.48 Error Events....253
9.2.49 LAN Signaling Events - CCE....253
9.2.50 Events for LLC Operation....253
9.2.51 Client-Related Events....254
9.2.52 QDC-CGWA-Related Events....254
9.2.53 QDC VoIPSD Error Report Events....255
9.2.54 SIP Events....255

10 Appendix: WAN/LAN Management....256
10.1 Utility Programs for TCP/IP Diagnostics....256
10.1.1 ping....256
10.1.2 ipconfig....257
10.1.3 nslookup....259
10.1.4 hostname....260
10.1.5 netstat....260
10.1.6 nbtstat....263
10.1.7 pathping....264
10.1.8 route....265
10.1.9 tracert....267
10.1.10 arp....267
10.1.11 Telnet....268
10.2 IP Addressing: Subnets....269
10.3 Port Numbers....275
10.3.1 Port Numbers on the OpenScape 4000 V10....275

10.4 PC Sound Settings for Voice over IP....276

11 Appendix: Internet References....278
11.1 RFCs....278
11.2 Other Sources....280

12 Glossary....281

Index....292

1 Introduction

This document describes the configuration of the HG 3500 on STMIX/STMIY gateway and the tools available for this configuration.

This chapter gives an overview of the manual. It describes:

- The target audience for this manual (see Section 1.1, "Target Audience")
- The contents of the chapters in this manual (see Section 1.2, "Contents of this Manual")
- Important note for Internet Explorer (see Section 1.3, "Note for Internet Explorer")
- The typographical conventions used (see Section 1.4, "Conventions Used")

1.1 Target Audience

This manual is aimed at administrators responsible for configuring the HG 3500 on STMIX/STMIY gateway. They should have experience in LAN administration and be familiar with the following areas:

- Hardware for data communication
- WAN (Wide Area Network) concepts and terms)
- LAN (Local Area Network) concepts and terms)
- Internet concepts and terms

They should have received instruction on the following:

- Installation and start-up of the HG 3500 on STMIX/STMIY gateway
- Configuring VoIP functions for the HG 3500 on STMIX/STMIY gateway
- Setting up and customized configuration of the data communication parameters on the HG 3500 on STMIX/STMIY gateway

1.2 Contents of this Manual

This manual offers a full description of administration options for the HG 3500 on STMIX/STMIY gateway and also contains background information on selected topics.

It explains how the HG 3500 on STMIX/STMIY gateway is to be administered after being installed in a subrack.

Further information on HG 3500 on STMIX/STMIY gateway may be found in the OpenScape 4000 V10 Service Manual.

Subsequent chapters provide a systematic description of the WBM interface for configuring and administering the HG 3500 on STMIX/STMIY gateway.

1.3 Note for Internet Explorer

IMPORTANT: After changing any Internet Explorer security settings for a WBM page (like adding the page in Trusted Sites) it is recommended to restart the browser in order to work correctly with the new settings.

1.4 Conventions Used

The following display conventions are used in this manual:

Table 1: Typographic Conventions

Convention	Example
`Courier`	Input and output Example: Enter `LOCAL` as the file name. `Command not found`
Italics	Variable Example: *Name* can contain up to eight characters.
Italics	Indicates user interface elements Example: Click *OK* Select *Exit* from the *File menu.*
Bold	Special emphasis Example: This name must **not** be deleted.
`<Courier>`	Keyboard shortcuts Example: `<CTRL>+<ALT>+<ESC>`
>	Menu sequence Example: Close file **>**.
Conventions Used	Cross-reference or hyperlink
	Additional information

2 Preparing the Board

All configuration data configured via the WBM of the board must be backed up by using the backup server. Otherwise all configuration data would be lost following a board swap out and the IP trunking connection could not be reestablished automatically. It is important to ensure that the backup server can be reached. If the backup server cannot be reached, the configuration data is also backed up in the board's flash.

IMPORTANT: As the STMIX/STMIY LW is no longer updated via HDLC compared to STMI2/4 a LW and OS update is mandatory, after receiving the board from supply chain.

3 USB Access

USB access is not often used. However, when you need to access a USB port, you can do it via a standard TRM account. The necessary drivers are stored in the installation ISO.

4 WBM

WBM stands for **W**eb **B**ased **M**anagement. WBM is the default administration interface for the STMIX/STMIY gateway. The WBM for STMIX has two parts: HG 3500 on STMIX/STMIY - SIP/IPDA and HG 3500 on STMIX/STMIY - HFA.

All PCs with TCP/IP-supported network connections running a compatible Web browser can access WBM if logged in to OpenScape 4000 Assistant. WBM has an integrated Web server, and can thus be accessed via a HTTPS URL.

Once WBM has been enabled on the gateway by the Root administrator, it is available via every TCP/IP connection, both via the LAN and the WAN.

The WBM user interface is available only in English.

Hardware requirements:

You need a standard PC or laptop with left button mouse for operating WBM.

Software requirements:

WBM is composed of HTML/XSL pages with frames. To use it, the following must be installed:

- Windows
- Microsoft Internet Explorer
- The following settings must be made in Microsoft Internet Explorer:
- – Activate the following option: *Tools -> Internet Options -> Advanced -> Empty Temporary Internet Files folder when browser is closed*
  – The connection from the administration PC to the gateway must not be routed over a proxy server. The following option should therefore be activated: *Tools -> Internet Options -> Connections -> LAN Settings: Settings... -> Proxy server: Bypass proxy server for local address*
  – The compatibility view mode has to be disabled for WBM of the HG 3500 on STMIX/STMIY: Tools -> Compatibility View

  Other browsers that support frames and JavaScript may also be compatible with WBM. Browsers that do not support frames cannot be used with WBM.

IMPORTANT: The inaccessibility of a DNS server configured on the administration PC significantly decreases WBM interface speeds when loading applets. If you encounter this problem, check the configured DNS server in the network settings of the administration PC. Remove unreachable DNS servers or enter reachable servers.

Initial configuration

This chapter describes initial configuration of the gateway.

Before starting the configuration, the gateway must have been installed according to the descriptions in the installation manual.

The basic configuration of the gateway involves four steps:

1) Preparatory work (see Section 4.1, "Preparing for Configuration").
2) Opening the WBM (see Section 4.2, "Starting and Finishing WBM").
3) Exiting the WBM session.

The WBM guides you through the configuration process step by step. The WBM session can be terminated once configuration is complete.

4.1 Preparing for Configuration

Appropriate preparations should be made before starting the configuration of the HG 3500 on STMIX/STMIY gateway to avoid unnecessary interruptions.

IMPORTANT: Ensure that the gateway was assigned the correct IP address before connecting it to the network.

4.2 Starting and Finishing WBM

Access options

There are two ways to start WBM for the HG 3500 on STMIX/STMIY gateway. It can be started via OpenScape 4000 Assistant, or directly from a Web browser using the WBM URL. Access via OpenScape 4000 Assistant is the most common method used.

Topics in this chapter

1) Section 4.2.1, "Starting via OpenScape 4000 Assistant" Section 4.2.2, "Starting via Web Browser" Section 4.2.3, "Finishing a WBM Session"

4.2.1 Starting via OpenScape 4000 Assistant

To start the WBM session, take the following steps:

1) Log in to OpenScape 4000 Assistant using your username and password.
2) In the tree structure, select *OpenScape 4000 Assistant* **>** *Expert Mode* **>** *Gateway Dashboard*. The *Gateway Dashboard* window is displayed with the existing boards:
3) In the line for the required HG 3500 on STMIX/STMIY board in the "Remote access" column, click *[WBM] [N/A]*. The Web server for the HG 3500 on STMIX/STMIY gateway is contacted. Since the server only works with HTTPS (secure data transmission), it sends a certificate.

NOTICE: You may see a message in the browser to the effect that there is a problem with the security certificate for the website. In this case, click *Continue to this website*.

4) Confirm the browser dialog with the certificate information. The WBM homepage is displayed:
5) In the *Configuration* and *Maintenance* modules, you can administer the HG 3500 on STMIX/STMIY gateway.

4.2.2 Starting via Web Browser

User Account

The user account "Administrator" is available for WBM. This account provides access to configuration settings.

The default user name is **TRM** and the default password is **HICOM** (as configured in AMO CGWB). You should modify these defaults in AMO CGWB.

Starting a WBM session

To start the WBM session, take the following steps:

1) Open your Web browser.
2) In the address bar of your Web browser, enter the WBM URL. The Web server for HG 3500 on STMIX/STMIY gateway is contacted. Since the server only works with HTTPS (secure data transmission), it sends a certificate.
3) Confirm the browser dialog with the certificate information. The login window for HG 3500 on STMIX/STMIY gateway.
4) Enter the username and password. Click *Login*. The homepage of WBM for HG 3500 on STMIX/STMIY gateway is displayed:
5) In the *Configuration* and *Maintenance* modules, you can administer the HG 3500 on STMIX/STMIY gateway.

4.2.3 Finishing a WBM Session

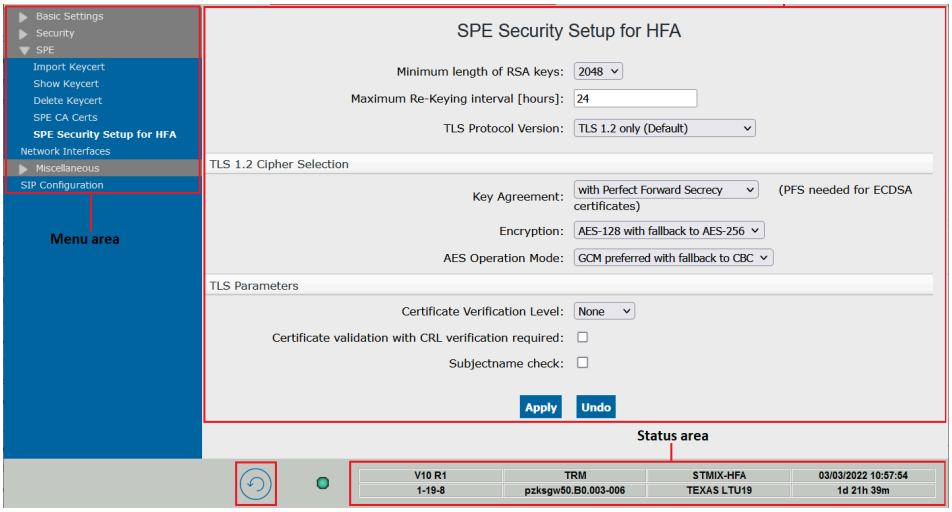
To finish the WBM session, take the following steps:

Click the *Logoff* module. The connection to the HG 3500 on STMIX/STMIY gateway is ended and the WBM session is closed.

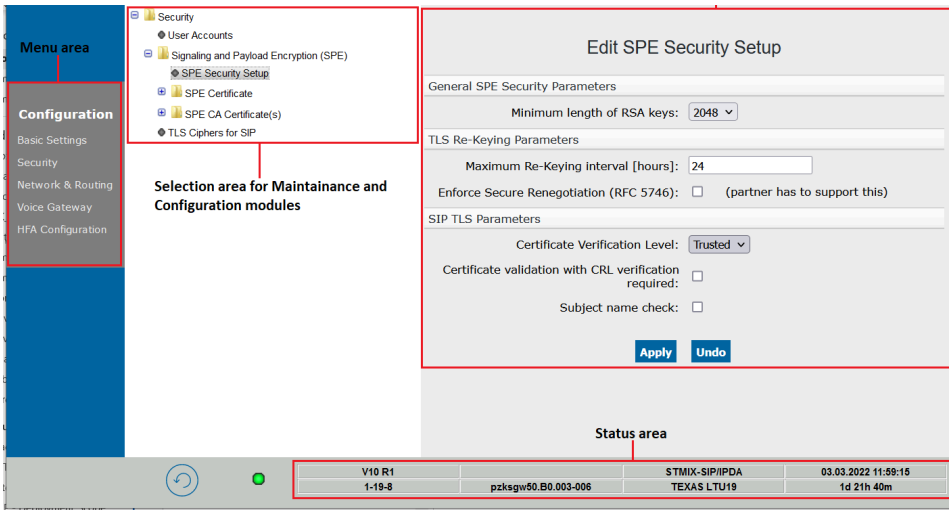
For more information on closing the WBM session, refer to Section 4.3.1.4, "Logoff".

4.3 WBM Application Interface

The main window in the WBM consists of the following areas:



WBM Interface - HFA



WBM Interface - SIP / IPDA

Module area:

The area under the banner displays the modules available. You can select the required module by clicking its name. Some selections with functionality will change to blue text when hovering over the selection. See Section 4.3.1, "Modules".

Menu area:

The area at the left is used for navigating within a module. The menus that are displayed here vary depending on the module selected.

Buttons and Status area:

The icons for controlling WBM and the status information that is constantly displayed are located at the bottom. For information on the meaning of the icons, see Section 4.3.2, "Icons in the WBM Window's Status Area".

Selection area for the *Maintenance* and *Configuration modules*

This area displays a Configuration-type tree structure where you can select individual functions.

4.3.1 Modules

The area under the banner displays the modules available. You can select the required module by clicking its name.

Modules available:

Configuration Maintenance Help Logoff

4.3.1.1 *Configuration*

The Configuration module features the necessary functions for configuring the gateway.

WBM path:

WBM **>** *Configuration*

The *Configuration* module's options are displayed on the left.

For a detailed description of the functions of the Configuration module, see Chapter 5, "Configuration".

4.3.1.2 Maintenance

This module contains all the functions necessary for gateway maintenance and administration.

WBM path:

WBM **>** *Maintenance*

The *Maintenance* module's options are displayed on the left.

For a detailed description of the functions of the *Maintenance* module, see Chapter 7, "Maintenance".

4.3.1.3 Help

WBM path:

WBM **>** *Help* > *Product Docu*

The following menu items are displayed:

- *About WBM*: The title of the WBM, for example `Web-Based Management for STMIX/STMIY-HFA`, is displayed.
- *Product Docu*: Single-click *Product Docu* in order to be redirected to the OpenScape 4000 Assistant login page.

4.3.1.4 Logoff

The gateway connection is cleared down when you click *Logoff* and the WBM session is ended. (see Section 4.3.2, "Icons in the WBM Window's Status Area").

WBM path:

WBM **>** *Logoff*

4.3.2 Icons in the WBM Window's Status Area

The control area is an applet that constantly provides control and status information. The figure below shows an example:

The following control icons are used:

Action Icon

The icon turns green to indicate a connection to the gateway Web server. The icon flashes red when there is no connection set up.

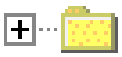
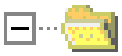
The following status information is also displayed:

- System version of OpenScape 4000 and installation location
- User access category and loadware version
- Board name and gateway location
- System date and time as well as time since last restart

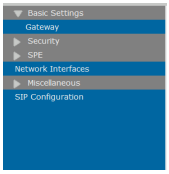
4.3.3 Icons in the WBM Tree Representations

The functions available in the *Configuration* and *Maintenance* modules are displayed in the contents area in a tree representation similar to Windows Explorer. This tree representation has the following icons:

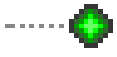
- Directories (SIP WBM)

	Any directory that contains hidden functions is characterized by a plus sign (+). A single-click will display these functions.
	The functions in this open directory are displayed. A single-click will hide these functions.

- Arrows (HFA WBM)

	(in the figure: *Basic Settings* = menu open): In the menu area, you can click these arrows to open or close a menu. Multiple menus can be opened. in the figure: Inactive menu items are green; active menu items are white.

- Bullet points (SIP WBM)

	**Gray:** This function can be activated but does not have status information.
	**Green:** This function is active and can be deactivated via an option on the WBM.
	**Red:** This function is inactive and can be activated via an option in the WBM.

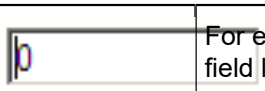
- Context menus
- Context menus are no longer displayed in the WBM.

4.3.4 Dialogs and Dialog Elements

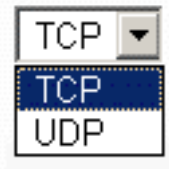
Inputs and modifications in the WBM are displayed in the browser window as dimmed dialogs within the browser window. Separate dialog windows can also be displayed, for example, to confirm a delete request.

The dialogs contain the following typical elements:12

Input fields

	For entering numeric or alphanumeric values. The relevant field label is displayed before, after or over the field. For security purposes, characters are exclusively displayed as unambiguous symbols, such as stars, in password fields. Characters unavailable on the keyboard can be inserted using the "Charmap" character table, for example, under MS Windows.

Dropdown lists

	Click the arrow to open or close the list. Select an entry with a left-click.

Check boxes

	(Here, the upper checkbox is disabled while the lower one is enabled): The relevant field label is displayed before, after or over the field. Click to enable or disable the relevant option.

Radio buttons

	(Here, the left check box is disabled while the right one is enabled): Radio buttons are combined in groups where one element is always selected. The relevant field label is displayed before, after or above the field. Click to enable or disable the relevant function.

Buttons

	Click to perform the action described by the button's label text. The texts are self-explanatory, for example *Undo* or *Apply*.

The following buttons are used:

- *Apply*: Data or changes entered are buffered in the RAM and, where applicable, verified.

- *Undo*: Data or changes entered in the dialog are discarded. The original status of the dialog is restored.
- *Add*: Add a new entry to a table.
- *OK*: Positive acknowledgment of separate dialog windows. The selected action is performed if you click this button (no undo available).
- *Load:* A previously selected file, for example for configuration data, is loaded.
- *Cancel*: Negative acknowledgment of separate dialog windows. The selected action is canceled if you click this button.
- *Delete*: The configured settings are deleted.
- *Back*: Change to the previous Web page within a multi-page dialog. This button is currently only used in wizards.

Sort sequence

	The sort sequence of a column can be changed, for example in ascending or descending alphabetical order, by clicking the triangle next to the title in a table header.

4.4 OpenScape 4000 Manager

OpenScape 4000 Manager is an administration tool for managing a OpenScape 4000 V10 and the OpenScape 4000 V10 nodes. The relevant parts of the OpenScape 4000 V10 network are displayed as a virtual OpenScape 4000 V10 system.

The IP address of the Management Client as well as the beginning and end of the session are logged at each session. The modified data continues to be logged in the OpenScape 4000 V10 nodes.

In the OpenScape 4000 V10 system, OpenScape 4000 Manager takes priority over other applications that are running. This means that the modified data is stored in the OpenScape 4000 V10 database and the application is alerted of the change.

A description of the OpenScape 4000 Manager may be found in the corresponding documentation.

5 HFA WBM - Configuration

5.1 Configuration

In this chapter the configuration of the HFA signaling protocol of the STMIX/ STMIY is described.

Configuration

WBM path

WBM **>** *Configuration*

The *Configuration* module is displayed

The Configuration module is used to define the basic settings of the STMIX/ STMIY-HFA gateway (basic settings) and to administer the Signaling & Payload Encryption (SPE) feature.

Options in the *Configuration* module

Basic Settings

Security

SPE

Miscellaneous

SIP Functions

5.2 Basic Settings

WBM path

WBM **>** *Configuration* **>** *Basic Settings*

In the *Basic Settings* menu, you can enter fundamental data about STMIX/ STMIY - HFA.

5.2.1 Gateway

WBM path

WBM **>** *Configuration* **>** *Basic Settings* **>** *Gateway* **>** *Gateway Properties*

The Gateway Properties dialog is displayed: You can enter basic data in this dialog.

Input fields

The following input fields are shown in this dialog:

- System Name: Enter the STMIX/STMIY - HFA name in this field, e.g. if multiple STMIX/STMIY-HFA systems are operated on a single AP shelf.

- Gateway Location: This field is read-only. The value is taken from AMO UCSU.

Buttons

The following buttons are shown in this dialog:

- Apply: Save your entries.
- Undo: The entries made are deleted and replaced by default values.

5.3 Security

In the *Security* menu you can manage Security Options and *TLS Configuration for HTTPs*.

WBM path

WBM **>** *Configuration* **>** Security

The following selection items are offered in this menu:

Security Options

TLS Configuration for HTTPS

5.3.1 Security Options

WBM path

WBM **>** *Configuration* **>** Security **>** *Security Options*

The Security Options mask is displayed.

Checkbox

The following checkbox is shown in this dialog:

- Force Secure TLS Renegotiation (RFC 5746): Only applies for HFA. TLS is vulnerable to situations where a malicious server establishes a connection to a target server, injects it with its own rogue data and then splices in the new TLS connection from a client. The target server treats the client's initial TLS handshake as a renegotiation of an existing connection that the malicious server has previously established and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. This problem can be avoided with secure renegotiation based on RFC 5746.

Buttons

The following buttons are shown in this dialog:

- Apply: Save your entries.
- Undo: The entries made are deleted and replaced by default values.

NOTICE: A SoftGate restart is required to make changes effective.

5.3.2 TLS Configuration for HTTPS

WBM path

WBM **>** *Configuration* **>** Security **>** *TLS Configuration for HTTPS*

Protocol TLSv1.3 with fallback to TLSv1.2 is supported from V10 onwards, SSLv2 and SSLv3 are not permitted due to security issues.

TLSv1.0 is no longer supported.

The TLS version for HTTPS protocol can be configured in WBM menu. It is offered and supported by the web server of the STMIX/STMIY - HFA.

The default TLS configuration is TLS 1.3 with fallback to 1.2.

NOTICE:

Web certificates with MD5 as signing algorithm are not supported anymore.

Please use SHA or SHA2 signed certificates.

5.4 SPE

SPE (Signaling & Payload Encryption) encrypts VoIP payload and signaling data streams to and from STMIX/STMIY - HFA. This feature is based on an asymmetric encryption process. Public and private keys are used for this type of process.

The individual VoIP clients and gateways, e.g. STMIX/STMIY - HFA, must be identifiable in the communication system. This is achieved using certificates containing private or public keys. Certificates are created either by a customer PKI certification authority (RA/CA) or by the DLS server's internal certification authority (CA). The DLS server sends the files containing these certificates to the gateway DLS client.

According to requirement, security settings for evaluating the certificates and encrypting data streams can be activated or deactivated. This increases or decreases the encryption security.

WBM path

WBM **>** *Configuration* **>** SPE

The *SPE* menu is displayed.

The following options are shown in this menu:

Import Keycert (STMIX/STMIY - HFA only)

Show Keycert

Delete Keycert

SPE CA Certs

SPE Security Setup for HFA

5.4.1 Import Keycert (STMIX/STMIY - HFA only)

NOTICE: When you import a certificate for the first time with active SPE, a reset is automatically performed.

NOTICE: You can import SPE certificates for STMIX/STMIY only here in the HFA WBM. The imported SPE certificates will be automatically distributed to the SIP/IPDA part. On the STMIX/STMIY - SIP/IPDA WBM you can view the certificates for diagnosis purposes.

NOTICE: Imported certificates will be automatically propagated to SIP functionality of STMIX/STMIY.

WBM **>** *Configuration* **>** SPE **>** *Import Keycert (STMIX/STMIY - HFA only)* **>** *Load a SPE Key Certificate via HTTP*

The Load a SPE Key Certificate via HTTP dialog is displayed. In this dialog, you can import an SPE key certificate by entering the decryption password and the file name. The file containing the certificate originates from a customer PKI certification authority (RA/CA) or the internal DLS server certification authority (CA) and must be available in PEM or PKCS#12 format.

The supported Public Key Algorithms for SPE certificates are:

- **RSA** with a minimum key length of 2048 bit for HFA and SIP.
- **ECDSA** for pure HFA STMIX/STMIY boards.

Input fields

The following input fields are shown in this dialog:

- *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
- *File with certificate and private Key (PEM or PKCS#12 format):* Enter the path and name of the file containing the certificate in this input field. You can also click Browse to select the file.

Buttons

The following buttons are shown in this dialog:

- View Fingerprint of Certificate: You can check the fingerprint to determine whether an unchanged certificate is available or whether it has been modified.
- Import Certificate from File: The certificate is imported from the file specified in the above input field.

Procedure

To load an SPE certificate, perform the following steps:

1) Select: WBM > *Configuration* > *SPE* > *Import Keycert (STMIX/STMIY - HFA only)*. The Load a SPE Key Certificate via HTTP is displayed. You can edit the following fields:
   - *Passphrase for decryption*: Enter the password used when creating the PEM or PKCS#12 file in this field.
   - *File with certificate and private Key (PEM or PKCS#12 format):* Enter the path and file name of the file containing the certificate data you wish to import. Click *Browse* to open a dialog to search for the file.
2) Click View Fingerprint of Certificate. A window appears showing the fingerprint of the certificate you wish to import:
   a) Check the fingerprint (hexadecimal figure). When the certificate is changed, the fingerprint always changes. Only an unchanged fingerprint guarantees an unchanged certificate. If the two fingerprints are not identical, an attack was probably attempted. In this case, the key should no longer be used and the specified measures should be taken.
   b) Click OK to close the fingerprint window.
3) Click Import Certificate from File if you are satisfied with your examination of the fingerprint. Do not import the certificate if the fingerprint does not satisfy your expectations.

5.4.2 Show Keycert

WBM path

WBM **>** *Configuration* **>** SPE **>** *Show Keycert* **>** *Certificate Information*

The Certificate Information dialog is displayed. In this dialog, you can see the SPE certificate, e. g. to test it.

Displayed data

The following certificate data is displayed:

- General data: *Certificate Name*, *Certificate Type*, *Serial Number of Certificate*, *Serial Number of Certificate (hex)*, *Type of Signature Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organization Unit (OU)*, *Common Name: (CN)*
- *Subject Name*: *Country (C)*, *Organization (O)*, *Organization Unit (OU)*, *Common Name: (CN)*
- *Subject Alternative Name*

Public Key Encryption Data: *Public Key Length*, *Public Key*, *Fingerprint*

5.4.3 Delete Keycert

WBM path

WBM **>** *Configuration* **>** SPE **>** *Delete Keycert* **>** *Remove SPE Certificate*

The *Remove SPE Certificate* dialog is displayed. In this dialog, you can remove the SPE certificate, e. g. if a new certificate is required.

Buttons

The following buttons are shown in this dialog:

- *Delete*: The SPE certificate is removed after a warning appears.
- *Cancel*: The removal procedure is canceled.

Procedure

To remove an SPE certificate, perform the following steps:

1) Select: *WBM* **>** *Configuration* **>** SPE **>** *Delete Keycert***.** A warning is displayed. The name of the certificate is specified for inspection purposes.
2) Click *Delete* and then click *OK* in the confirmation dialog. The SPE certificate will also be deleted for SIP.

5.4.4 SPE CA Certs

WBM path

WBM **>** *Configuration* **>** SPE **>** *SPE CA Certs*

The PEM or binary file sent by the DLS server and generated by a PKI certification authority (RA/CA) or the DLS server's internal certification authority (CA) can contain up to 16 trusted CA certificates in addition to the SPE certificate.

Procedure:

Proceed as follows to import a trusted CA certificate, (see above, *Import Keycert (STMIX/STMIY - HFA only)*)

Display SPE CA Certificate

You can display an SPE CA certificate, for example, if you want to check it.

1) The *Certificate Information* mask is displayed. This displays general certificate data (such as the name, type and serial number), information on the issuer and the subject name as well as encryption data. The public key used and the fingerprint are displayed in hexadecimal format.

View CDP and CLR

With this function you can display the CRL Distribution Point (CDP) of a Certificate Revocation List (CRL).

Already issued certificates can be declared to be invalid, because they have become insecure, for example.

The CDP is an URI or an URL. With this URI / URL you can find a CRL to a certificate (e.g.: ldap://ldapserver.de/cdps/â¦).

5.4.5 SPE Security Setup for HFA

WBM path

WBM **>** *Configuration* **>** SPE **>** *SPE Security Setup for HFA*

The *Edit SPE Security Setup for HFA* dialog is displayed. In this dialog, the security settings for Signaling and Payload Encryption (SPE) can be adapted to the customer's security requirements. This affects the encryption of signaling

and payload data in communication between the STMIX/STMIY - HFA and the VoIP clients, or between two STMIX/STMIY - HFA systems.

Dropdown lists, input fields, check boxes

The following settings are shown in this dialog:

- *Minimum length of the RSA key: The lengths 512, 1024 and 2048 can be selected. The larger this value, the more secure the key.*
- *Maximum Re-Keying interval [hours]:* This value specifies the length of time a specific key should be used for encrypting signaling and payload data. When this time has elapsed, a new key is defined.
- *Enforce Secure Renegotiation (RFC 5746)*: Activate by checkbox.
- *TLS Protocol Version:* You can select TLS 1.3 with fallback to TLS 1.2 (Default), TLS 1.3 only, or TLS 1.2 only.

TLS 1.2 Cipher Selection

- *Key Agreement*: Select with Perfect Forward Secrecy or without.
- *Encryption*: Select AES-128 with fallback to AES-256 or AES-256 only.
- *AES Operation Mode*: Select GCM preferred with fallback to CBC, GCM only, or CBC only.

NOTICE: If ECDSA certificates have been imported for SPE, then the Cipher selection has to ensure that Perfect Forward Secrecy (PFS) ciphers are enabled in the WBM GUI (for SIP or HFA). Otherwise, the TLS handshake of the SIP/HFA clients fails.

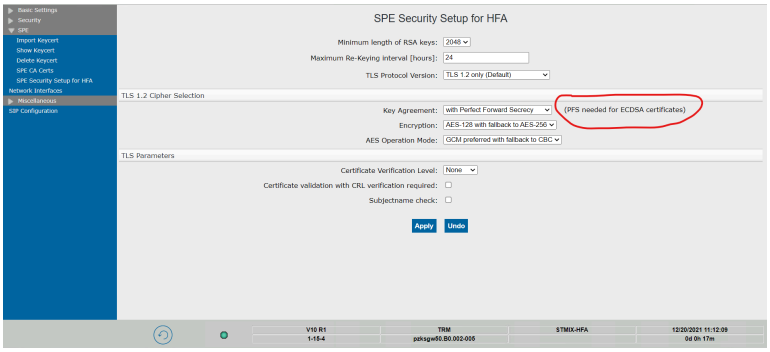


Figure 1: PFS in SPE Security Setup for HFA

TLS Parameters

- *Certificate Verification Level:* None, Trusted or Full
- *Certificate validation with CRL verification required:* Activate/Deactivate
- *Subjectname check:* Activate / Deactivate

Buttons

The following buttons are shown in this dialog:

- *Apply:* Save your entries.
- *Undo:* The entries made are deleted and replaced by default values.

5.5 Network Interfaces

WBM path:

WBM **>** *Configuration* **>** Network Interfaces

With this option, you can configure LAN1 interface details. The function of the first LAN interface is predefined:

You can display detailed information on using the LAN1/LAN2 interface.

- Interface name: LAN1
- Active Interface: eth0
- IP address: Interface IP address
- Subnet mask: Subnet mask
- *IP Address of the Default Router*
- *Link Mode*
- *Link Status*
- *Auto-Negotiation:* On/Off
- Maximum Data Packet Size (Byte): Maximum data packet size in bytes to
- apply to the IP protocol.
- IEEE802.1p/q Tagging: Ethernet format sent from the board.

The LAN2 configuration is done by AMO CGWB by assigning or deleting a Management IP address.

â¢ Use the Second LAN as: Mirror/bond for LAN1 or management LAN.

5.6 Miscellaneous

WBM path

WBM **>** *Configuration* **>** Miscellaneous

The *Miscellaneous* menu opens.

The following options are shown in the menu:

NGS

QoS-Data-Collection

5.6.1 NGS

WBM path

WBM **>** *Configuration* **>** Miscellaneous **>** *NGS* **>** *NGS Settings*

The NextGen Service (NGS) Webservice solution transmits the IPv4 and/or IPv6 addresses as well as all other data required for routing information from the HG 3500 on STMIX/STMIY to the NGS server.

The *NGS Settings* dialog is displayed: Enter the IP address of the NGS server in this dialog.

Input fields

The following input fields are shown in this dialog:

- *IP Address of NGS Server [IPv4 or IPv6]:* The IP address can be entered in the format IPv4 or IPv6. The default format is IPv4: 0.0.0.0.

Buttons

The following buttons are shown in this dialog:

- Apply: The input is saved. HG 3500 on STMIX/STMIY must be restarted to activate the changes.
- Undo: The input is rejected and the default value restored.

5.6.2 QoS-Data-Collection

Quality of Service Data Collection (QDC) - tasks and functions:

The OpenScape IP service "QoS Data Collection" is a tool which collects data on OpenScape products. This data is used to analyze the voice and network quality of the products.

With its range of features, the QoS Data Collection service aims to:

- reduce general expenses for QoS problem analysis
- increase the remote clearance rate
- detect network malfunctions in good time in order to prevent voice quality problems

This results in:

- reduced service outlay
- competitive maintenance contracts
- quick and qualified responses to customer problems
- increased general customer satisfaction with products and technologies
- the possibility to identify changes in the customer network environment and to align the marketing activities of OpenScape services accordingly

By using QDC, key improvements can be achieved in the entire service (break/fix) process.

Background Information on QDC

Please refer to *OpenScape 4000 V8, Gateways HG 3500 and HG 3575, Administrator Documentation.*

WBM path

WBM **>** *Configuration* **>** Miscellaneous **>** QoS-Data-Collection **>** *Quality of Service Data Collection*

Selection and Input Fields

QDC Configuration

- *Send to QCU:* Enable this check box if you want to send data to the QCU. Default value: Check box not activated.
- QCU IP Address: Enter the IP address or the name of the QCU host here. Default value: 0.0.0.0.
- QCU Receiving Port: Receive port for QCU. Enter the port number for the QCU host here. Default value: 12010.

- Send to Network Management enabled: Enable this check box if you want to send data to the Network Management system. Default value: Check box not activated.
- IP Address of Network Management: Enter the IP address or name here. Default value: 0.0.0.0.
- Community String: n/a

IMPORTANT: If one of the check boxes Send to QCU or Send to Network Management enabled is activated (checked), QoS reports will be generated.

QDC Report Mode

- Send Report if: Select the send time for the report from the list box. The following options are available:
- End of session and threshold exceeded: A report will only be sent at the end of a session and only if the threshold is exceeded.
- End of report interval and threshold exceeded: A report will be sent for each report interval once the threshold has been exceeded.
- End of session, unconditional: A report is always sent when the session ends.
- *End of report interval, unconditional:* A report is always sent at the end of a reporting interval.The following fields can be edited:
- *Report Interval (sec):* Enter the interval (in sec.) at which the reports should be sent. A QoS report will be sent for each report interval if the report mode is set correspondingly.Default value: 60 sec.Valid values: 0 ... 65535
- *Observation Period (sec):* This parameter cannot be adjusted. Default value: 10 sec.
- *Minimum Session Length (* 100 msec):* Enter the minimum session length (* 100 msec) here. A QoS report will not be sent if a session (for example, a call) is shorter than the set minimum value. Default value: 20 (2 sec) Valid values: 0 ... 255

IMPORTANT: The time scale is segmented during the observation period and the report interval. Each observation period is checked to monitor if the threshold has been exceeded. A QoS report will be sent for each report interval if the corresponding report mode setting is enabled.

QDC Threshold Values

- Upper Jitter Threshold (msec): In this field, enter the upper threshold value for report generation. The jitter is checked to monitor if this threshold has been exceeded and is measured in the time between two consecutive RTP packets. Default value: 20 msec Valid values: 0 ... 255
- Average Round Trip Delay Threshold (msec): Round trip delay reflects the total runtimes in both directions. , ; In this field, enter a threshold value for the average round trip delay that results in report generation. Default value: 100msec Valid values: 0 ... 65535
- Thresholds Values (for) Compression Codec: In this field, enter the required number of packets for the compression codec thresholds. The following options are available:

- – lost packets (per 1000 packets): In this field, enter a threshold value for the packets lost during voice decoding. This value represents the packet loss in relation to the total number of packets. Default value: 10 Valid values: 0 ... 255
  – consecutive lost packets: In this field, enter a threshold value for consecutive lost packets. The number of consecutive packets lost (uninterrupted by "good" packets) is counted. If the value counted is greater than the value specified, the threshold has been exceeded. Default value: 2 Valid values: 0 ... 255
  – consecutive good packets: In this field, enter a threshold value for consecutive good packets. The number of consecutive "good" packets (uninterrupted by lost packets) is counted. If the value counted is less than the value specified, the threshold has been exceeded. Default value: 8 Valid values: 0 ... 255
- *Thresholds Values (for) Non-Compression Codec:* In this field, enter the required number of packets for the non-compression codec thresholds. The following options are available:
- – *lost packets (per 1000 packets):* For a description see Thresholds Values (for) Compression Codec.
  – *consecutive lost packets:* For a description see Thresholds Values (for) Compression Codec.
  – *consecutive good packets:* For a description see Thresholds Values (for) Compression Codec.

  Description and application of compression and non-compression codecs:

  Table 2: Codecs - Types

Codec	Audio Mode	Application
High quality preferred	Uncompressed voice transmission.	Use uncompressed voice transmission. Suitable for broadband intranet connections.
Low bandwidth preferred	Use compressed voice transmission (preferred).	Suitable for connections with different bandwidths.
Low bandwidth only	Use compressed voice transmission only.	Suitable for connections with low bandwidth.

  Click Apply followed by OK in the confirmation dialog.

Buttons

The following buttons are shown in this dialog:

- Apply: The input is saved. HG 3500 on STMIX/STMIY must be restarted to activate the changes.
- Undo: The input is rejected and reset to the default value

5.7 SIP Functions

WBM path

WBM **>** *Configuration* **>** SIP Functions

See Chapter 6 and Chapter 8 for descriptions of the STMIX/STMIY - SIP/IPDA WBM.

6 SIP/IPDA WBM - Configuration

In this chapter the configuration of the SIP signaling protocol of the STMIX/ STMIY is described.

6.1 Configuration

In this module you will find functions which are required for the configuration of the HG 3500 on STMIX/STMIY.

WBM path:

WBM **>** *Configuration*

The *Configuration* module options are displayed on the left.

Options in the *Configuration* module:

Basic Settings Security Network & Routing Voice Gateway

HFA Functions

6.2 Basic Settings

In this module you will find functions which are required for the configuration of the HG 3500 on STMIX/STMIY. The basic settings of the gateway HG 3500 on STMIX/STMIY include visible hardware data and editable basic data of the gateway functionality.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings*

The tree structure for *Basic Settings* is displayed.

Entries under *Basic Settings*:

System Gateway Quality of Service

6.2.1 System

The "System" folder provides information on the current status or the current configuration of key system components.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** *System* **>** *Gateway Properties*

Single-click the plus sign (+) next to *System* to display the following:

Partnumber

Software Build

The *Gateway Properties* mask is displayed. For more information about the individual fields, see Section 6.2.2, "Gateway".

6.2.1.1 Partnumber

WBM path:

WBM > *Configuration* > *Basic Settings* > *System* > *Partnumber*

The Part Numbers window is displayed. It contains the hardware ID and parts list.

6.2.1.2 Software Build

WBM path:

WBM > *Configuration* > *Basic Settings* > *System* > Software Build > *Software Build Version*

The *Software Build Version* dialog is displayed. The following information is displayed:

Currently active gateway image:

- *Software build version* (precise version of active software)
- *Loadware version*
- *Loadware info*

OpenScape system:

- *OpenScape system version:* Version of OpenScape 4000 system

Third party and Open Source Software

6.2.2 Gateway

This entry displays gateway properties and settings.

WBM path:

WBM > *Configuration* > *Basic Settings* > *Gateway* > *Gateway Properties*

This option allows you to display and edit the gateway properties and settings.

The *Gateway Properties* mask is displayed. You can display and edit the following data:

General:

- *Board Name*: This field contains the name of the system. Enter a character string in this field.
- *Physical Node Number (4K)*: Unique identification number of the OSk4 system. Format: 0-0-0
- *Gateway Location*: This field contains information about the installation site of the HG 3500 on STMIX/STMIY. This information helps service technicians to locate the gateway when the device has to be physically accessed. The value of this field is taken from AMO UCSU and cannot be changed via WBM.
- *Contact Address*: This field contains information about the person to be contacted if problems arise with the gateway. Enter a character string in this field.

- *System Country Code*: The country code is set by the OSk4 system and is configured by AMOs.
- Type G.711 Global Gateway: is configured in AMO and is read-only in WBM. Default is a-law.
- Type G.711 Global Gateway for the LAN Side: Digitalization procedures for Alaw or Î¼-law analog audio signals can be configured in line with the ITU-T recommendation G.711. Default is a-law.
- Supported IP Versions: configured in AMO CGWB and read-only in WBM. Possible values are IPV4 only, IPV4 and IPV6 (dual stack), or IPV6 Only
- *Gateway IP Address*: The gateway's IP address is displayed for information purposes. This entry cannot be modified here.
- *Gateway Subnet Mask*: The gateway's subnet mask is displayed for information purposes. This entry cannot be modified here.

Additional features:

- *Conference Improvement:* During a conference, targeted fallback is performed on the G.711 encoding.
- *Support for Dispatch Application* - only for native SIP trunking GW
- *Allow SIP Register for Trunking*- only for native SIP trunking with profile.
- *Use Early Media for Disconnect to SIP* - only for Native SIP Trunking GW.
- Use instant DMC: DMC (Direct Media Connection) is used to exchange the user data directly between two SIP endpoints in the IP network. Default: yes.
- *Signaling Protocol for IP Networking:* SIP. This setting is configured in AMO and is read-only. Possible values are *SIP*, *H.323*, or *Not configured.*
- *Display Name Character Code Set*: Support for Cyrillic display names. The character coding is configured at the gateway for this purpose based on the input of a character string:
- – Default: Blank string
  – The string is a sequence of the icons {'*', '1', '5', 'R', 'D'}: '*' = default, '1' = ISO8859-1, '5' = ISO-8859-5, 'R' = CorNet-TS (RUSSKYR), 'D' = H4000-GERMAN.

  The coding for the Downstream Subscriber (DS) translation occurs at the first position in the string, following by the coding for the Upstream Subscriber (US) translation, followed by DS/US Trunking and HFAviaSIP-DS/US.

  The default (= '*') is used for unavailable positions in the string (translation points).

  The default is ISO-8859-1 Latin-1 (='1') for DS/US Subscriber and DS/US Trunking and CorNet-TS (='R') for HFAviaSIP.

  If a specific translation is only defined for one of the two twin parameters (-DS and -US) and the other is defined by default, then the corresponding coding is also defined for the other parameter, i.e. assumed as the default.

  The gateway has to be restarted to accept the setting.

  Click *Apply* followed by *OK* in the confirmation dialog. Click *Undo t*o discard the changes entered. Restart the gateway.

6.2.3 Quality of Service

In HG 3500 on STMIX/STMIY, "Quality of Service " is supported by IP packet prioritization. Prioritization is performed on the basis of information in the IP header. For this to work, the relevant transmission partner must use the same "Quality of Service" procedure. You can display and edit this procedure.

In the case of IP data traffic, packets produced by HG 3500 on STMIX/STMIY are split into various groups.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** *Quality of Service*

The *Quality of Service* window is displayed. This option allows you to edit the current gateway settings for quality of service.

You can edit the following data:

- *Priority Class for Signaling Data*:Priority class for the connection setup. Cannot be modified.
- *Priority Class for Fax/Modem Payload (IP Networking only)*:Select the relevant priority class for the fax and modem data of the IP connection.
- The following can be selected:
  - *AF:* Assured Forwarding (under fixed conditions). Data traffic is assigned classes and intercept priorities. This means that data forwarding can be assured as long as a certain data volume is not exceeded. If the data volume threshold is exceeded, data packets are intercepted according to their intercept priorities.
    - *AF11, AF12, AF13:* Class 1 data volume with intercept priorities low (AF11), medium(AF12) and high (AF13)
    - *AF21, AF22, AF23:* Class 2 data volume with intercept priorities low (AF21), medium(AF22) and high (AF23)
    - *AF31, AF32, AF33:* Class 3 data volume with intercept priorities low (AF31), medium(AF32) and high (AF33)
    - *AF41, AF42, AF43:* Class 4 data volume with intercept priorities low (AF41), medium(AF42) and high (AF43)
  - *EF:* Expedited Forwarding. Aimed at data traffic that is only permitted to have low loss and low latency.
  - *Best effort / DF:* This priority is designed for typical router behavior.
  - *CS1, CS2, CS3, CS4, CS5, CS6, CS7:* Class Selector. This prioritization is used for Network Control Packets (e.g. SNMP).
  - *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; used to prioritize IP packets.
- *Priority Class for Network Control*: Priority class for network control data, such as SNMP trap transmission). Cannot be modified.
- *Priority Class for Voice Payload*:Priority class for voice data on the IP connection.

Click *Apply* followed by *OK* in the confirmation mask. Click *Undo t*o discard the changes entered.

IMPORTANT: The default values do not usually need to be modified.

6.2.4 Timezone Settings

WBM path:

WBM **>** *Configuration* **>**

NOTICE: The timezone setting is sent via the OpenScape system and cannot be changed via WBM.

6.3 Statistics

Statistics can be used to monitor the gateway performance and status.

The call statistics provide statistical information on voice, TSC, DMC, and data calls.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** *Statistics*

Statistics can be used to monitor the gateway performance and status.

Single-click the plus sign (+) next to *Statistics* to display the following entries:

Entries under *Statistics*:

Call Statistics

6.3.1 Call Statistics

Single-click the plus sign (+) next to *Call Statistics* to display the following entries:

1) *Delete Statistics*

Call Statistics (1 h) Call Statistics (24 h) Call Statistics (Total) Call Statistics (Maximum Parallel) LAN Call Statistics PBX Call Statistics Current Connections

6.3.1.1 Delete Statistics

Deletes all statistics (apart from the counters from the last reboot).

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** Statistics **>** Call Statistics **>** *Delete Statistics*

The *Delete Statistics* mask is displayed. Click *Delete* to reset the counters. Click *Cancel to* exit the dialog without making any changes.

6.3.1.2 Call Statistics (1 h)

These statistics list the totals for voice, TSC, DMC, and data calls during the last hour.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** *Statistics* **>** Call Statistics **>** *Call Statistics (Last Hour)*

You can view the totals for voice, TSC, DMC and data calls during the last hour.

The *Call Statistics (Last Hour)* mask is displayed. The totals displayed can be split into four categories:

- Voice calls
- TSC calls (**T**emporary **S**ignaling **C**all)
- DMC calls (**D**irect **M**edia **C**onnection)
- Data calls

via LAN or PBX. In all four categories, the display indicates

- the number of successful connections (*... Connected*) and
- the number of calls successfully accepted (*... Received*).

In addition, the total duration of all connections is displayed in seconds.

6.3.1.3 Call Statistics (24 h)

These statistics list the totals for voice, TSC, DMC, and data calls during the last 24 hours.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** *Call Statistics* **>** *Call Statistics (Last 24 Hours)*

You can view the totals for voice, TSC, DMC, and data calls for the LAN and PBX during the last 24 hours.

The *Call Statistics (Last 24 Hours)* mask is displayed. For a brief description of the data, see Section 6.3.1.2, "Call Statistics (1 h)".

6.3.1.4 Call Statistics (Total)

These statistics list the totals for voice, TSC, DMC, and data calls for the LAN and PBX since the last reboot.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** Statistics **>** *Call Statistics* **>** *Call Statistics (Total)* **>** *Call Statistics (Total since last reboot)*

You can view the totals for voice, TSC, DMC, and data calls for the LAN and PBX since the last reboot.

The *Call Statistics (Total)* mask is displayed. For a brief description of the data, see Section 6.3.1.2, "Call Statistics (1 h)".

6.3.1.5 Call Statistics (Maximum Parallel)

These statistics list the totals for voice, TSC, DMC, and data calls for the LAN and PBX processed simultaneously by the gateway during peak load.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** Statistics **>** *Call Statistics* **>** *Call Statistics (Maximum Parallel)* **>** *Call Statistics (Maximum concurring events since last reboot)*

These statistics list the totals for voice, TSC, DMC, and data calls for the LAN and PBX processed simultaneously by the gateway during peak load.

The *Call Statistics (Maximum Parallel)* mask is displayed. For a brief description of the data, see Section 6.3.1.2, "Call Statistics (1 h)".

6.3.1.6 LAN Call Statistics

LAN calls are connections with other OpenScape 4000 V10 nodes (IP trunking) and VCAPI.

These statistics list the voice, TSC, DMC, and data calls received via LAN during the last hour, the last 24 hours, since the last reboot, and all calls processed by the gateway during peak load.

WBM path:

WBM **>** *Configuration* **>***Basic Settings* **>** Statistics **>** *Call Statistics* **>** *LAN Call Statistics* **>** *LAN Call Statistics Initiated*

The *LAN Call Statistics Initiated* mask is displayed.

The totals displayed can be split into four categories: one for the past hour, one for the past 24 hours, one for all calls received since the last reboot, and one for calls assigned the property "Maximum Parallel." The number of successful connections (*... Connected*) and the number of calls successfully accepted (*... Received*) are displayed for all categories. In addition, the total duration of all connections is displayed in seconds. All figures apply exclusively to connections conducted over LAN.

6.3.1.7 PBX Call Statistics

PBX calls are calls with system clients.

These statistics list the voice, TSC, DMC, and data calls routed via PBX during the last hour, the last 24 hours, since the last reboot, and all calls processed by the gateway during peak load.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** Statistics **>** *Call Statistics* **>** *PBX Call Statistics* **>** *PBX Call Statistics Initiated*

You can view the total number of voice, TSC, DMC, and data calls routed via PBX during the last hour, the last 24 hours, since the last reboot, and all calls processed by the gateway during peak load.

The *PBX Call Statistics Initiated* mask is displayed. For a brief description of the data, see Section 6.3.1.6, "LAN Call Statistics". All figures from these statistics, however, apply exclusively to connections conducted over PBX.

6.3.1.8 Current Connections

Number of currently connected and attempted calls without distinction between call type or origin.

WBM path:

WBM **>** *Configuration* **>** *Basic Settings* **>** Statistics **>** *Call Statistics* **>** *Current Connections*

You can view the number of currently connected and attempted calls.

The *Current Connections* mask is displayed. The total displayed is the result of the number of currently connected and attempted calls without distinction between call type or origin.

6.4 Security

Filters belong to the security-relevant authorizations of the HG 3500/3575 for accessing devices or connections and the access management of the Gateway administration.

WBM path:

WBM > *Configuration* > *Security*

The *Security* tree structure is displayed.

Entries under *Security* tree structure:

User Accounts Signaling and Payload Encryption (SPE)

TLS Ciphers for SIP

6.4.1 User Accounts

All user accounts defined with the AMO CGWB are displayed in a table.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *User Accounts*

The *User Accounts* mask is displayed. The table indicates the *Name* and the *Authorization* for each user account.

User Accounts are displayed as a list. Single-clicking *User Accounts* opens a tree structure where you can view the user accounts configured. *Name* and *Authorization* are displayed for the relevant user account.

Name

Name of the user account

Authorization

Authorization for the user account

6.4.2 Signaling and Payload Encryption (SPE)

The Signaling and Payload Encryption (SPE) function encrypts VoIP user and signaling data streams to and from the gateway. For this feature a PKI (Public Key Infrastructure) is needed.

The needed certificates are generated either by a customer PKI certification authority (RA/CA) or the internal certification authority of the DLS server (CA). The DLS server then sends the files containing these certificates to the DLS client of the gateway.

Depending on the customer's requirements, security settings can be configured, activated or deactivated for certificate evaluation and signaling and payload encryption. This increases or decreases the security.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)*

Single-click the plus sign (+) next to *Signaling and Payload Encryption (SPE)* to display the following entries:

SPE Security Setup for SIP

SPE Certificate SPE CA Certificate(s)

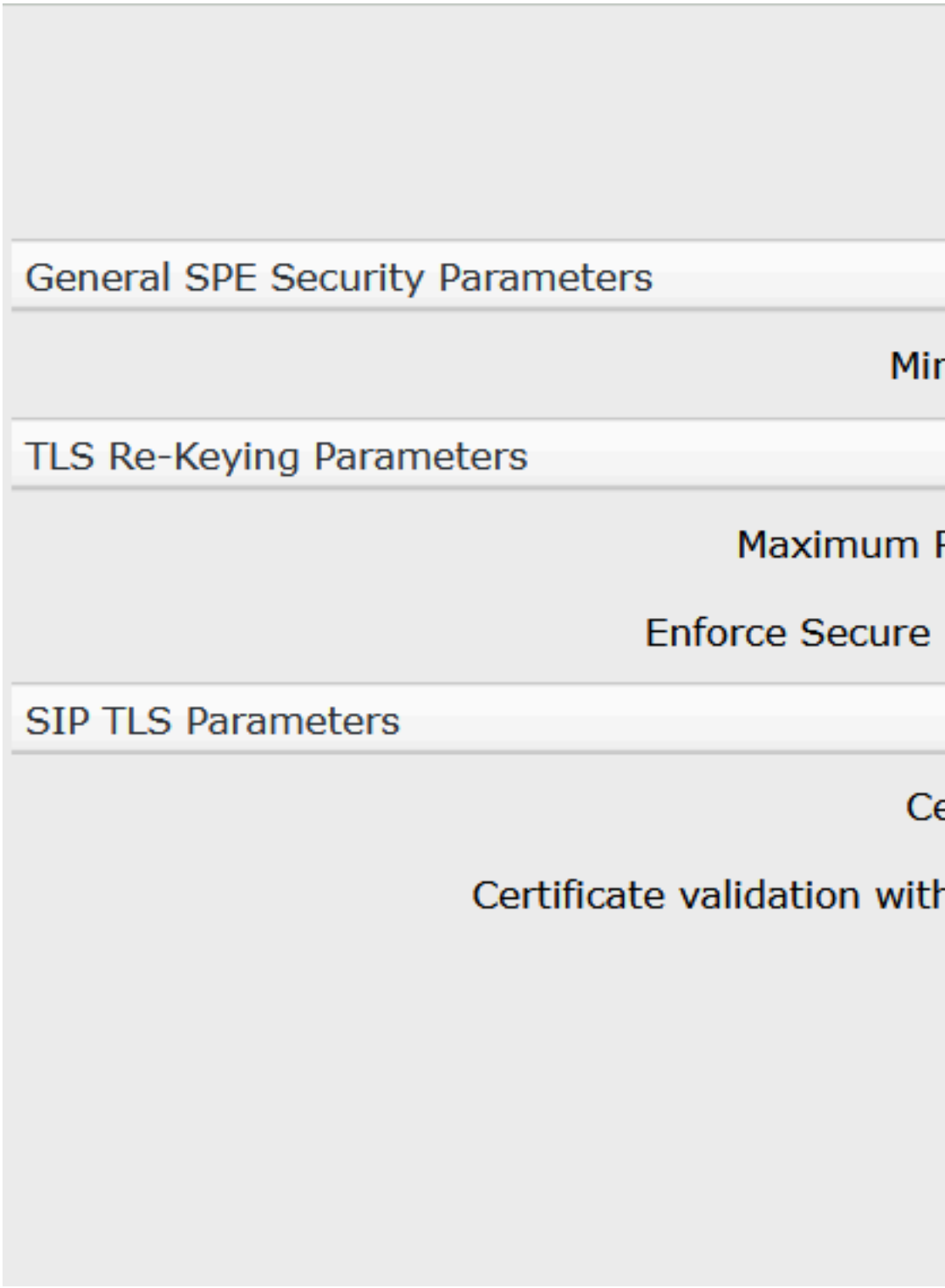
6.4.2.1 SPE Security Setup for SIP

The *SPE Security Setup* mask shows the security settings for Signaling and Payload Encryption (SPE), for the encryption of signaling and payload between the gateways and VoIP clients as well as between two gateways.

Procedure:

Proceed as follows to display the SPE security configuration:

1) Select: *WBM* **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup.* The *Edit SPE Security Setup* dialog is displayed containing the following data:



Minimum Length of RSA Keys

Define the minimum length of RSA key in the certificate received from the remote entity. The greater the value, the more secure the key.

The minimum length of RSA keys set in the WBM:

- 512 bits

The maximum length:

- 2048 bits

WBM path:

WBM > *Configuration* > *Security* > *Signaling and Payload Encryption (SPE)* > *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>** Minimum Length of RSA Keys

Maximum Re-Keying Interval

The TLS/SSL connections remain permanently active and are renewed at regular intervals. The time interval for renegotiation is set in the WBM:

- Maximum value 167 hours
- Minimum 6 hours
- Disabled 0 (NOT RECOMMENDED)

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>** *TLS Re-Keying Parameters* > *Maximum Re-Keying Interval [hours]*

Enforce Secure Renegotiation (RFC 5746)

TLS is vulnerable to situations where a malicious server establishes a connection to a target server, injects it with its own rogue data and then splices in the new TLS connection from a client. The target server treats the client's initial TLS handshake as a renegotiation of an existing connection that the malicious server has previously established and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. This problem can be avoided with secure renegotiation based on RFC 5746.

Only if all remote entities, which are connected over TLS, support secure renegotiation (RFC 5746), enable this feature. If a remote entity does not support RFC the renegotiation fails, even the establishment of the TLS connection fails in some scenarios.

This behavior can be changed by checkbox:

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>***TLS Re-Keying Parameters* **>** *Enforce Secure Renegotiation (RFC 5746)*

Certificate Verification Level

During session setup of TLS (Transport Layer Security) the product needs to check the presented identity (certificate) of the opposite side of the communication channel. This checking needs to be done on client side of the TLS session regarding the identity of the server side or on both the client and server side if MTLS (Mutual TLS) is being used.

IMPORTANT: If on the TLS server side Trusted or Full is configured, the certificate from the TLS client is requested (Mutual TLS). If on the gateway subscribers are configured, but do not have a certificate, then select on the gateway (which is on

this interface TLS server) as Certificate Verification Level None, the client is not allowed to choose the verification level. SPE can only be enabled or disabled (the server certificate is either selected or unselected).

IMPORTANT: For SIP-Q trunks the Certificate Verification Level None is not allowed, because Mutual TLS is mandatory.

IMPORTANT: If for native SIP trunks the gateway has a certificate the Certificate Verification Level should not be None in order to check the received certificate.

IMPORTANT: For all SIP interfaces on a gateway the Certificate Verification Level is the same. Thus it is not possible to have on one gateway SIP-Q trunking and SIP subscribers without certificates configured.

For the certificate verification three different levels are defined which can be selected:

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>** SIP TLS Parameters

- None - no authentication of the remote entity performed
- The certificate of remote entity is not requested and not checked.
- Trusted - the certificate (including certificate chain) provided by the remote entity is requested and checked for integrity
- This means that the chain of trust for the digital signature provided by the remote entity ends up in one of the (root) CA-certificates, which are preconfigured for that interface on the product. And that all certificates in the chain are not expired (i.e. current date/time is within the certificate's given validity period).
- Full - the certificate (including certificate chain) provided by the remote entity is requested and checked against the same criteria as in Trusted mode, plus: the correct use of all extensions is checked. If an extension is marked critical and is not recognized, the certificate must be rejected. And the correct use of known extensions is checked (e.g. Basic constraints, Key Usage, Extended Key Usage).
- Subject name check: The end entity's identity is verified by its alternate name or common name. This behavior can be changed by checkbox.
- There are optional checks:

  In level Trusted and Full:
- Certification validation with CRL verification required:
- The certificate revocation list (CRL) is used to specify whether and why a certificate should be blocked/revoked. If a certificate or certification authority (CA) declares a certificate invalid, it enters the certificate's serial number in

its list. This list can be downloaded from the certification authority's Internet site for certificate inspection.

Check that none certificate in the chain is revoked. This behavior can be changed by checkbox:

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>** SIP TLS Parameters **>** Certification validation with CRL verification required.

In level Full:

- Subject name check: The end entity's identity is verified by its alternate name or common name. This behavior can be changed by checkbox:

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Security Setup for SIP* **>** *Edit SPE Security Setup* **>** SIP TLS Parameters **>** Subject name check.

6.4.2.2 SPE Certificate

This folder contains the SPE client certificate with the private key and is empty by default. The certificate must first be imported. You can view the imported certificate as required. The file containing the certificate must be available in PEM or PKCS#12 format. This file originates in a customer PKI certification authority (RA/CA) or the DLS server's internal certification authority (CA).

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Certificate*

***SPE Certificate* folder:**

Import SPE certificate plus private key (PEM or PKCS#12)

Import SPE certificate plus private key (PEM or PKCS#12)

A PEM or PKCS#12 file contains the data for a certificate and the associated private key. You can import the relevant PEM or PKCS#12 file to use this certificate.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Certificate* **>** *Import SPE certificate plus private key (PEM or PKCS#12)* **>** *Load SPE Key Certificate via HTTP*

Procedure:

NOTICE: You can import certificates via the STMIX/STMIY-HFA WBM, see Section 5.4.1, "Import Keycert (STMIX/STMIY - HFA only)".

Show SPE Certificate

You can display an SPE certificate, for example, if you want to check it.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Certificate* **>** *(left-click) SPE Certificate*

Procedure:

1) Select: *WBM* **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE Certificate* **>** *SPE Certificate* **>** *(left-click) SPE Certificate*. The *Certificate Information* mask is displayed. This displays general certificate data (such as the name, type and serial number), information on the issuer and the subject name as well as encryption data. The public key used and the fingerprint are displayed in hexadecimal format.

2) Click *OK*. The mask is closed.

6.4.2.3 SPE CA Certificate(s)

This folder contains trusted SPE CA certificates.

STMIX/STMIY-SIP/IPDA supports multi-level CA certificate hierarchies. You can therefore also import multi-level CA certificate hierarchies. Upon receipt of a certificate chain from a TLS partner the entire received certificate chain will now be verified.

When using multi-level certificate hierarchies you need to

1) Import into the "SPE CA Certificates" folder the CA certificates of all intermediate certification authorities of the hierarchy of the own SPE certificate. Optionally, you may import the certificate of the Root Certification Authority (RootCA). When establishing the TLS connection the own certificate is then sent together with the chain of CA certificates.

In addition, you need to import into the "SPE CA Certificates" folder the CA certificates of all the Root Certificate Authorities that shall be considered as "trusted". During verification of a received certificate chain the Root CA certificates in the "SPE CA Certificates" folder are used.

The import sequence of certificates is arbitrary.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)*

Single-click the plus sign (+) next to *SPE CA Certificate(s)* folder to display the following:

1) Import Trusted CA Certificate (PEM or Binary)

Import trusted CA Certificate (PEM or Binary)

The PEM or binary file sent by the DLS server and generated by a PKI certification authority (RA/CA) or the DLS server's internal certification authority (CA) can contain up to 16 trusted CA certificates in addition to the SPE certificate.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)* **>** *Import trusted CA Certificate (PEM or Binary)*

Procedure:

NOTICE: You can import certificates via the STMIX/STMIY-HFA WBM, see Section 5.4.1, "Import Keycert (STMIX/STMIY - HFA only)".

Single-click SPE CA Certificate to display.

Display SPE CA Certificate

You can display an SPE CA certificate, for example, if you want to check it.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)* **>** SPE CA Certificate(s) **>** *(left-click) SPE CA Certificate*

Procedure:

1) Select: *WBM* **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)* **>** SPE CA Certificate(s) **>** *Show SPE CA Certificate*. The *Certificate Information* mask is displayed. This displays general certificate data (such as the name, type and serial number), information on the issuer and the subject name as well as encryption data. The public key used and the fingerprint are displayed in hexadecimal format.
2) Click *OK*. The mask is closed.

Show CDP and CRL

With this function you can display the CRL Distribution Point (CDP) of a Certificate Revocation List (CRL).

Already issued certificates can be declared to be invalid, because they have become insecure, for example.

The CDP is an URI or an URL. With this URI / URL you can find a CRL to a certificate (e.g.: ldap://ldapserver.de/cdps/â¦).

WBM path:

WBM **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)* **>** SPE CA certificate **>** *Certificate Information*

Procedure:

1) Select: *WBM* **>** *Configuration* **>** *Security* **>** *Signaling and Payload Encryption (SPE)* **>** *SPE CA Certificate(s)* **>** SPE CA certificate **>** *Certificate Information*. The *Certificate Information* mask is displayed. This displays general certificate data (such as the name, type and serial number), information on the issuer and the subject name as well as encryption data. The public key used and the fingerprint are displayed in hexadecimal format.
2) Click *OK*. The mask is closed.

6.4.3 TLS Ciphers for SIP

Protocols TLSv1.0 and higher are supported, SSLv2 and SSLv3 are not permitted due to security issues.

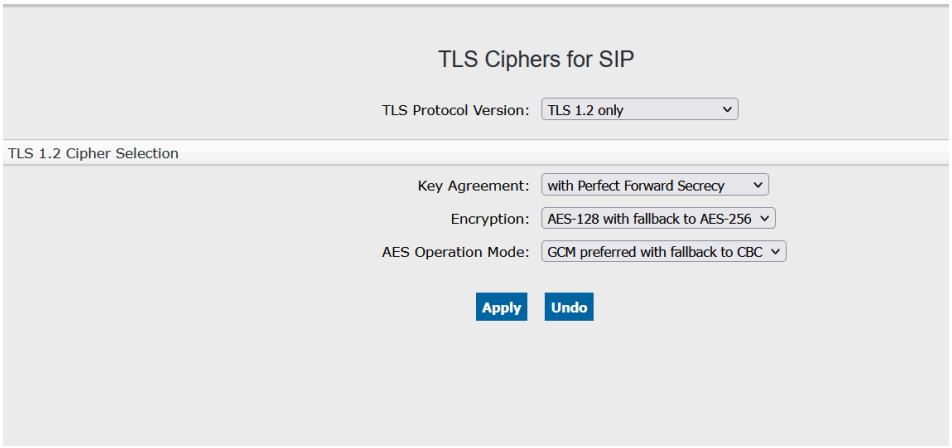
The TLS version can be configured in WBM menu.

WBM path:

WBM **>** *Configuration* **>** *Security* **>** TLS Ciphers for SIP

The TLS version, and for TLSv1.2 also the key agreement method, encryption algorithm and AES operation mode can be configured. (see https://www.ietf.org/rfc/rfc5246.txt for more information about TLSv1.2).

IMPORTANT: After changing and saving TLS settings, the gateway must be rebooted for the changes to take effect.



6.5 Network & Routing

The gateway has two LAN interfaces. Both interfaces can be configured independently.

With HG 3500 on STMIX/STMIY, the second LAN interface is deactivated by default.

If you want to use the second LAN interface, you have to activate the function and define the operating mode in which the interface should work.

WBM path:

WBM > *Configuration* > *Network & Routing*

The *Network & Routing* tree structure is displayed:

1) *Routing*

6.6 Routing

In small networks, a routing table can be set up manually on every router by the network administrator. In larger networks, this task is automated with the help of a protocol that distributes routing information in the network.

An IP packet can transit many routers before it reaches its destination. The route it takes is not defined centrally, but by the routing tables in the individual routers along the way. Each router only establishes the next step on the path and relies on the next router to forward the packet correctly.

Configurable in the HG 3500 on STMIX/STMIY are IP routing, IP mapping, NAT, PSTN routing and SCN routing.

WBM path:

WBM **>** *Configuration* **>** *Network & Routing* **>** *Routing*

The *Routing* tree structure is displayed.

Entries under *Routing*:

IP Routing

Dialing Parameters

6.6.1 IP Routing

Diagnostic and monitoring tools are also available for routing.

WBM path:

WBM **>** *Configuration* **>** *Network & Routing* **>** *Routing* **>** *IP Routing*

The following entries are listed:

Static Routes Default Router DNS Server ICMP Request

6.6.2 Static Routes

Allows users to **Add/Edit(Change)/Delete** Static Routes for both STMIX and STMIY boards from the WBM page. Static routes connect two devices with each other. They are created manually.

The page also represents the Static Route Table, where the following parameters are set :

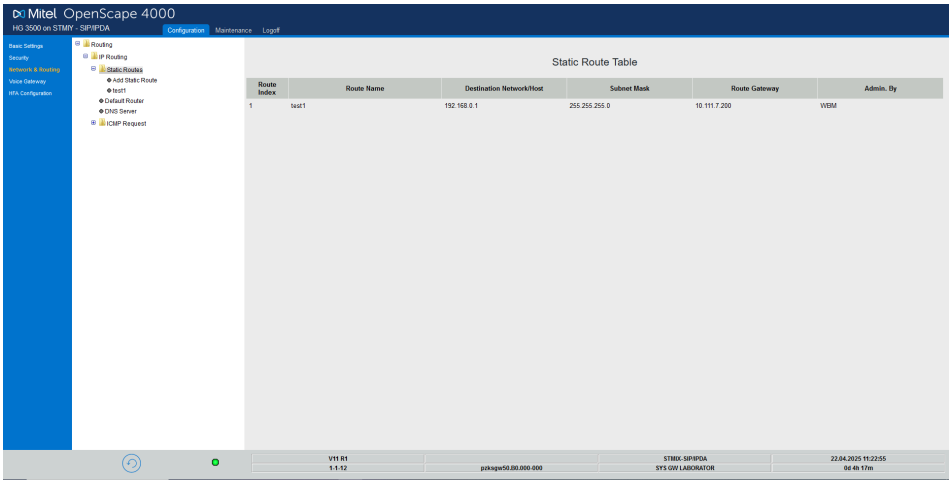
- **Route Index**
- **Route Name**
- **Destination Network/Host**
- **Subnet Mask**
- **Route Gateway**
- **Admin. By**

WBM path:

*WBM***>** *Configuration***>** *Network & Routing***>** *Routing***>** *IP Routing* **>** *Static Routes*

The following entries are listed:

- Add Static Route



6.6.2.1 Add Static Route

You can create a new static route between two IP devices.

WBM path:

WBM> *Configuration*> *Network & Routing*> *Routing*> *IP Routing* > *Static Routes*> *Add Static Routes*

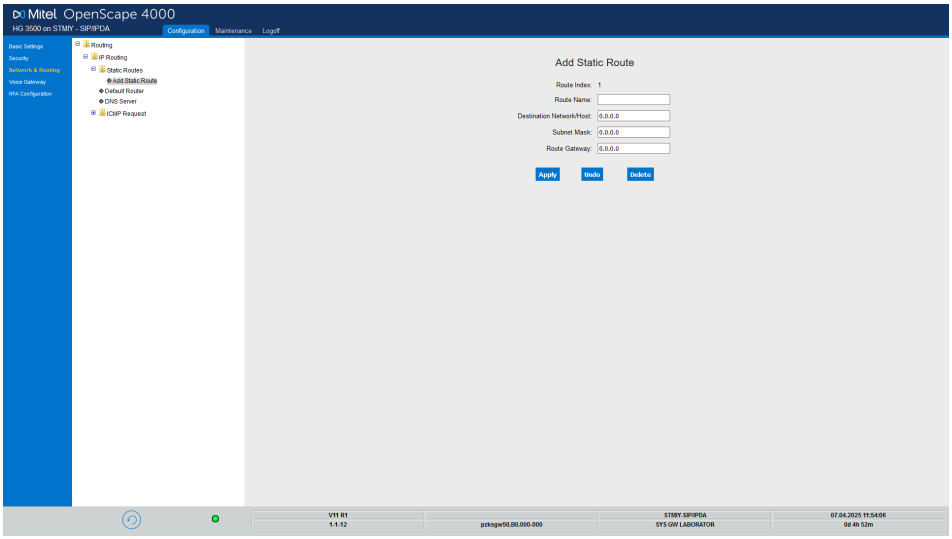
The **Add Static Route** mask is displayed. The serial number of the route is shown under *Route Index*. You can edit the following fields:

- **Route Name**: The name of the static route. Enter a character string.
- **Destination Network/Host**: The IP address of the destination network.
- **Subnet Mask**: The subnet mask of the destination network.
- **Route Gateway**: The IP address of the next router on this route or the IP address of the local or remote interface of a PSTN peer.

The route index is automatically assigned and only displayed for information purposes. It cannot be modified.

When all settings are complete, click *Apply* followed by *OK* in the confirmation mask. Changes will automatically be saved.

You can delete existing static routes. The data associated with the static route to be deleted is displayed for verification purposes.



6.6.3 Default Router

To ensure that the gateway reaches destinations that are not explicitly listed in the route table, a gateway must be specified for forwarding packets of this kind (Default Router).

WBM path:

WBM > *Configuration* > *Network & Routing* > *Routing* > *IP Routing* > *Default Router*

You can view the current default router settings.

The *Default Router* mask appears The current default router settings are displayed:

- *Default Routing via:* Displays via which network, for example LAN, the default router is reachable.
- *IP Address of Default Router:* The IP address of the default router is displayed.

6.6.4 DNS Server

You can view the IP addresses for the preferred and alternative DNS server (Domain Name System). DNS servers are used for name resolution, i. e. to transform alphanumeric IP addresses into numeric IPv4 or IPv6 addresses that can be processed by a computer.

WBM path:

WBM > *Configuration* > Routing > IP Routing > DNS Server > *DNS Settings*

The *DNS Settings* appears. The *DNS Server* addresses are configured in AMO CGWB.

- *IP Address of primary DNS Server:* This shows the IP address of the preferred DNS server.

- *IP Address of secondary DNS Server:* This shows the IP address of the alternative DNS server.

6.6.4.1 ICMP Request

For verification purposes, you can execute ping and traceroute commands to check the routing function.

WBM path:

WBM > *Configuration* > Routing > IP Routing > *ICMP Request*

Single-click the plus sign (+) next to *ICMP Request* to display the following entries in the tree structure:

1) *Ping Traceroute*

6.6.4.2 Ping

You can execute ping command for verification purposes to check the routing function between the HG 3500 on STMIX/STMIY and a random destination address.

WBM path:

WBM **>** *Configuration* **>** *Network & Routing* **>** *Routing* **>** *IP Routing* **>** *ICMP Request* **>** *Ping*

Network connection between STMIX/STMIY-SIP and the destination address of the host being tested is checked. To do this, an ICMP "Echo Request" packet is sent to the destination address. The recipient must return the ICMP "Echo Reply" packet if they support the protocol. This response packet is displayed, together with the round trip delay.

The *Ping* mask is displayed.You can edit the following fields:

- *Destination Address*: Address to which a request is to be sent with a ping.
- *Number of Echo Requests to Send*: Specify how many packet requests should be exchanged. The usual values are 3 or 4.

Click *Send* or *Send (in a separate window)*.

The result of the ping request is displayed.

The following buttons are provided in the output area: *Smaller* reduces the font size in the output. *Bigger* increases the font size in the output. *Reload* repeats the ping request.

6.6.4.3 Traceroute

For verification purposes, you can execute traceroute commands to check the routing function. The traceroute tests the network connection between HG 3500 on STMIX/STMIY and the destination address using ICMP "Echo Request" packets. ICMP Echo Request Packets are sent with incremental TTL (Time-To-Live) values. The response receipts are displayed, together with the round trip delay.

WBM path:

WBM > *Configuration* > *Network & Routing* > *Routing* > *IP Routing* > *ICMP Request* > *Traceroute*

You can start the Traceroute command to test the routing function.

The *Traceroute* mask is displayed. You can edit the following fields:

- *Destination Address*: Enter the IP address of the destination. The traceroute between the STMIX/STMIY/SIP and this destination address is determined.
- *TOS Byte*: Specify whether TOS bytes (TOS = Type of Service) are to be sent. TOS bytes provide information on the quality of a service.

Click *Send* or *Send (in a separate window)*.

The result of the traceroute request is displayed.

The following buttons are provided in the output area: *Smaller* reduces the font size in the output. *Bigger* increases the font size in the output. *Reload* repeats the traceroute request.

6.6.5 Dialing Parameters

The extension numbers configured as S0 stations in OpenScape 4000 V10 using OpenScape 4000 Manager can be assigned a VCAPI client, the MSN/DID number of a PSTN peer or the router call number in HG 3500/3575. The dialing parameters can be configured via WBM. Configured subscribers and IP addresses can also be viewed.

WBM path:

WBM > *Configuration* > *Network & Routing* > *Routing* > *Dialing Parameters*

Single-click the plus sign (+) next to *Dialing Parameters* to display the following entries:

Edit General Dialing Parameters

Configured Subscribers Configured IP Addresses

6.6.5.1 Edit General Dialing Parameters

You can display or edit the basic settings. Configuration is optional.

WBM path:

WBM > *Configuration* > *Network & Routing* > *Routing* > *Dialing Parameters* > *Edit General Dialing Parameters*

The *General Dialing Parameters* mask is displayed. You can edit the following fields:

- *Confirm CLIR*:This is a security function. Select this checkbox to prevent a caller number marked as private from being forwarded to the LAN. The background to this option is that the CLIR functionality is not explicitly defined for IP routing in LANs because the terminal interface to the public network does not match the type found in classic telephony.

E.164

- *International Prefix*: The prefix for international numbers (including the trunk access digit).
- *National Prefix*: The prefix for national calls (including the trunk access digit).
- *Subscriber Prefix*: The trunk access digit or the prefix for calls to the public telephone network.
- *Country Code*: The country ID for the location of HG 3500 on STMIX/STMIY.
- *Area Code*: The area code for the location of HG 3500 on STMIX/STMIY.
- *Location Code*: The location code for HG 3500/3575 (if available).

Example:

In OpenScape 4000 V10, 0 is configured as the trunk access digit. The system is located in Munich and its connection number is 722:

International prefix= 000	Country code = 49
National prefix = 00	Area code = 89
Subscriber prefix = 0	Location code = 722

In HG 3500/3575, station number analysis is performed exclusively on the basis of the dialing parameters configured here and independent of any other corresponding OpenScape 4000 V10 parameters. You must ensure that the numbering scheme used for HG 3500/3575 is set up in accordance with the relevant configuration in OpenScape 4000 V10. Based on the above example, this means: If OpenScape 4000 V10 signals HG 3500/3575 using the implicit station number format with exchange code 0, the prefix for trunk access must also be set to 0 in the dialing parameters. In the example, the national prefix is set to 00 and the international prefix is 000. In both cases, the first 0 stands for the trunk access code.

Private numbering plan

- *Level 0 prefix*: Subscriber prefix
- *Level 1 prefix*: National prefix
- *Level 2 prefix*: International prefix
- *Level 0 code*: Location code
- *Level 1 code*: Area code
- *Level 2 code*: Country code

Click *Apply* followed by *OK* in the confirmation mask.

6.6.5.2 Configured Subscribers

These are configured S0 subscribers.

WBM path:

WBM **>** *Configuration* **>** *Network & Routing* **>** *Routing* **>** *Dialing Parameters* **>** *Configured Subscribers*

You can display a list of configured subscribers.

The *Configured Subscribers* mask is displayed. The station numbers and subscriber types are listed in a table. Subscriber types are, for example, HFA system clients or PSTN peers.

6.6.5.3 Configured IP Addresses

These addresses are the IP addresses of, for example, the LAN interfaces, the individual subscribers or the PSTN peers.

WBM path:

WBM **>** *Configuration* **>** *Network & Routing* **>** *Routing* **>** *Dialing Parameters* **>** *Configured IP Addresses*

You can display a list of the relevant IP addresses.

The *Configured IP Addresses* mask is displayed. The IP addresses and subscriber types are listed in a table. Subscriber types are, for example, LAN interfaces or PSTN peers.

The entries can be sorted. An arrow after a column name indicates the sort criterion. If you wish to sort the table by another column, click the respective column name.

6.7 Voice Gateway

By supporting Voice over IP (VoIP), STMIX/STMIY-SIP/IPDA facilitates the use of OpenScape 4000 V10 features via IP networks.

WBM path:

WBM > *Configuration* > *Voice Gateway*

The *Voice Gateway* tree structure is displayed.

Entries under *Voice Gateway*:

1) H.323 Parameters SIP Parameters (not for HG3575) Codec Parameters IP Networking Mode SIP Trunk Profile Parameter (not for HG3575)

SIP Trunk Profiles

Hunt Group

Destination Codec ParametersDARs for MLPP *Clients ISDN Classmarks*

6.7.1 H.323 Parameters

This option allows you to view and configure settings for the H.323 protocol for voice transmission via the IP network.

WBM path:

WBM **>** *Configuration* **>** *Voice Gateway* **>** *H.323 Stack Parameters*

The *H.323 Stack Parameters* mask is displayed.

You can edit the following fields:

- *Basic User Input String for Outband Signaling* This field activates and deactivates the function for "Outband Signaling (postdialing)" with H.245 user inband "String for Outbound" signaling.

- *User Input for DTMF Outband Signaling*: This field activates and deactivates the function for "Outband Signaling (postdialing)" with H.245 user inband "DTMF Outbound" signaling.

Click *Apply* followed by *OK* in the confirmation mask.

6.7.2 SIP Parameters (not for HG3575)

This option allows you to view and in some cases set SIP parameters for the IP network.

WBM path:

WBM **>** *Configuration* **>** *Voice Gateway* **>** *SIP Parameters*

The *SIP Parameters* window is displayed. You can display the following fields:

SIP User Agent

- *Use SIP Registrar*: The SIP registrar is a server in an SIP (**S**ession **I**nitiation **P**rotocol) network that accepts and processes SIP REGISTER requests. To be reachable, each SIP subscriber must log in to an SIP registrar. Possible displays: Yes/No
- *SIP Registrar IP Address*: IP address of the SIP registrar.
- *SIP Registrar TLS Port Number*: Number of the TLS port on the SIP registrar. TLS (**T**ransport **L**ayer **S**ecurity) is a protocol for encrypting data transmissions via Internet.
- *SIP Registrar TCP/UDP Port Number*: Number of the TCP/UDP port on the SIP registrar. TCP (**T**ransmission **C**ontrol **P**rotocol) and UDP (**U**ser **D**atagram **P**rotocol) are protocols for IP communication.
- *Alternative SIP Registrar IP Address*: IP address of the second SIP registrar, which should be used when the first SIP registrar is unavailable.
- *Alternative SIP Registrar TLS Port Number*: Number of the TLS port on the second SIP registrar.
- *Alternative SIP Registrar TCP/UDP Port Number*: Number of the TCP/UDP port on the second SIP registrar.
- *Period of registration (sec)*: When this registration period has elapsed, SIP subscribers must re-register.

SIP Server (Registrar / Redirect)

- *SIP Server IP Address*: IP address of the SIP server.
- *SIP Server TCP/UDP Port Number*: Number of the TCP/UDP Port on the SIP server.
- *SIP Server TLS Port Number*: Port number of the SIP server for TLS.
- *Default Registration Period (sec):* 600 (used when no âExpires' value received)
- *Range used for Randomized Registration (%)*: 25 (0 means: don't use Randomization).

RFC 3261 Timer Values

Transaction Timeout (msec): The SIP Timer is defined in RFC 3261.

SIP Transport Protocol

- *SIP via TCP*: (Abbreviation for **T**ransmission **C**ontrol **P**rotocol). Alongside IP, this is the most important Internet protocol. It provides a connection-based, reliable, full-duplex service in the form of a data channel.
- *SIP via UDP*: (Abbreviation for **U**ser **D**atagram **P**rotocol). This protocol can be used as an alternative to TCP if reliability is not important. UDP does not guarantee packet delivery or a specific sequence of receipt.
- *SIP via TLS*: (Abbreviation for Transport Layer - Security). TLS is a hybrid encryption protocol on the Internet and successor to SSL (Secure Socket Layer).

SIP Session Timer:

- *RFC 4028 support*: In RFC 4028, sessions timers are defined as an extension of SIP. This enables periodic updates off SIP sessions.
- *Session Expires (sec)*: Time after which a session expires.
- *Minimal SE (sec)*: Minimum time after which a session expires.

DNS-SRV Records

- *Blocking time for unreachable destination (sec)*: Time for which non-reachable destinations are locked out. DNS: **D**omain **N**ame **S**ystem, SRV: **Serv**ice

Trunking Parameter

- *Interval for Sending SIP OPTIONS ping (sec)*: Interval in seconds when the "SIP OPTIONS ping" message is sent for polling the operational readiness of the receiving device. The value "0" means that the message is not sent. Value range of 2 to 720 seconds

Call Supervision

- *MakeCallReq Timeout (sec)*: Timeout time spent waiting for a MakeCallReq message.
- SIP Connect Timeout (sec): 300

Buttons

Click *Apply* followed by *OK* in the confirmation mask. Click *Undo* to discard the changes entered.

6.7.3 Codec Parameters

You can view the settings for the G.711-A-law, G.711-Âµ-law, G.729, G.729A, G.729B, and G.729AB codecs and for the T.38 Fax protocol.

WBM path:

WBM **>** *Configuration* **>** *Voice Gateway* **>** *Codec Parameters*

For descriptions of the individual fields, see below.

The *Codec Parameters* mask is displayed. In the "Codec" table you can view following parameters for the G.711 A-law, G.711 Âµ-law, G-723, G.729, G.729A, G.729B, G.729AB, G722 and Opus:

- *Priority:*This field contains the priority for using the codec. The priority can be set from 1 (high) to 7 (low). Assign different priorities to the codecs. In the default configuration, G.711 A law has priority 1, G.711 Âµ law has priority 2, G.729A has priority 4, and G.729AB has priority 3. G.729B, G.729 have the status "not used".
- *Voice Activity Detection (VAD)*:This field defines whether or not Voice Activity Detection (VAD) should be used for the relevant codec.
- *Frame Size*:You can set the sampling rate in this field. The adjustable values depend on the codecs.
- Opus parameters
- – Use Inband Forward Error Correction (FEC): On
  – Use Constant Bitrate: Off
  – Low delay: off
  – Payload Type of Opus: Standard: 124. Value range: 96-126
  – Maximum Playback Sample Rate: Standard: 16000. Range: 0-48000
  – Complexity: Standard: 1. Value range: 1-10.

T.38 Fax

- *T.38 Fax*: This field defines whether or not the T.38 Fax protocol is to be used.
- *Max. UDP Datagram Size for T.38 Fax*: Maximum size of a T.38 UDP datagram in bytes.
- *Error Correction Used for T.38 Fax (UDP)*: Defines the methods for error correction that should be used (t38UDPRedundancy and t38UDPFEC).
- Time Range for Immediate Switch to T.38 fax (s): A value between 0 and 60 is permitted. The value "0" means that no switchover is performed.

IMPORTANT: The G.729 codec is identical to the G.729A codec and the G729B codec is identical to the Codec G.729AB codec (no "payload" difference). Thus, the G.729 and G.729B codecs are deactivated by default.

IMPORTANT: In H.323 signaling, the G.729 and G.729A codecs, and the G.729B and G.729AB codecs do differ.

IMPORTANT: Some non-OpenScape H.323 endpoints (Cisco GK) use the codec names G.729 or G.729B in "H.323 signalling". In this case, the G.729 and G.729B codecs must be used in HG 3500/3575 as well.

IMPORTANT: In a pure OpenScape network, the G.729 and G.729B codecs can remain deactivated.

Miscellaneous:

- *ClearMode (ClearChannelData)*: This field defines whether or not the ClearChannel function is to be enabled.
- *Frame size*:You can set the sampling rate in this field. Possible settings are 10, 20, 30, 40, 50, and 60 milliseconds (msec). The default setting is 20 msec.

RFC2833:

- *Transmission of Fax/Modem Tones according to RFC2833*: Events supported: 32 to 36 and 49. For a detailed description of the standard see http:///www.faqs.org/rfcs/rfc2833.html.
- *Transmission of Dtmf Tones according to RFC2833*: Events supported: 0 to 15. For a detailed description of the standard see http:///www.faqs.org/rfcs/rfc2833.html
- *Payload type for ClearChannel*: Default: 96, payload type for the ClearChannel codec.
- *Payload type for RFC2833*: Default: 98
- *Payload type for RFC2198*: Default: 99, corresponds to "Payload type for RFC2833" +1
- Redundant Transmission of RFC2833 Tones according to RFC2198: All tones transmitted by RFC2833 are secured according to RFC2198, provided that RFC2198 is active. For a detailed description of the standard see http:///www.faqs.org/rfcs/rfc2833.html and http:///www.faqs.org/rfcs/rfc2198.html

Click *Apply* followed by *OK* in the confirmation mask. Click *Undo* to discard the changes entered.

6.7.4 IP Networking Mode

WBM path:

WBM > *Configuration* > *Voice Gateway* > *IP Networking Mode*

The IP Networking Mode window is displayed. It contains what is used Signaling protocol for IP networking (SIP) and the SIP protocol variant for IP networking (SIP-Q) and a table of the IP networking rates with the Record number (circuit), number of configured B channels and Locked.

The *IP Networking Mode* window is displayed. It contains the following information:

- *Signaling Protocol for IP Networking*: e.g. SIP, is configured by AMO
- *SIP protocol variant for IP networking: SIP-Q*
- *SIP protocol variant for IP networking: Native SIP*
- *Max. Number of B-channels for SIP-Q: This is the value from the AMO CGWB, e.g. B. 0.*
- *SIP protocol variant for native SIP: This is the value from the AMO CGWB, e.g. B. 30.*
- *SIP DNS-SRV survivability mode: Yes / No (DNS: Domain Name System, SRV: Service)*
- *Number of Ports Configured for IP Networking*: e.g. 0, 2

The window contains a table with all the IP Networking Ports:

- *Port Number (circuit)*
- DMC verwenden: Bei einer IP-Vernetzung zwischen HiPath 3000/ OpenScape Business und OpenScape 4000 werden Gateway-Verbindungen Ã¼ber sogenannte DMC-KanÃ¤le realisiert (DMC: Direct Media Connection).
- Instant-DMC verwenden: DMC (Direct Media Connection) wird verwendet, um zwischen zwei SIP-Endpunkten im IP-Netz die Nutzdaten direkt auszutauschen. Default: Ja.
- *Use DMC: Enabled/Disabled*

- *Use Instant DMC: Enabled/Disabled*
- *Is Locked: Yes/No*

6.7.5 SIP Trunk Profile Parameter (not for HG3575)

To enable SIP trunking, the SIP trunking settings must be adapted to the requirements of the relevant SIP provider. To do this, profiles for trunks via SIP-Q and profiles for trunks via native SIP can be activated or deactivated.

WBM path:

WBM > *Configuration* > *Voice Gateway* > *SIP Trunk Profile Parameter*

The *SIP Trunk Profile Parameter* mask is displayed. For field descriptions see below.

This option allows you to edit the settings for *SIP Trunk Profile Parameter*.

The *SIP Trunk Profile Parameter* mask is displayed. It contains:

- SIP protocol variant for IP networking: SIP-Q (cannot be edited)
- SIP protocol variant for IP networking: Native SIP (cannot be edited)
- *Use Profiles for Trunks via SIP-Q*: Can be activated/deactivated. Default setting: deactivated.
- *Use Profiles for Trunks via Native SIP*: Can be activated/deactivated. Default setting: activated.
- *Enable SIP Peer Filtering*: Can be activated/deactivated. Default setting: deactivated. If this feature/checkbox is enabled, only requests from "known" peers are answered. All requests from "unknown" peers are ignored.
- *Participate at SIP load balancing:* Can be activated/deactivated. Default setting: deactivated.

6.7.6 SIP Trunk Profiles

WBM path:

WBM > *Configuration* > *Voice Gateway* > SIP Trunk Profiles

The following sub-folders with the names of SIP providers are displayed in the *SIP Trunk Profiles* tree structure. Each sub-folder contains the settings for that SIP provider. The settings can be displayed, modified or enabled.

WBM > *Configuration* > *Voice Gateway* > SIP Trunk Profiles > *(single-click)* <SIP provider sub-folder> > *SIP Trunk Profile*

The SIP trunk profile for the selected SIP provider is displayed. The following settings can be made:

- *Profile Name:* cannot be changed
- *Account/Authentication required:* can be activated/deactivated.
- *Remote Domain Name:* Enter the name for a remote domain.
- *SIP Transport Protocol:* UDP or TCP can be selected in the option field. Both of these protocols belong to the transport layer in the TCP/IP reference model (UDP: User Datagram Protocol, TCP: Transmission Control Protocol).

Security:

- *Released Security Level:* This cannot be changed.

- *TLS used:* not configurable
- *RTP Security Mode:* Mikey and SDES
- *Payload Encr. used:* not configurable

Registrar:

- *Use Registrar:* Can be activated/deactivated. Determine whether a domain name registrar is to be used.
- *IP Address/Host Name:* Enter the IP address or host name of the domain name registrar.
- *Define Port:* Can be activated/deactivated. Define Port for the Domain Name Registrar.
- *Reregistration Interval (s):* Determine the intervals at which re-registration is required.

Proxy:

- *IP Address/Host Name:* Enter the IP address or host name of the proxy server. This is the provider's SIP server.
- *Define Port:* Can be activated/deactivated. Define the port for the proxy server.

Outbound Proxy:

- *Use Outbound Proxy:* Can be activated/deactivated. This is the proxy server used to access the provider's SIP server. For outbound data traffic for the SIP provider.
- *IP Address/Host Name:* Enter the IP address or host name of the outbound proxy server.
- *Define Port:* Can be activated/deactivated. Define the port for the outbound proxy server.

Inbound Proxy:

- *Use Inbound Proxy:* Can be activated/deactivated. This is the proxy server used to access the provider's SIP server. For inbound data traffic for the SIP provider.
- *IP Address/Host Name:* Enter the IP address or host name of the inbound proxy server.
- *Define Port:* Can be activated/deactivated. Define the port for the inbound proxy server.

Buttons

Click the button *Apply* in order to update the data, *Undo* in order to restore the previous values or *Delete*, to delete the sip trunk profile.

6.7.7 Hunt Group

WBM path:

WBM > *Configuration* > *Voice Gateway* > *Hunt Group* > Hunt Group for SIP Video Clients

The Hunt group for SIP video users table is displayed. It contains the hunt groups for SIP video users with the main number and two secondary numbers.

6.7.7.1 Add

A hunt group for SIP video users can be added. After it has been added, the new hunt group appears in the Hunt group for SIP video users table.

WBM path:

WBM > *Configuration* > *Voice Gateway* > *Hunt Group* > *Add* > Hunt Group for SIP Video Clients

The Hunt group for SIP video users input window is displayed. The main number and up to four secondary numbers can be entered.

Click Apply followed by OK in the confirmation dialog. Click Undo to discard the changes entered, click Delete, to remove the changes.

6.7.8 Destination Codec Parameters

You can add, change or delete the codecs G.711 A law, G.711 Âµ law, G.729A and G.729B for a specific IP address.

WBM path:

WBM **>** *Configuration* **>** *Voice Gateway* **>** *Destination Codec Parameters*

6.7.8.1 Add Destination Codec Parameters

You can add destination codec parameters for a specified IP address.

If you have added a destination codec parameter for a specified IP address, you can also edit it.

You can delete destination codec parameters for a specified IP address.

WBM path:

WBM > *Configuration* **>** *Voice Gateway* **>** *Destination Codec Parameters* **>** *Add Destination Codec Parameters* **>** *Destination Codec Parameters*

The Destination *Codec Parameters* mask is displayed. In the "Codec" table you can enter the following parameters for the "G.711 A-law", "G.711 Âµ-law","G.729", "G.729A", "G.729B" and "G.729AB"protocols:

- *Priority:*This field contains the priority for using the codec. The priority can be set from 1 (high) to 7 (low). Assign different priorities to the codecs. In the default configuration, G.711 A law has priority 1, G.711 Âµ law has priority 2, G.729A has priority 4 and G.729AB has priority 3). G.729B and G.729 have the status "not used".
- *Voice Activity Detection (VAD)*:This field defines whether or not Voice Activity Detection (VAD) should be used for the relevant codec.
- *Frame Size*:You can set the sampling rate in this field. The adjustable values depend on the codecs.

Destination

- *Destination Address Type*: Select the *host*, *subnet* or *area*.
- *IP address*: Enter the associated IP address for the entry.

Buttons

Click Apply followed by OK in the confirmation dialog. Click Undo to discard the changes entered, click Delete, to remove the selected Destination code rule.

6.7.8.2 DARs for MLPP

You can display and edit the digit analysis results (DARs) for MLPP.

WBM path:

WBM > *Configuration* > *Voice Gateway* > *DARs for MLPP* > *DARs for MLPP*

The *DARs for MLPP* table is displayed. It contains the digit analysis results for calls.

The digit analysis results can be changed. The maximum number of characters permitted is 16. These are: 0 to 9, *, #.

The following digit analysis results can be changed:

- Routine Call (DSNR)
- Priority Call (PRTY)
- Immediate Call (IMMED)
- Flash Call (FLASH)
- Flash_Override (FLASHOV)

Click *Apply* button in order to update the data. *Click Undo* to discard the changes entered.

6.7.9 Clients

You can display client settings. Client settings are made using OpenScape 4000 Manager. WBM can only display these settings.

WBM path:

WBM **>** *Configuration* **>** *Voice Gateway* **>** *Clients*

Clients (folder):

Single-click the plus sign (+) next to *Clients* in the tree structure to display the following entries:

1) *UFIP SIP*

Classic SIP

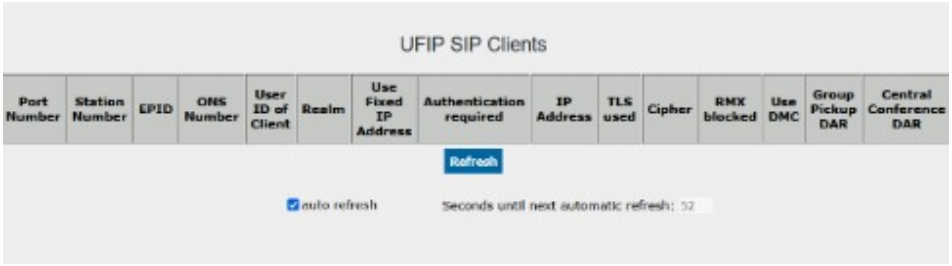
6.7.9.1 UFIP SIP

This option allows you to view the UFIP SIP clients configured in the IP network

You can view the settings for all UFIP SIP clients in a table.

WBM path:

WBM > *Configuration* > *Voice Gateway* > *Clients* > *UFIP SIP* > *UFIP SIP Clients*



A bold line indicates that the SIP client registered successfully.

The *SIP Clients* table is displayed. You can view the following fields:

- *Port number: Displays the internal OpenScape 4000 device identifier of the SIP client.*
- *Station number*: Displays the internal DID of the SIP client.
- EPID: Displays the endpoint identifier (physical device identifier) of the SIP client.
- *ONS Number:* Displays the One Number Service Number of the SIP client.
- *User-Id of Client*: Displays the user name for SIP client access. *Authentication Required* must be activated.
- *Realm*: Displays the area (security zone) for confidential authentication to the SIP client. *Authentication Required* must be activated.
- *Authentication Required*: Configuration parameter in OpenScape 4000, which indicates that authentication (user name and password) is required from the SIP client.
- IP Address: Displays the IP address or host name assigned to the SIP client.
- TLs used: Displays if the SIP client used TLS to register.
- Cipher: Configuration parameter in OpenScape 4000 (AMO SDAT parameter CLASSEC) of the SIP client.
- Use DMC: With an IP network between HiPath 3000 / OpenScape Business and OpenScape 4000, gateway connections are realized via so-called DMC channels (DMC: Direct Media Connection).
- Use instant DMC: DMC (Direct Media Connection) is used to exchange the user data directly between two SIP endpoints in the IP network. Default: yes.
- *Locked: OpenScape 4000 parameter of the SIP client.*
- Use DMC: OpenScape 4000 parameter of the SIP client.
- Group Pickup DAR (Digit Analysis Result): OpenScape 4000 paremeter of the SIP client.
- Central Conference DAR (Digit Analysis Result): OpenScape 4000 parameter of the SIP client.

Button

Refresh: Click this button to refresh the table.

Check box

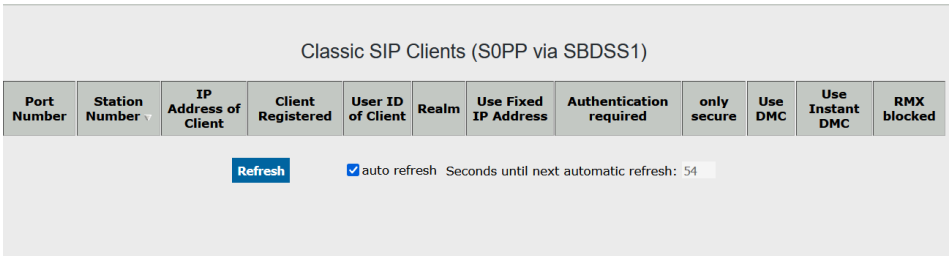
Refresh: Can be activated/deactivated. If the check box is enabled, the "SIP Clients" table is refreshed at regular intervals as specified in the input field *(Seconds to next refresh)*.

6.7.9.2 Classic SIP

WBM path:

WBM > *Configuration* > Voice Gateway > Clients > *Classic SIP* > *Classic SIP Clients (S0PP via SBDSS1)*

You can view the settings for all Classic SIP clients in a table.

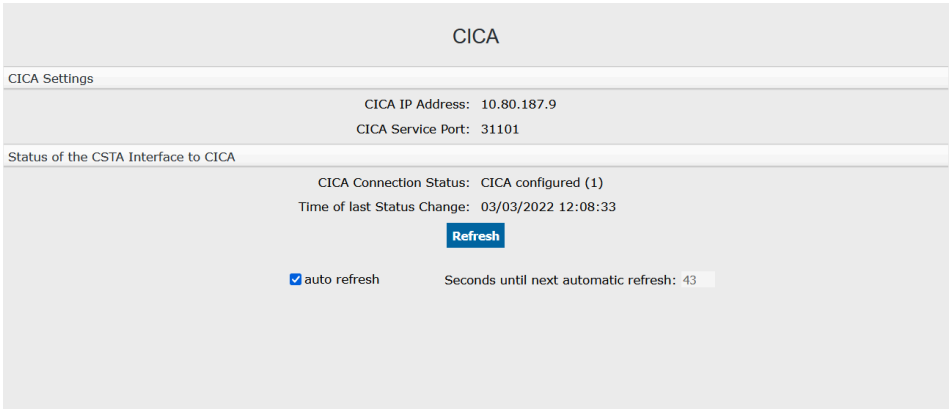


6.7.10 CICA

The CICA functionality requires an NGS IP address configured in accordance with the documentation.

WBM path:

WBM > *Configuration* > Voice Gateway > CICA



6.7.11 ISDN Classmarks

This option allows you to view or change the settings for the ISDN classmarks for CorNet-N transport.

WBM path:

WBM > *Configuration* > *Voice Gateway* > *ISDN Classmarks*

This option allows you to view the settings for ISDN classmarks.

The *ISDN Classmarks for CorNet-N Transport* dialog is displayed.

You can change the following fields:

- *External connection*: Mark this field in order to allow external connections. If the field is not marked, only internal connections are allowed.

- *Hold/transfer*: Mark this field in order to allow functions for holding and transferring calls.
- *Call forwarding*: Mark this field in order to allow call forwarding.
- *Callback*: Mark this field in order to allow callbacks.

Click *Apply* button in order to update the data. *Click Undo* to discard the changes entered.

6.8 Payload

Payload allows you to display and configure connection types and protocols in the gateway, Media Stream Control (MSC) and gateway expansion modules.

WBM path:

WBM **>** *Configuration* **>** *Payload*

The *Payload* tree structure is displayed.

Entries under *Payload*:

1) *Payload Parameters*

Fax/Modem Tone Handling

6.8.1 Payload Parameters

WBM path:

WBM **>** *Configuration* **>** *Payload* **>** Payload Parameters

You can display the list of fax parameters.

The Payload Parameter dialog is displayed. It contains the following settings in the Fax Parameters area:

- Error Correction Mode: Enable/Disable
- Open Fax Channel with Detected Tone: Enable/Disable
- Number of Redundancy Packets: Value range 0 to 2; default is 2
- Maximum Network Jitter (ms): Value range 140 to 500; default is 200

Click Apply and OK in the confirmation dialog. Click Undo to restore the previous values.

6.8.2 Fax/Modem Tone Handling

The parameters in the *Fax/Modem Tone Handling* dialog allow you to decide whether the processing of certain Fax/Modem tone signals shall be disabled (ignored) or enabled.

WBM Path:

WBM > *Configuration* > *Voice Gateway* **>** *Payload* > *Fax/Modem Tone Handling*

You can view and edit the current parameter settings.

The *Fax/Modem Tone Handling* dialog with the following parameters is displayed.

- *Disable Processing of CT Tone*: (Yes/No)
- *Disable Processing of CNG Tone*: (Yes/No)
- *Disable Processing of Early ANS/CED Tone*: (Yes/No)
- *Disable Processing of ANS/CED Tone*: (Yes/No)
- *Disable Processing of CT Tone*: (Calling Tone sent from Modems). If you activate this parameter, the CT Tone sent by the calling modem will be ignored.
  - Possible settings: Enabled/Disabled
  - Default value: Disabled
- *Disable Processing of CNG Tone*: (Calling Tone sent from Faxes). If you activate this parameter, the CNG Tone sent by the calling fax will be ignored.
  - Possible settings: Enabled/Disabled
  - Default value: Disabled
- *Disable Processing of Early ANS/CED Tons*: (Early Detection of Called Tone sent from Modem or Fax). If you activate this parameter, the Early ANS/CED Tone sent by the called fax or modem will be ignored.
  - Possible settings: Enabled/Disabled
  - Default value: Disabled
- *Disable Processing of ANS/CED Tons*: (Called Tone sent from Modem or Fax). If you activate this parameter, the ANS/CED Tone sent by the called fax or modem will be ignored.
  - Possible settings: Enabled/Disabled
  - Default value: Disabled

  Click *Apply* followed by *OK* in the confirmation mask.

6.9 HFA Functions

WBM path

WBM **>** *Configuration* **>** HFA Functions

See Chapter 5 and Chapter 7 for descriptions of the STMIX/STMIY - HFA WBM.

7 HFA WBM - Maintenance

7.1 Maintenance

The *Maintenance* module provides features for maintaining and administering STMIX/STMIY. These features include software updating, saving configurations, working with log files, activating trace profiles, creating a secure trace, creating diagnostic files and determining status information on OpenScape 4000 SoftGate and H.323 telephones.

WBM path

WBM > Maintenance

The *Maintenance* module is displayed.

Options in the *Maintenance* module:

SW-Update

Backup/Restore

Logs

Secure Trace

DLS Client

Diagnostic

Status Information

Reboot OS

7.2 SW-Update

The menu (SW: software) provides functions for displaying the software version, for updating software and for activating software in STMIX/STMIY - HFA.

WBM path

WBM **>** Maintenance **>** SW-Update

The following options are shown in the menu:

Show SW-Version

LW Update

LW Activation

OS Update

7.2.1 Show SW-Version

WBM path

WBM **>** Maintenance **>** SW-Update **>** *Software Version*

The Software Version dialog is displayed. This dialog contains details of the currently installed software and hardware versions.

Information

The following entries are made here:

- *System Version (PBX):* This area shows the OpenScape 4000 Version under:
- *Platform Version:* The details include:
- Hardware, Serial Number, Platform Version, Imported Platform Version, OS Update Status
- **Loadware Version:** This pane shows the installed software and loadware versions. For example:
- *Loadware Version, APS Version*
- *Component Versions:* This pane shows the versions of the installed SoftGate components. For example:
- *IMS SVN Version, SoftGate SVN Version, Soco-common Version*
- *Additional Package Versions:* This pane shows any additional software and associated versions required. For example:
- Java Version

7.2.2 LW Update

WBM path

WBM **>** Maintenance **>** LW Update **>** *Loadware Update*

The Loadware Update dialog is displayed. You can load the STMIX/STMIY application in this dialog. The loadware file is the same as for the OpenScape 4000 SoftGate.

Input field

This dialog contains the following input field:

- *Filename:* Enter the path and file name containing the current software in this field. You can also click Browse to select the file.

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified file is loaded.
- Undo: The path and file name entered are deleted.

Procedure

To load the STMIX/STMIY application, take the following steps:

- Enter the path and file name where the current software is stored or click *Browse* to select the file.

Click Load. The software is loaded. Once the software is loaded, the next WBM page is displayed.

7.2.3 LW Activation

WBM path

WBM **>** Maintenance **>** LW Activation **>** *Loadware Activation*

The Loadware Activation dialog is displayed. In this dialog, you can activate the loaded STMIX/STMIY application either immediately, at a specific time in the future, or after a certain amount of time has passed.

Information

The following information is provided in this dialog:

- *Software Version:* Shows the software version for the STMIX/STMIY application loaded in the Software Update dialog.
- *Start Action on:* The STMIX/STMIY application should be activated at a specific time. The day should be entered using the dropdown lists or via the Calendar button.
- *Start Action in:* The STMIX/STMIY application should be activated after a certain time period.
- *Stop Action:* A previously started action for scheduled activation is stopped.
- *System Time:* This is the local time on OpenScape and the reference time for scheduled activation. This information cannot be edited.

Buttons

The following buttons are shown in this dialog:

- *Apply:* Modifications made to settings are saved.
- *Undo:* Modifications made to settings are deleted and replaced by default values.
- *Start immediately:* Activation of the STMIX/STMIY application is started immediately.

Procedure for immediate activation

To immediately activate the loaded software, follow these steps:

1) Click Start immediately. The software is activated.

Procedure for scheduled activation

To schedule activation for the loaded software, follow these steps:

1) Specify time or duration:

2)
- Time when the activation should occur: Select the Start Action on radio button and enter the Day, Month, Year, HH:MM in the dropdown lists and input fields. You can also use the Calendar button.
- Duration after which the activation should occur: Select the Start Action in radio button and enter the Days and HH:MM in the input fields.

3) Click Apply. The modifications are saved. The action for scheduled activation is started.

Procedure for stopping the scheduled activation

To stop an action for scheduled activation, follow these steps:

1) Activate the Stop Action radio button.

2) Click the Apply button. The action is stopped.

7.2.4 OS Update

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update

The following selection is offered in this menu:

1) OS Update Settings

OS Update Actions

7.2.4.1 OS Update Settings

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update **>** OS Update Settings

The OS Update Settings dialog is displayed. The transfer parameters from the central host for updating the OS (Operating System) of the STMIX/STMIY can be defined in this dialog.

P2P Transfer Parameter from Central Host (Standalone SoftGates

- *Limit Max. Download Speed:* Activate/Deactivate check box. The maximum download speed for updating the OS can be limited to a value that is defined in the input field below.
- *Max. Download Speed (KB/s):* Input field for defining the maximum download speed in KBytes per second.
- *Limit Max. Upload Speed:* Activate/Deactivate check box. The maximum upload speed for updating the OS can be limited to a value that is defined in the input field below.
- *Max. Upload Speed (KB/s):* Input field for defining the maximum upload speed in KBytes per second.

Buttons

- Apply: The input is saved.
- Undo: The input is rejected and the default value restored.

7.2.4.2 OS Update Actions

WBM path

WBM **>** Maintenance **>** SW-Update **>** OS Update **>** OS Update Actions

The OS Update Actions dialog is displayed. The transfer from the central host for updating the OS (Operating System) can be canceled in this dialog.

IMPORTANT: These settings are not yet possible for standalone SoftGates in OpenScape 4000 V7R1. The "Remote Appliance Reinstall (RAR)" function should be used instead.

OS Update Transfer from Central Host (Standalone SoftGates only)

Button:

- *Cancel Transfer:* Transfer of the OS software is canceled.

OS Update Activation

- *Platform Version:* Indicates the Platform version of STMIX/STMIY.
- *Imported Platform Version:* Indicates the imported Platform version of the STMIX/STMIY
- *OS Update Status:* Indicates whether a new update package is available for the OS.
- *Use SoftGate LW from the Update Package (recommended):* Can be activated/deactivated. If this option is not selected, the currently installed SoftGate LW/STMIX/STMIY application will be kept after the OS Update.

Button:

- *Activate OS Update:* Activate the OS update.

7.3 Backup/Restore

In the Backup/Restore menu, you can backup (export) the STMIX/STMIY configuration locally. This local backup can be loaded (imported) and activated.

WBM path

WBM **>** Maintenance **>** Backup/Restore

The Backup/Restore menu is displayed.

Backup/Restore **menu**

The following options are shown in this menu:

1) Export Config

Export Sec Config

7.3.1 Export Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Export Config **>** *Export Configuration*

The *Export Configuration* dialog is displayed. You can back up (export) the STMIX/STMIY configuration locally using this dialog. This backup also contains the SIP

Buttons

The following buttons are shown in this dialog:

- *Apply:* Start the configuration export.
- *Undo:* Cancel the configuration export.

Procedure

To export the configuration, follow these steps:

1) Click *Apply.* The security configuration is exported to a ZIP file. A *File Download* window appears, asking you to open or save the ZIP file.
2) Click *Save* and select the folder where you wish to store the file. Then click *OK*. The ZIP file is saved.

7.3.2 Export Sec Config

WBM path

WBM > Maintenance > Backup/Restore > Export Sec Config > *Export Security Configuration*

The *Export Security Configuration* dialog is displayed. You can back up (export) the STMIX/STMIY configuration (including SIP security configuration) locally using this dialog.

Buttons

The following buttons are shown in this dialog:

- Apply: Start the configuration export.
- Undo: Cancel the configuration export.

Procedure

To export the security configuration, follow these steps:

1) Click Apply. The configuration is exported to a ZIP file. A File Download window appears, asking you to open or save the ZIP file.
2) Click Save and select the folder where you wish to store the file. Then click OK. The ZIP file is saved.

7.3.3 Import Config

WBM path

WBM > Maintenance > Backup/Restore > Import Config > *Import Configuration*

The *Import Configuration* dialog is displayed. In this dialog, you can import the STMIX/STMIY configuration saved locally.

Input field

This dialog contains the following input field:

- *Filename:* Enter the path and file name where the configuration you wish to import is stored in this field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *Load:* The specified configuration file is loaded.
- *Undo:* The path and file name entered are deleted.

Procedure

Proceed as follows to import a configuration file:

1) Enter the path and name of the configuration file or select the file with the *Browse* button.
2) Click the *Load* button. The configuration file is loaded.

STMIX/STMIY has to be restarted for the configuration changes to take effect.

7.3.4 Import Sec Config

WBM path

WBM **>** Maintenance **>** Backup/Restore **>** Import Sec Config **>** *Import Security Configuration*

The Import Security Configuration dialog is displayed. In this dialog, you can import the STMIX/STMIY security configuration saved locally.

Input field

This dialog contains the following input field:

- Filename: Enter the path and file name where the security configuration you wish to import is stored in this field. You can also click Browse to select the file.

Buttons

The following buttons are shown in this dialog:

- Load: The specified file is loaded.
- Undo: The path and file name entered are deleted.

Procedure

Proceed as follows to import the security configuration:

- Enter the path and file name where the security configuration you wish to import is stored or click Browse to select the file.
- Click Load. The file is loaded.

IMPORTANT: STMIX/STMIY has to be restarted for the configuration changes to take effect.

7.3.5 Import of classic STMI backup data to STMIX/STMIY

WBM path

To import classic STMI backup data to STMIX/STMIY, use the existing import mechanism:

Maintenance > Backup/Restore > Import Config

NOTICE: The automatic HBR restore mechanism via Assistant also works, if a STMI board is replaced by a STMIX/STMIY board.

Implementation

The following data will be imported from STMI to STMIX/STMIY:

- The active SIP trunk profile status and parameters
- SIP Parameters
- The configuration of Codecs

NOTICE: The parameter "Allow SIP Register for Trunking" needs to be re-configured if used via *Basic Settings* > *Gateway*.

The SPE configuration is handled via DLS or Assistant.

The STMI backup is based on a file named export.xml. The STMIX/STMIY accepts zip files that contain a file with this name.

A positive HBR restore is confirmed via the following HISTA message:

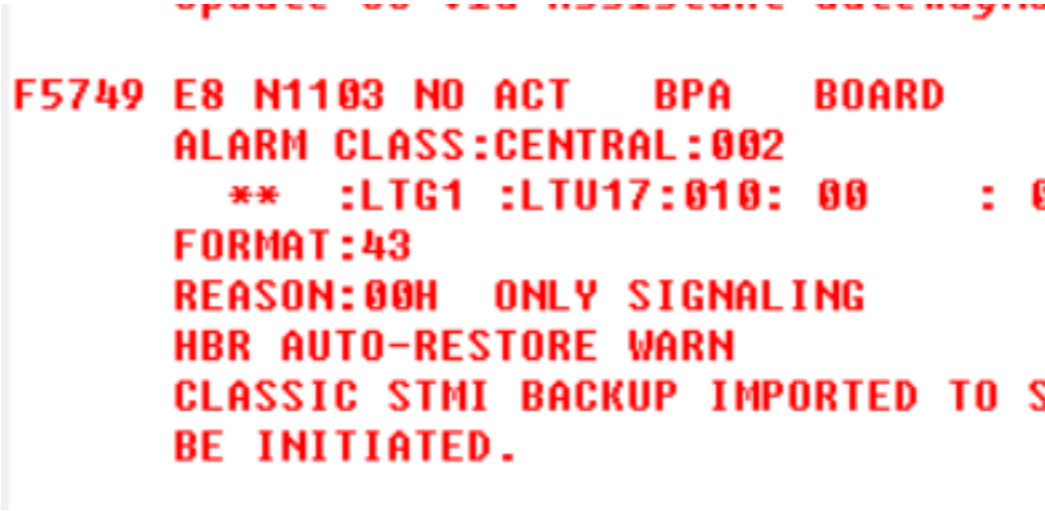


Figure 2: F5749 HISTA message

NOTICE:

This message is not visible in case of a restore via WBM.

After the import, it is recommended to initiate a new HBR backup.

7.3.6 Factory Reset

WBM path

WBM>Maintenance > *Backup/Restore* >*Factory Reset*

The **Reset Configuration to Factory Default** dialog is displayed.

You can factory reset the STMIX/STMIY board using this dialog.

WARNING:

Choosing Factory Reset will shutdown the board.

Buttons

The following button is shown in this dialog:

- **Reset to Factory Default**: Start the Factory Reset.

Procedure

To trigger the factory reset, follow these steps:

1) Click **Reset to Factory Default.** This will trigger the procedure in the background and will shutdown the board after it's done.
2) Remove the board after reset.

7.4 Logs

In the *Logs* menu, you can export log files for diagnostic purposes to a ZIP file. To create new log files, you can delete the old (i.â
e. exported) log files.

WBM path

WBM **>** Maintenance **>** Logs

The following options are shown in the menu:

1) Export Logs

   Delete Logs

   Trace Profiles

7.4.1 Export Logs

WBM path

WBM **>** Maintenance **>** Logs **>** Export Logs **>** *Export Logfiles*

The *Export Logfiles* dialog is displayed. You can store (export) the STMIX/ STMIY log files locally using this dialog.

Buttons

The following buttons are shown in this dialog:

- Export: The log files selected via check box are stored locally (exported).

Procedure

To export log files, follow these steps:

1) Click Export. The log files are exported to a ZIP file. A File Download window appears, prompting you to open or save the ZIP file.
2) Click Save and select the folder where you wish to store the file. Then click OK. The ZIP file is saved.

7.4.2 Delete Logs

WBM path

WBM **>** Maintenance **>** Logs **>** Export Logs **>** Delete Logs **>** *Delete Logfiles*

The Delete Logfiles dialog is displayed. In this dialog, you can select and delete one or several of the log files listed.

Check boxes

The following check boxes are shown in this dialog:

- *Soco, JLM, IMS, SPA, ETS, Status Collector, Update, Backtrace, Heap Dump, Corelogs, Garbage Collection, Gateway (vHG) Logs, LS-DCL, Load Balancer, DHCP, System Diagnostics*
- *All:* All log (diagnostic) files are selected.

Buttons

The following buttons are shown in this dialog:

- *Delete:* All selected log files are deleted.
- *Undo:* Modifications made to settings are deleted and replaced by default values.

Procedure

To delete log files, follow these steps:

1) Enable the check boxes next to the log files you wish to delete.
2) Click Delete. The selected log files are deleted.

7.4.3 Trace Profiles

WBM path

WBM **>** Maintenance **>** Logs **>** Trace Profiles **>** *Edit Trace Profile Configuration*

NOTICE: This function may only be used by developers.

The *Edit Trace Profile Configuration* dialog is displayed. In this dialog, you can enable trace profiles for detailed analysis of the STMIX/STMIY. Each trace profile records special information. The Trace Profile settings will be reset to Default during Loadware or OS Update.

Trace Profiles

Enable the trace profiles listed here to explore the following problems:

- *acw-cc:* Developer-specific
- *cg:* Developer-specific
- *dataloading:* Developer-specific
- *dcl2:* Developer-specific
- *debug-all:* Developer-specific
- *dls-client:* Developer-specific
- *dmc-detail:* Developer-specific

- h323-performance:
- *heap-diag:* Developer-specific
- *hfa-call:* Used for problems with HFA connection signaling and HFA device login/logoff.
- *hfa-reg:* Used for problems with HFA device registration, e.g. faulty displays on the devices.
- *ipconfig:* Developer-specific
- *ipv6:* Used if problems occur when networking via IP V6.
- *lcphone:*
- *maintenance:* Developer-specific
- *osa:* Trace profile for OpenScape Access
- *osa-clock:* Trace profile for OpenScape Access
- *osa-light:* Trace profile for OpenScape Access
- *osa-trace:* Trace profile for OpenScape Access
- *payload:* Used for problems with voice connections (like payload-light). Affects system performance! Due to the creation of comprehensive trace output, this profile may not be enabled in cases of heavy system load.
- *payload-light:* Used for problems with voice connections. Can also be enabled in cases of increased system load. See also paragraph "payload".
- *payload-native:* Developer-specific
- *qdc:* Developer-specific
- *reconnect:* Developer-specific
- *scc:* Used for general payload problems, conference connections and IPDA connections.
- *sip:* When this trace profile is enabled, the STMIX/STMIY - SIP trace messages configured in the local STMIX/STMIY - SIP WBM are transferred to the SoftGate log file. At the same time, SIP-relevant scc traces are recorded.
- snmp:
- *startup:* Used for boot problems on the SoftGate and virtual boards.
- STMIX/STMIY:
- *system:* This trace profile is always enabled and cannot be disabled.
- *thread-profiling:* Developer-specific
- *wbm:* Developer-specific

Buttons

The following buttons are shown in this dialog:

- Apply: The settings for the enabled/disabled check boxes are saved.
- Undo: The settings for the enabled/disabled check boxes are reset.
- *Restore Default:* The settings for the enabled/disabled check box is set to default.

Procedure

To enable trace profiles, follow these steps:

1) Select the check box for the trace profile you need for an analysis.
2) Click Apply. The settings for the enabled/disabled check boxes are saved.

7.5 Secure Trace

A secure trace is used to detect faults in the communication system. The secure trace produces records via encrypted VoIP payload and signaling streams to and from STMIX/STMIY - HFA.

The secure trace contains encrypted records. These records can be decrypted by developers using a key.

WBM path

WBM **>** Maintenance **>** Secure Trace

The *Secure Trace* menu is displayed.

The following options are shown in the menu:

1) Import Certificate

Show Certificate

State

Start Trace

Stop Trace

Basic procedure for creating a secure trace

To create a secure trace, proceed as follows:

1) The service technician detects a problem in the customer network. Upon consultation with the developer, the necessity of creating a secure trace is determined.

2) The customer is informed of this need and must confirm that they have been informed. The customer orders the creation of a secure trace, including the date and time when the monitoring should start and end.

3) Development creates a pair of keys consisting of a public and a private key. Only one secure trace can be created with this pair of keys. Certificates are applied as follows:

4)
- The certificate with the private key is strictly confidential and can only be used by authorized developers.
- The certificate with the public key is provided to the service technician or can be downloaded from the HiSat home page (https://hisat.global-intra.net/wiki/index.php/SecureTrace).

5) The service technician informs the customer about the beginning of trace activities. The customer must inform the affected users.

IMPORTANT: Recording calls and connection data is a criminal offence if the affected users have not been informed.

---

1) The service technician supplies the certificate to the vHG 3500 HFA gateway for which the secure trace is being created; see Section 6.14.1, "Import certificate".

2) The service technician activates the secure trace function; see Section 6.14.4, "Start Trace". A secure trace is created. The activation and later deactivation (Section 6.14.5, "Stop Trace") are logged by the communication systems involved.

3) After a secure trace has been created, the customer is informed about the end of trace activities. The service technician removes the certificate from the system.
4) The secure trace is provided to the developer.
5) The developer decrypts the secure trace using the private key. The developer then analyzes the decrypted records.

After the analysis is complete, all relevant materials and data must be securely destroyed. This includes the destruction of the private key, preventing unauthorized copies of the secure trace from being decrypted.

7.5.1 Import Certificate

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Import Certificate **>** *Load the Secure Trace Certificate via HTTP*

The *Load the Secure Trace Certificate via HTTP* dialog is displayed. You can import a secure trace certificate using this dialog. This certificate is a requirement for creating a secure trace. The service technician receives it from the developer. It contains the public key and must be available in PEM or binary format. The certificate is always valid for a maximum of one month.

Input field

This dialog contains the following input field:

- *Certificate file (PEM or binary):* Enter the path and name of the file containing the certificate in this input field. You can also click *Browse* to select the file.

Buttons

The following buttons are shown in this dialog:

- *View Fingerprint of Certificate*: You can check the fingerprint to determine whether an unchanged certificate is available or whether it has been modified.
- *Import Certificate from File*: The certificate is imported from the file specified in the above input field.

Procedure

Proceed as follows to import the certificate:

1) Select: *WBM* **>** Maintenance **>** Secure Trace **>** Import Certificate. The *Load the Secure Trace Certificate via HTTP* dialog is displayed.
2) Click *Browse* to select the file containing the certificate and confirm by clicking *Open*. The file is loaded.
3) Click *View Fingerprint of Certificate*. A window appears showing the fingerprint of the certificate you wish to import:
4) **a)** Check the fingerprint (hexadecimal figure). When the certificate is changed, the fingerprint always changes. Only an unchanged fingerprint guarantees an unchanged certificate. If the two fingerprints are not identical, an attack was probably attempted. In this case, the key should no longer be used and the specified measures should be taken.

   Click *OK* to close the fingerprint window.

5) Click *Import Certificate from File* if you are satisfied with your examination of the fingerprint. Do not import the certificate if the fingerprint does not satisfy your expectations.

A secure trace can now be created.

7.5.2 Show Certificate

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Show Certificate **>** *Certificate Information*

The *Certificate Information* dialog is displayed. In this dialog, you can see the secure trace certificate, e. g. to test it.

Displayed data

The following certificate data is displayed:

- *General data: Certificate Name, Certificate Type, Serial Number of Certificate, Serial Number of Certificate (hex), Type of Signature Algorithm, Start Time of Validity Period (GMT), End Time of Validity Period (GMT), CRL Distribution Point*
- *Issued by CA: Country (C), Organization (O), Organization Unit (OU), Common Name (CN)*
- *Subject Name: Country (C), Organization (O), Organization Unit (OU), Common Name (CN)*
- *Subject Alternative Name*
- *Public Encryption Key Data*: *Public Key Length*, *Public Key*, *Fingerprint*

7.5.3 State

WBM path

WBM **>** Maintenance **>** Secure Trace **>** State **>** *Secure Trace State*

The *Secure Trace State* dialog is displayed. In this dialog, you can find out whether a secure trace is being created.

Displayed data

The following data is displayed:

- *Secure Trace is active*: This line shows if a secure trace is currently being created.
- *Automatic Deactivation Time*: This line shows when the secure trace is to be created and when the secure trace function will be automatically deactivated.

Secure Trace for these protocols: This line shows the protocols for which the secure trace was created. These may be: Media Server (SRTP).

7.5.4 Start Trace

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Start Trace **>** *Start Secure Trace*

The *Start Secure Trace* dialog is displayed. You can start the secure trace in this dialog. The following requirements must be met:

- The secure trace is not yet active.
- The customer has authorized the creation of a secure trace and wishes to enter their *Secure Trace Activation Passphrase* in the WBM.
- You have received a public key from the developer and loaded it to the WBM.

Input fields and check boxes

- *Start Parameters*:
- – *Secure Trace Activation Passphrase*: To limit the usage of the secure trace function, activation is secured by a special passphrase known only to the customer. This passphrase is the customer's key and the certificate is the service technician's key. Both keys are required to activate the secure trace function.

  Passphrases are passwords that consist of multiple words up to a maximum length of 20 characters.

  – *Duration of Secure Trace (Mins.)*: You must enter the duration of the secure trace in minutes.
- *Secure Trace protocols*:
- – *MediaServer (SRTP)*: The secure trace is created for MediaServer. The SRTP (Secure Real-Time Transport Protocol) is used for encrypted transmission via IP-based networks and uses AES (Advanced Encryption Standard) for encryption.

Buttons

The following button is shown in this dialog:

- *Start Secure Trace*: This starts the secure trace. The requirements named in this document must be fulfilled to start the secure trace.

Procedure

Proceed as follows to start the secure trace:

1) Check if the requirements named earlier have been fulfilled.
2) Select: *WBM* **>** Maintenance **>** Secure Trace **>** Start Trace. The *Start Secure Trace* dialog is displayed.
3) In the *Start Parameters* area, enter the *Secure Trace Activation Passphrase* and the *Duration of Secure Trace (Mins.)*.
4) Select the *MediaServer (SRTP)* protocol.

Click the *Start Secure Trace* button. The secure trace is created for the duration specified.

7.5.5 Stop Trace

WBM path

WBM **>** Maintenance **>** Secure Trace **>** Stop Trace **>** *Stop Secure Trace*

The *Stop Secure Trace* dialog is displayed. In this dialog, you can stop an active secure trace, even if the duration specified under Start Trace has not yet elapsed.

Button

The following button is shown in this dialog:

Stop Secure Trace: The secure trace is stopped.

7.6 DLS Client

1) The DLS client is used for administration of PKI data and the QDC configuration (DLS: **D**ep**l**oyment **S**ervice or **D**eployment and **L**icencing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

NOTICE: The DLS client can only be configured in the STMIX/STMIY - HFA WBM. The configurations will be distributed to the STMIX/STMIY - SIP/IPDA part.

WBM path

WBM **>** Maintenance **>** DLS Client

The *DLS Client* is displayed.

The following options are shown in the menu:

1) DLS Settings

Enter PIN

Reset Bootstrapping

Contact DLS

Bootstrapping

Bootstrapping allows a secure, certificate-based SSL connection to be established between the DLS server and DLS client.

Based on a connection request from the DLS client to a DLS server as well as the subsequent response - i.e. still an unreliable connection - a reliable connection is established through the alternating authentication and exchange of certificates (i.e. bootstrapping = a simple system develops inherently into a complex system).

Because a different DLS server can respond to the connection request from the DLS client instead of the desired DLS server in order to take the desired connection for itself, security measures must be put in place. The DLS server (i.e. its IP address and port) that is to contact the DLS client can be administered using the AMO.

It is recommended to authorize the DLS client at the DLS server by entering a bootstrap pin on the STMIX/STMIY WBM, which was previously generated randomly by the DLS server. Authorization of the DLS client can also be performed with an internal standard system PIN that does not have to be entered, or PIN authorization can also be relinquished completely. These two options are not recommended however.

The certificates are exchanged once the reliable connection has been established, see below.

Certificate generation and distribution for communication between the DLS client and DLS server:

All certificates and private keys for encrypted communication between the DLS client and DLS server are generated by the DLS server's self-signing certification authority (CA) and sent by the DLS server during bootstrapping to the DLS client.

The PKCS#12 file sent from the DLS server to the DLS client contains the DLSC client certificate, the private key contained in it and the certificates of the DLS server's certification authority (DLSC CA certificate). The DLS server can read all certificates it delivers apart from the private key.

Certificate generation and distribution for the secure connection between WBM and the DLS server:

The administrator manually sends the WBM certificate containing the private key generated by the customer's PKI certification authority to OpenScape 4000 Assistant. OpenScape 4000 Assistant then automatically sends its WBM certificate to all gateways. The DLS client uses this certificate to identify itself at the DLS server.

7.6.1 DLS Settings

Apart from automatic registration of the DLS client at the DLS server with the ContactMe response, the DLS client can also be registered manually. To do this, you need the IP address and port of the DLS server for bootstrapping mode. The IP address and the port of the DLS server can be configured using the AMO. This change only becomes effective after restarting STMIX/STMIY.

Once the IP address and port of the DLS server have been set, another attempt is made when the system reboots (and each subsequent reboot) to initiate bootstrapping by sending a connection request.

Other connection setup attempts can be initiated manually with the menu option *Contact DLS*. If bootstrapping has still not been performed, it is initiated automatically, otherwise it is simply checked whether the DLS is accessible.

WBM path

WBM **>** Maintenance **>** DLS Client **>** DLS Settings **>** *Edit DLS Client Basic Setup*

The *Edit DLS Client Basic Setup* dialog opens.

Input field

The following input field is shown in the *Current DLS Client Basic Configuration* area:

- *Time interval for ContactMe Response*: Amount of time the DLS client waits after sending its connection request to receive the ContactMe response from the DLS server. The wait time must be restricted so that ContactMe responses cannot be intercepted by unwanted DLS servers.

Displays

The following displays are shown in this dialog:

- *Current DLS Client Basic Configuration*:
- – *PIN required for DLS Bootstrapping*: The PIN can be entered under the menu option Enter PIN. *Yes*: A PIN was entered. *No*: No PIN was entered.
  – *Secure Communication with DLS Server*: *Enabled* or *Disabled*
- *Current DLS Client Server Configuration*:
- – *IP Address of DLS Server*: The IP address of the DLS server for bootstrapping mode can be configured using the AMO. You must reboot STMIX/STMIY.
  – *Port of DLS Server*: The port of the DLS server for bootstrapping mode can be configured using the AMO. You must reboot STMIX/STMIY.
  – *Secure Port of DLS Server*: STMIX/STMIY port for secure connection to the DLS server. The *Secure Port* can be configured in AMO.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The modified settings are saved.
- *Undo:* The modified settings are rejected and the default value is restored.

7.6.2 Enter PIN

WBM path

WBM **>** Maintenance **>** DLS Client **>** Enter PIN **>** *Enter the Bootstrap PIN*

The *Enter the Bootstrap PIN* dialog opens. The bootstrap PIN generated randomly by the DLS server can be entered in this dialog.

Input field

The following input field is shown in this dialog:

- *Bootstrap PIN*: If a PIN was entered in this input field and saved by clicking *Apply*, the *Edit DLS Client Basic Setup* dialog (menu option DLS Settings) shows that a PIN is required for DLS bootstrapping.

Buttons

The following buttons are shown in this dialog:

- *Apply:* The modified settings are saved.
- *Undo:* The modified settings are rejected and the default value is restored.

7.6.3 Reset Bootstrapping

WBM path

WBM > Maintenance > DLS Client > Reset Bootstrapping > *Reset DLS Client Bootstrapping*

The *Reset DLS Client Bootstrapping* dialog opens.

Button

The following button is shown in this dialog:

- *Reset Bootstrapping*: Bootstrapping for the DLS client is reset.

7.6.4 Contact DLS

Additional attempts to set up a connection to the DLS server can be initiated manually with the menu option *Contact DLS*. If bootstrapping has still not been performed, it is initiated automatically, otherwise it is simply checked whether the DLS is accessible.

WBM path

WBM > Maintenance > DLS Client > Contact DLS

The *Contact DLS* dialog opens.

The following selection options are offered in this menu:

1) DLSC Keycert

DLSC CA Certs

***Contact DLS* dialog**

The following button is shown in this dialog:

1) *Contact*: The DLS server is contacted in order to check whether it is still available.

7.6.4.1 DLSC Keycert

The DLSC client certificate with the private key can be found under this menu option. The DLS client uses these certificates to identify itself at the DLS server. The DLS client receives the certificate from the DLS server in bootstrapping mode.

WBM path

WBM > Maintenance > DLS Client > Contact DLS > DLSC Keycert

The DLSC Keycert menu opens

The individual DLSC client certificates can be selected under this menu option:

7.6.4.2 1.DLSC Keycert

WBM path

WBM > Maintenance > DLS Client > Contact DLS > DLSC Keycert > 1.DLSC Keycert > *Certificate Information*

The *Certificate Information* dialog opens.

Data displayed

The following data from the certificate is shown:

- General data: *Certificate Type*, *Serial Number of Certificate*, *Serial Number of Certificate (hex)*, *Type of Signature Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Name*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Alternative Name*
- *Public Key Encryption Data*: *Public Key Length (parameter)*, *Public Key*, *Fingerprint*

7.6.5 DLSC CA Certs

WBM path

WBM > Maintenance > DLS Client > Contact DLS > DLSC CA Certs

This folder contains the DLSC CA certificates delivered by the DLS server in bootstrapping mode.

The *DLSC CA Certs* menu opens.

The individual DLSC client certificates can be selected under this menu option:

"1. DLSS CA Cert," "2. DLSC CA Cert"

7.6.5.1 "1. DLSS CA Cert", "2. DLSC CA Cert"

WBM path

WBM > Maintenance > DLS Client > Contact DLS > DLSC CA Certs > "1. DLSS CA Cert", "2. DLSC CA Cert"

The *Certificate Information* dialog opens.

Data displayed

The following data from the certificate is shown:

- General data: *Certificate Type*, *Serial Number of Certificate*, *Type of Signature Algorithm*, *Start Time of Validity Period (GMT)*, *End Time of Validity Period (GMT)*, *CRL Distribution Point*
- *Issued by CA*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*

- *Subject Name*: *Country (C)*, *Organization (O)*, *Organizational Unit (OU)*, *Common Name (CN)*
- *Subject Alternative Name*
- *Public Key Encryption Data*: *Public Key Length (parameter)*, *Public Key*, *Fingerprint*

7.7 Diagnostic

Under *Diagnostic*, you can configure settings for monitoring IP connections and create diagnostic files.

WBM path

WBM **>** Maintenance **>** Diagnostic

The *Diagnostic* menu is displayed.

The following options are shown in the menu:

1) Diagnostic Functions

Diagnostic Files

7.7.1 Diagnostic Functions

WBM path

WBM **>** Maintenance **>** Diagnostic **>** Diagnostic Functions

The *Diagnostic Functions* dialog is displayed. In this dialog, you can modify settings for IP connection monitoring, for internal LAN capture control, for thread profiling and for heap monitoring.

Areas

The following areas are shown in this dialog:

1) Internal LAN Capture Control

Thread Profiling

Heap Monitoring

Buttons

The following buttons are shown in this dialog:

- Apply: Modifications made to settings are saved.
- Undo: Modifications made to settings are deleted and replaced by default values.

Internal LAN Capture Control

Settings for internal monitoring of IP package in the LAN can be made in the pane. This monitoring is carried out with tshark or tcpdump for example. The current content is written to the backtrace file in case of a critical restart. Older capture files are deleted when monitoring is started. If these are still needed, you have to export them using Logs > Export Logs.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
- – *Headers Only:*Only the IP packet headers should be monitored.
  – *Start:* The internal LAN capture control should be started.
  – LoopBack Interface (only): Only the LoopBack interface should be used.
- Selection field:
- – *Filter:*You can select a filter for monitoring IP packets. Choose from:
  – – *none* (no filter)
    – *tcp* (only Transmission Control Protocol IP packets)
    – *udp* (only User Datagram Protocol IP packets)
- Display:
- – *Status:* The status display indicates whether internal LAN capture control is active.

Thread Profiling

Thread profiling can be used to check whether threads fully utilize the CPU as planned. This means thatâ
threads where low CPU utilization is expected should meet this expectation.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
- – *Start:* Thread profiling should be started.
- Input fields:
- – *Sample Rate, ms (100-500):* You can set the sample rate, with the default setting at 250.
  – *Thread CPU Load Threshold for Stacktrace, % (10-90):* You can set the maximum CPU usage; default: 50.
- Display:
- – *Status:* This shows whether thread profiling is active.

Heap Monitoring

Create a heap dump to write all objects in the heap to a file.

Controls and indicators

This area contains the following controls and indicators:

- Check boxes:
- – *Start:* Start heap monitoring.
- Input fields:
- – Sample Rate, ms (500-5000): You can set the sample rate, with the default setting at 1000.
  – Memory Usage Threshold for Heapdump, % (50-90): You can set the amount of memory to be used for the head dump; default: 80.
- Display:
- – *Status:* This shows whether heap dump monitoring is active.

7.7.2 Diagnostic Files

WBM path

WBM **>** Maintenance **>** Diagnostic **>** Diagnostic Files

The *Diagnostic Files* dialog is displayed.

Log files are stored on the RAM disk, i.â
e. on a virtual temporary data medium in the main memory. These log files can be exported and unpacked in an archive file. A backup trace file contains the content of the stack at the time of generation.

Buttons

The following buttons are shown in this dialog:

- Create Heap Dump: Creates a file containing all Java objects reachable at the moment of creation. You can use this file to analyze main memory usage.

  NOTICE: The Backtrace archive file (content of RAMDISK/ramdisk.zip) contains all log files stored on the RAM disk and is now included in the ordinary log export.

7.8 Status Information

WBM path

WBM **>** Maintenance **>** Status Information

The *Status Information* menu is displayed.

The following options are shown in the menu:

1) System Information

SoftGate Connection Control

7.8.1 System Information

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information

The System Information menu is displayed.

The following option is shown:

Show Thread Health

7.8.1.1 Show Thread Health

WBM path

WBM **>** Maintenance **>** Status Information **>** System Information **>** Show Thread Health **>** *Thread Health*

The *Thread Health* table is displayed. This table displays currently active threads. The following information is displayed: T*hread Name, Thread ID, Context Class Hashcode, time blocked [ms], max. time blocked [ms].*

7.8.2 SoftGate Connection Control

WBM path

WBM **>** Maintenance **>** Status Information **>** SoftGate Connection Control

The *SoftGate Connection Control* menu is displayed.

The following option is shown in the menu:

1) Show All Connections

7.8.2.1 Show All Connections

WBM path

WBM **>** Maintenance **>** Status Information **>** SoftGate Connection Control **>** Show All Connections **>** *SCC connection table*

The *SCC connection* table is displayed. This table displays all currently active SCC connections. The following information is displayed: Device, Type.

Button

Refresh: The connection list is refreshed manually by clicking this button.

Check boxes

Refresh: Can be activated/deactivated. The connection list is refreshed automatically every 60 seconds if this check box is enabled.

Display

Seconds to next refresh: Indicates in how many seconds the connection list will be refreshed automatically.

7.9 Reboot OS

WBM path

WBM **>** Maintenance **>** Reboot OS

The *Reboot OS* menu is displayed.

7.9.1 Reboot OS

WBM path

WBM **>** Maintenance **>** Reboot OS

The STMIX/STMIY operating system can be restarted in this window.

Button

- Reboot OS: The STMIX/STMIY operating system is shut down and then automatically restarted by clicking this button.

8 SIP/IPDA WBM - Maintenance

8.1 Maintenance

This module contains all the functions necessary for HG 3500 on STMIX/STMIY - SIP/IPDA maintenance and administration.

WBM path:

WBM **>** *Maintenance*

The *Maintenance* module's options are displayed on the left.

Options in the Maintenance module:

1) *Config & Update Job List Traces & Events*

8.2 Config & Update

8.2.1 Configuration

Configuration and ("SSL data") can be saved externally and reloaded. It is also possible to reset the configuration to the factory default.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration*

The *Configuration* tree structure is displayed.

Entries under *Configuration*:

Configuration Data SSL Data

Reset Configuration to Factory Default

8.2.2 Configuration Data

You can back up and restore configuration data. You can also define what data should be saved or what data should be loaded.

The configuration data is saved as plain text and can be read or printed using any text editor.

SIP Configuration export is an expert diagnosis mechanism. The normal Backup and Restore is done on the STMIX/STMIY HFA WBM.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration Data*

The *Configuration Data* tree structure is displayed.

Entries under *Configuration Data*:

Load from Gateway Load to Gateway

8.2.2.1 Load from Gateway

This is the backup function. You can backup the current STMIX/STMIY - SIP configuration at a secure location.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration Data* **>** *Load from Gateway*

The *Load Configuration from the Gateway via HTTP* mask appears. In this dialog, you can set which configuration data should be backed up.

***Load Configuration Data from the Gateway via HTTP* dialog:**

In the individual window areas, you can select the data you wish to back up:

- *Optional parameters*:
  - *Use Compression:* Depending on the storage available, you can define whether backed up data should be compressed.
- *Specify Tables to Back Up*:
  - *Select all tables*: All subsequent tables are set to *All*.
  - *Deselect all tables*: All subsequent tables are set to *None*.

  You can also select/deselect tables individually.
- *Trunking Data*:
  - *All*/*None*: If *All* is selected, the table entry is marked. The selection is canceled by clicking *None*.
  - The list includes: *Class Mark*
- *IP Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - You can mark the following individually: *Global IP Settings*
- *LAN Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - You can mark the following individually: *LAN1 Interface*, *LAN2 Interface*, *PPTP/PPPoE Parameters*
- *Payload Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - The list includes: *DSP Channel Conf.*
- *H.323 Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - The list includes: *H.323*, *Endpoint Registration*

- *SIP Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - The list includes: *SIP Parameters*, *Internet Telephony Service Provider*, *Internet Telephony Station*, *SIP Protocol Manager*, *Loadable SIP Profiles*, *Hunt group for SIP video users*
- *Diagnostic Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - The list includes: *Global Trace Information*, *Event Log Conf.*, *Event Reaction Table*, *Trap Destination*, *E-mail List*, *Trace via LAN Conf.*
- *Miscellaneous Data*:
  - *All*/*None*: If you select *All*, all the data listed in that table is marked. If you select *None*, none of the data in that table is marked.
  - The list includes: *Global Data*, *Automatic Actions*, *Online Help*, *TFTP Servers*, *Port Administration (Global)*, *Port Administration (Local)*, *Version Information*, *Global Network Routing DataCodecs*, *Destination Codecs*, *Class Mark*, *DLS Addressing*

Once you have selected the data you wish to back up, click *Load*. An information window is displayed that you must confirm with *OK*. Click Undo to discard the changes entered.

8.2.2.2 Load to Gateway

This is the restore function. You can load an externally stored configuration to the gateway.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration Data* **>** *Load to Gateway* **>** *Load via HTTP*.

The *Load configuration to the Gateway via HTTP* dialog appears.

"Load Configuration Data to the Gateway via HTTP" dialog:

The following is displayed:

- *Remote File Name (PC File System)*: Enter the file name under which the data is saved.
- *Browse*: You can search the local file system for the backup file.

Then click *Load*. An information window is displayed that you must confirm with *OK*. The data is now loaded to the gateway flash memory (but not yet activated).

The mask *Do you want to activate the configuration now?* is now displayed. In this mask, you can set which configuration data should be loaded.

In the individual window areas, you can select the data you wish to back up. For explanations on this, please see the previous section *Load from Gateway*. Finally click *Activate Now*.

Save data:

The changes will be automatically saved - if necessary - perform a restart (note the Reset icon! See also Section 4.3.2, "Icons in the WBM Window's Status Area").

IMPORTANT: If the configuration file downloaded should be activated at a later date, click *Do Not Activate*. To activate the configuration data at a later point, click *Job List* in the maintenance menu and then activate this job (see Section 8.3, "Job List").

8.2.3 SSL Data

The SSL/SPE configuration data for SIP is encrypted when downloaded from the gateway and must be protected by an encryption password. This encryption password must be specified again for loading the configuration data into the gateway.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration* **>** *SSL Data*

The *SSL Data* tree structure is displayed.

Entries under *SSL Data*:

1) *Load from Gateway Load to Gateway*

8.2.3.1 Load from Gateway

NOTICE: Normal backup is done via HFA maintenance.

WBM path:

WBM **>** *Maintenance* **>** *Config & Update* **>** *Configuration* **>** *SSL Data* **>** *Load from Gateway* **>** *Load SSL/SPE Configuration Data from the Gateway via HTTP*

The *Load SSL/SPE Configuration Data from the Gateway via HTTP* dialog appears.

***Load VPN/SSL/SPE Configuration Data from the Gateway via HTTP* dialog:**

The following is displayed:

- *Encryption Password*: Enter encryption password for the SSL/SPE configuration data.
- *Re-enter Encryption Password*: Repeat the encryption password.

Click *Load* after selecting the data to be backed up. A message window is displayed that you have to acknowledge with *OK*.

8.2.3.2 Load to Gateway

This is the restore function. You can load a configuration that is saved externally to the gateway.

NOTICE: Normal restore is done via HFA maintenance.

WBM path:

WBM > *Maintenance* > *Config & Update* > *Configuration* > *SSL Data* > *Load to Gateway*.

The *Load VPN/SSL/SPE Configuration Data to Gateway via HTTP* dialog appears.

***Load VPN/SSL/SPE Configuration Data to Gateway via HTTP* dialog:**

The following is displayed:

- *Remote File Name (PC File System)*: Enter the required file name under which the data is saved.
- *Browse*: You can search the local file system for the backup file.

Then click *Load*. A message window is displayed that you have to acknowledge with *OK*. The data is now loaded to the gateway flash memory. It is not activated yet, however.

The dialog *Do you want to activate the configuration now?* is now displayed. In this dialog, you can define which configuration data should be loaded.

Save data:

The changes will be automatically saved - if necessary - perform a restart (note the Reset icon. See also Section 4.3.2, "Icons in the WBM Window's Status Area").

IMPORTANT: If the configuration file downloaded is to be activated at a later date, click *Do Not Activate*. To activate the configuration data at a later point, click *Job List* in the maintenance menu and then activate this job (see Section 8.3, "Job List").

8.2.4 Reset Configuration to Factory Default

You can reset the SIP configuration to the factory defaults that were preset upon delivery.

WBM path:

WBM > *Maintenance* > *Config & Update* > *Configuration* > *Reset Configuration to Factory Default*

An important message is displayed that you should read:

NOTICE: This action resets the complete SIP configuration to the delivery status. All administration and customer data

is deleted! Only the IP address, netmask, and IP address of the default router for LAN1 are preserved. The gateway automatically reboots while this action is running.

Then click *Reset to Factory Settings*. The STMIX/STMIY automatically reboots while this action is running.

8.3 Job List

The job list contains entries for current data transmissions.

WBM path:

WBM **>** *Maintenance* **>** *Job List*

The list of jobs is displayed. The list contains the following columns:

- *Type*: This column shows the task of each job and how it was started.
- *ID*: The column shows the unique job number in each case.
- *Duration*: This column shows how many seconds have passed since the job was started.
- *Status*: This column indicates whether jobs are still in progress or already completed.
- *Action*:
- – Use the *Abort and Delete Job* button to cancel the corresponding action.
  – The downloaded configuration is activated using the *Activate Configuration* button.

The following buttons are also provided:

- *Refresh*: The displayed job list is reloaded and shows the current data.
- *Delete All Jobs*: All jobs in the list are deleted. An information window must be confirmed with *OK*.

8.4 Traces & Events

This section documents Traces and Events in the WBM.

8.4.1 Traces

A trace logs the execution of a software component. A technician can use these process records to determine the cause of an error.

IMPORTANT: Activating traces can have a negative impact on the performance of the system. When the trace file has reached the maximum size, it is closed and saved as "trace.bak" in the same directory. At the same time a new (empty) "trace.txt" is created.

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Traces*

The *Traces* tree structure is displayed.

Entries under *Traces*:

1) *Load All Logs*

Delete All Logs

Trace Configuration

Load Trace Log

Clear Trace Log

Trace Profiles

Stop All Trace Profiles

Trace Components

Display Started Trace Components

Stop All Trace Components

Secure Trace

M5T Trace Components

M5T Syslog Trace

Service Center

With the trace configuration you can define whether traces should be logged and how this should be performed. If the traces on the gateway machine are logged in a file, you can save and delete the trace log for this file. Using trace profiles and trace components, you can configure the traces to be logged, and the detail in which this information should be provided.

8.4.1.1 Load All Logs

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Traces* **>** *Load All Logs*

The *Load All Logs* dialog is displayed.

Options

- *Trace Log*: Can be activated/deactivated. The trace log can be loaded.
- *Event Logs*: Can be activated/deactivated. The event log can be loaded.

Buttons

- *None*: The enabled check boxes are disabled.
- *Load*: The selected logs are loaded.
- Undo: The changes are discarded.

8.4.1.2 Delete All Logs

You can delete all SIP related logs stored on the gateway. For example: Trace and Event logs as well as Core logs.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Traces* > *Delete All Logs*

Click *Delete Logs* to delete all logs.

8.4.1.3 Trace Configuration

You can check/specify which interface should be used to output trace data.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Traces* > *Trace Configuration*

The trace configuration is displayed. You can edit the following fields:

Console trace

- Activate synchronous console trace:
- If this option is activated, trace messages are not buffered, i.e. if trace messages are called, they are output immediately on the console. This type of tracing slows down the software process and should only be used for diagnosis. It is especially suitable for tracing before system crashes. By activating the option all other trace interfaces are deactivated.
- Activate console trace:
- Check this option to have the trace data output to the console on the V.24 connection.
- Copy the trace entries into the SoftGate log
- Activate synchronous copying: can be activated / deactivated

  Activate copy: can be activated / deactivated. If this checkbox is activated, this impairs the performance of the module

File Trace

- *Switch File Trace On*: Activate this option to write the trace data to a log file.

The following fields provide additional information:

- *Maximum Trace File Size (byte)*: The maximum size of the log file if the option *Switch File Trace On* is activated.

General Trace Configuration

- *Trace Levels Survive Upgrade*: Activate this option to trace upgrade problems.

Trace via LAN (XTracer)

- *Switch Trace via LAN (XTracer) On*: Activate this option to transfer the trace data via the LAN interface. A server port is opened when you do this, which is used for connections from a LAN tracer client. The server port remains open following deactivation until the next reboot.

The following fields provide additional information:

- *XTracer connected*: Indicates whether or not XTracer is connected.
- *Timer Value (sec)*: The interval in seconds until data is transferred if the option *Switch Trace via LAN On* is activated.
- *Server Port*: Server port for connections from a LAN tracer client

IMPORTANT: All other trace interfaces are deactivated automatically if the trace output is handled via ServiceCenter/ CSDA.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.1.4 Load Trace Log

If file trace is activated, (see Section 8.4.1.3, "Trace Configuration"), you can load the log file from the gateway to the administration PC or to another computer. You can also delete the log file.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Traces* > *Load Trace Log*

Load via HTTP

You can save trace log files from STMIX/STMIY - SIP on the administration PC.

The data starts to load when the *Load via HTTP* menu item is selected. The alert message "File loading. Please wait!" is displayed.

IMPORTANT: You have to wait for the load process to complete. This may take some time. The load process is canceled if you launch another function in the WBM during this time.

Once the file has been transferred it is shown immediately in the system editor.

8.4.1.5 Clear Trace Log

The log file can be deleted from the gateway flash memory. This is useful if you have performed Load via HTTP.

WBM path:

WBM > Maintenance > Traces & Events > Traces > *Clear Trace Log*

An important warning is displayed. Click *Delete* followed by *OK* in the confirmation mask.

8.4.1.6 Trace Profiles

Trace profiles define the data to be logged and the detail in which this information should provided. Trace components (see Section 8.4.2, "Events") are assigned to a trace profile. This allows you to specify the gateway components for which a trace profile process and status information should be logged. The detail provided in the logs can be set using trace levels.

You can create, modify and delete user-defined trace profiles. Predefined trace profiles are also provided. You can stop all trace profiles at once, or start and stop them individually. When you start a trace profile, logging is activated for this profile. When you stop the profile, logging is deactivated.

See also: Section 9.1.2, "Trace Profiles".

NOTICE: Activated trace profiles will automatically be deactivated during Loadware or OS Update.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Traces* > *Trace Profiles*

Single-click the plus sign (+) next to *Trace Profiles* to view the individual trace profiles. Trace profiles with a green bullet point have been started, those with a red bullet point have been stopped.

You can view a list of all predefined and user-defined trace profiles.

The *List of Trace Profiles* mask is displayed. The name of each trace profile is displayed together with status information indicating whether the trace profile has been started.

Display All Trace Profiles

You can view a list of all predefined and user-defined trace profiles.

The *Trace Profile:[Name]* mask is displayed. The profile name is displayed together with status information indicating whether the trace profile is write-protected and whether it is currently started. The table underneath provides a list of the trace components assigned to the trace profile and the trace level configured in each case.

Permanent trace profile

Permanent tracing profiles allows you to diagnose the issues from the data stored automatically on the gateway, thus optimizing the time needed for analysis. Also, due to it's permanent activation, it allows you to identify the sporadic issues.

Permanent tracing is handled as a new trace profile: Permanent Tracing. The profile is enabled by default.

8.4.1.7 Stop All Trace Profiles

You can stop all started trace profiles at once (see Section 8.4.1.8, "Trace Components").

WBM path:

WBM > *Maintenance* > *Traces & Events* > Traces > *Stop All Trace Profiles*

The *Traces* tree structure is updated.

8.4.1.8 Trace Components

Trace components are gateway components for which process and status information can be logged. You can view and edit the settings for trace components as well as activating and deactivating monitoring by trace components.

See also: Section 9.1.1, "Trace Components".

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Traces* **>** *Trace Components*

Trace Components (folder):

Single-click the plus sign (+) next to *Trace Components t*o view the individual trace components. Trace components with a green bullet point have been started, those with a red bullet point have been stopped.

The *Edit All Trace Components* is displayed by default. For each trace profile, the subsystem name, component index, and configured trace level are displayed together with status information as to whether the trace component is currently started.

You can view a list of all trace components that are currently started.

For each trace profile, the subsystem name and the configured trace level are displayed.

You can call up a list of all trace components containing detailed information, and modify the trace level data provided.

The subsystem name is shown for each trace profile. You can edit the following fields:

- *Trace Level*: Specify the accuracy (trace level) that the corresponding trace component should apply. Trace levels have a value range from 0 to 9. 0 stands for the least amount, and 9 for the greatest amount of detail. Thus, the higher the number, the more trace information provided.
- *Trace On*: Activate this field to start the corresponding trace component.

IMPORTANT: There are trace components which cannot be modified or which can be modified with restrictions. Non-changeable elements of a trace component are displayed in gray.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.1.9 Display Started Trace Components

You can view detailed information for an individual trace component.

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Traces* **>** selected trace component **>** *List of Started Trace Components*

The *Trace Component mask: [Name]* is displayed. This mask shows the trace component index, subsystem name, configured trace level and whether the trace level is currently started. The area *Data Included in the Trace Output* lists the trace data that is logged for this trace component. Exact field descriptions are provided in Section 8.4.1.8, "Trace Components".

8.4.1.10 Stop All Trace Components

You can view a list of all trace components that are currently stopped.

WBM path:

WBM > *Maintenance* > *Traces & Events* > Traces > *Display Stopped Trace Components*

The *List of Stopped Trace Components* mask is displayed.

8.4.1.11 Secure Trace

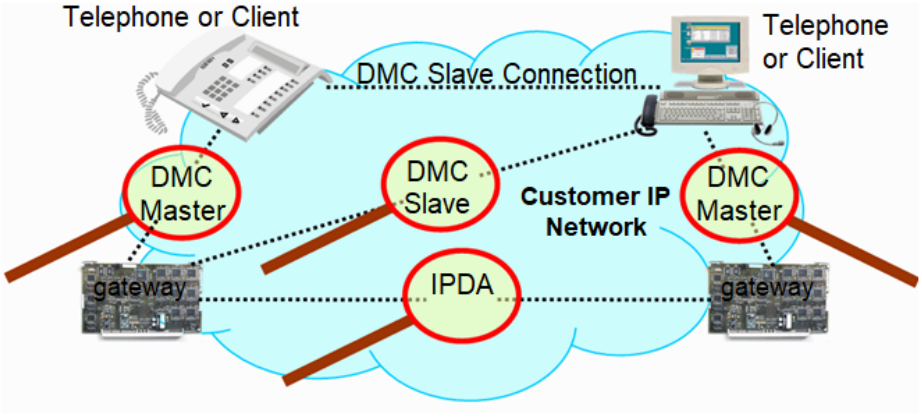
WBM path:

WBM > Maintenance > Traces & Events > Traces > *Secure Trace*

What is a secure trace?

Secure Trace is a feature for determining malfunctions in the OpenScape system. It produces information about encrypted VoIP user and signaling data streams to and from the common gateway.

IMPORTANT: In this document, a gateway is the HG 3500 gateway on OpenScape 4000 V10.



A secure trace can be generated for the following connections:

- DMC master connections (gateway <-> client/telephone)
- DMC slave connections (gateway <-> client/telephone)
- Standard SIP connections (gateway <-> client/telephone)
- CorNet-IP NQ network (gateway <-> gateway)
- SIP-Q network (gateway <-> gateway)

- IPDA connectivity (SL200 <-> gateway)

The secure trace contains encrypted information. This information can be decrypted by the developer with an appropriate key.

Secure trace procedure:

The procedure for creating a secure trace is as follows:

1) The service technician detects a problem in the network. The technician discusses the need for a secure trace with the developer.
2) The customer is informed of this need and must confirm receipt of notification. The customer then issues a secure-trace request specifying when monitoring should start and end (with date and time).
3) The developer generates a key pair consisting of the public key and the private key. This key pair can only be used for one secure trace. The certificates are used as follows:
4) • The certificate with the private key is strictly confidential and can only be used by authorized developers.
   • The certificate with the public key is provided to the service technician.
5) The service technician informs the customer about the beginning of trace activities. The customer must inform the affected users.

IMPORTANT: Recording calls and connection data is a criminal offence if the affected users have not been informed.

---

1) The service technician supplies the certificate to the gateways for which the secure trace is being created; see Section 8.4.1.12, "Secure Trace Options".
2) The service technician activates the secure trace function. A secure trace is created. The activation and later deactivation are logged by the OpenScape systems involved.
3) Once the secure trace has been generated, the customer is informed about the end of trace activities. The service technician removes the certificate from the system.
4) The secure trace is forwarded to the developer.
5) The developer decrypts the secure trace using the private key. He or she then analyzes the decrypted recordings.
6) All relevant material and data must be safely destroyed once analysis is complete. The private key must also be destroyed to prevent decryption of any illegal copies of the secure trace.

8.4.1.12 Secure Trace Options

This entry allows you to display and edit the gateway properties and settings.

WBM path:

WBM > Maintenance > Traces & Events > Traces > *Secure Trace* > *Secure Trace Options*

Secure Trace State

This mask indicates if a secure trace is currently active.

The *SecureTrace State* mask is displayed with the following data:

- *SecureTrace is active*: This field shows if a secure trace is currently underway.
- *Automatic Deactivation Time*: This field shows when the secure trace is scheduled to finish and when the secure trace function will automatically deactivate.
- *SecureTrace for these protocols*: This field shows the protocols for which the secure trace is generated. The options are: SIP Core/SSA (TLS), MSC (SRTP).

8.4.1.13 Start Secure Trace

Prerequisites:

You can only start the secure trace if the following prerequisites have been satisfied:

- Secure trace is not yet active.
- The customer requested a secure trace and would like to enter the *SecureTrace Activation Password* in WBM (passphrase: a password that consists of multiple words and contains up to 20 characters).
- You received a public key from the developer and imported it into WBM.

WBM path:

WBM **>** Maintenance **>** Traces & Events **>** Traces **>** *Secure Trace* **>** *Start Secure Trace*

Procedure:

Proceed as follows to start the secure trace:

1) Select:WBM **>** Maintenance **>** Traces & Events **>** Traces **>** *Secure Trace* **>** *Start Secure Trace.* The *Start SecureTrace* mask is displayed.

2) Enter the following data in the "Start Parameters" area:

3)
- *SecureTrace Activation Password*: To restrict the use of the Secure Trace function, activation is protected by a special passphrase known only to the customer. This passphrase is therefore the customer's key and the certificate is the service technician's key. Both keys are needed to start the secure trace.
- *Duration of SecureTrace (s)*: This is a mandatory entry.

4) Set the protocols for which the secure trace is to be created: All protocols in the "SecureTrace protocols" area are activated by default. Deactivate the protocols for which a secure trace should not be generated:

5)
- TC (TLS)
- H.323 Core/HSA (TLS)
- MMX (PEP)
- SIP Core/SSA (TLS)
- MSC (SRTP)

6) Click *Start SecureTrace*. The secure trace is generated.

8.4.1.14 Stop Secure Trace

WBM path:

WBM > *Maintenance* > Traces & Events > Traces > *Secure Trace* > *Stop Secure Trace*

Procedure:

Click *Stop SecureTrace* in the "Stop SecureTrace" mask.

8.4.1.15 Import Secure Trace Certificates (PEM or Binary)

Certificate:

This certificate is needed to generate a secure trace and is provided by the developer. It contains the public key and must be provided in PEM or binary format. The certificate is valid for up to one month.

WBM path:

WBM > Maintenance > Traces & Events > Traces > *Secure Trace* > *Import Secure Trace Certificates (PEM or Binary)* > *Load the Secure Trace Certificate via HTTP.*

Procedure:

Proceed as follows to import the certificate:

1) Select: WBM > Maintenance > Traces & Events > Traces > *Secure Trace* > *Import Secure Trace Certificates (PEM or Binary)* > *Load the Secure Trace Certificate via HTTP*. The *Load the Secure Trace Certificate via HTTP* mask is displayed.
2) Click *Browse* to select a file containing the certificate and confirm with *Open*. The file is loaded.
3) Click *View Fingerprint of Certificate*. A window showing the fingerprint of the certificate to be imported is displayed:

Check the fingerprint (= hexadecimal numeral). The fingerprint always changes if a certificate has been changed. An unchanged fingerprint is the only guarantee that the certificate is authentic. If the two fingerprints are not identical, an attempted attack has probably occurred. If this happens, you must destroy the key and take appropriate measures.

Click *OK* to close the window with the fingerprint.

1) Click *Import Certificate from File* if you are satisfied with the fingerprint check. Do not import the certificate if the fingerprint does not meet your expectations.

You can now generate the secure trace.

8.4.1.16 M5T Trace Components

WBM path:

WBM > Maintenance > Traces & Events > Traces > M5T Trace Components > *Edit All Trace Components*

The *Edit all Trace Components* dialog is displayed. The table contains the following parameters:

- *Package Name*: Name of trace component, cannot be changed
- *Trace Level*: Value range 0 to 9
- *Trace on*: Yes/No

Click *Apply* and *OK* in the confirmation dialog.

Displaying packages

In the *M5T Trace Package: <Name of Trace Component>* dialog, the package for the trace component is displayed. For a description of the individual parameters, see M5T Trace Package.

M5T Trace Package

WBM **>** Maintenance **>** Traces & Events **>** Traces **>** M5T Trace Components **>** *<Trace Component>* **>** *M5T Trace Package*

The *M5T Trace Package: <Name of Trace Component>* dialog is displayed. The packages contain the following parameters:

- *Package Name*: Name of trace component, cannot be changed
- *Index*: cannot be changed
- *Trace Level*: Value range 0 to 9
- *Trace on*: Yes/No

Starting the trace component

WBM **>** Maintenance **>** Traces & Events **>** Traces **>** M5T Trace Components *<Non-active Trace Component>* **>** *Trace On*

The trace is started. The symbol in front of the module name switches from default black to green.

Stopping the trace component

WBM **>** Maintenance **>** Traces & Events **>** Traces **>** M5T Trace Components *<Active Trace Component>* **>** *Trace Off*

The trace is stopped. The symbol in front of the module name switches from default black to red.

Click *Apply* and *OK* in the confirmation dialog. Click Undo to discard the changes entered.

8.4.1.17 M5T Syslog Trace

The M5T Syslog Trace mask is displayed. The following parameter is shown:

Address the M5T Trace shall be sent to:

- IP Address:
- Port: e.g (6000)

Click *Apply* and *OK* in the confirmation dialog. Click Undo to discard the changes entered.

8.4.1.18 Service Center

The Service Center is an additional diagnostic tool for developers.

NOTICE: This function may only be used by developers.

WBM path:

WBM > Maintenance > Traces & Events > Traces > M5T Trace Components *Service Center*

The *Service Center* window is displayed. It contains settings for the Service Center, i. e. whether the Service Center is enabled and its server port.

Use the *Activate Service Center* check box to enable or disable the Service Center.

8.4.2 Events

Events report problems in the SIP part of STMIX/STMIY. The administrator should check the network or gateway configuration to correct the irregularity.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Events*

Single-click the plus sign (+) next to *Events* to display the following entries:

1) *Event Configuration E-Mail Reaction Table*

8.4.2.1 Event Configuration

You can view the event configuration settings and specify whether the event log should be transferred via a LAN.

WBM path:

WBM > *Maintenance* > *Traces & Events* > *Events* > *Event Configuration*

You can view the current event configuration settings.

The *Event Configuration* mask is displayed. For descriptions of the individual fields, see below.

A special tool, for example, TMT-Tracer or X-Trace, is needed for event logging over LAN. You can activate and deactivate event logging via LAN.

Event file settings

The following fields provide additional information:

- *Maximum Event Buffer Size (byte)*: The number of log files saved to the buffer memory.
- *Maximum Event File Size (byte)*: The maximum size of the log file.
- *Event Timer (sec)*: The interval in seconds until data is written to the log file.

Event via LAN (XTracer)

You can edit the following field:

- *Switch Event Logging via LAN On*: Using this option you can activate and deactivate event logging.

The following field is shown for information purposes:

- *Timer Value (sec)*: The interval in seconds before data is transferred.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.2.2 E-Mail

You can review and define the e-mail address to which a warning should be sent if an event occurs.

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Events* **>** *E-mail Settings*

You can view detailed information on mail delivery when an event occurs.

The *E-mail Settings* mask is displayed. For descriptions of the individual fields, see Section 8.4.2.2, "Edit E-mail Settings".

Edit E-mail Settings

You can modify detailed information for mail delivery when an event occurs.

The *E-mail Settings* mask is displayed. You can edit the following fields:

- *SMTP Server (IP Address)*: Enter the IP address of the computer via which e-mails routed using SMTP should be sent. As HG 3500/3575 does not support authentication for SMTP, select an SMTP server without authentication.
- *SMTP Server (Port)*: Enter the SMTP server port. The default value is 25.
- *SMTP Domain*: Enter the domain name of the computer via which e-mails routed using SMTP should be sent. The SMTP domain corresponds to the domain name of the mail server.

IMPORTANT: Adhere to the conventions in accordance with RFC 821 and RFC 822. The SMTP server settings are required because the STMIX/STMIY - SIP only supports the "relay agent" function and cannot itself be used as an SMTP server.

- *From*: Enter the text that should appear in the "From" field in the case of notification e-mails.
- *Subject*: Enter the text that should appear in the "Subject" field in the case of notification e-mails. The subject line should specifically refer to a message in the event log.
- *Recipient 1* to *Recipient 5*: You can enter up to five e-mail addresses in this field. Notification e-mails are sent to all addresses entered.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.2.3 Reaction Table

You can define individually for *Events* how the system should react to this event.

NOTICE: The events in the reaction table are described in *Overview: Event Codes*.

WBM path:

WBM **>** *Maintenance* **>** *Traces & Events* **>** *Events* **>** *Reaction Table* **>** *Event Reaction Configuration*

Reaction Table (folder):

Single-click the plus sign (+) next to *Reaction Table* to view the individual event messages. Single-click an individual event message to display the *Event Reaction Configuration.*

Edit All Events

Details of the individual events are displayed clearly in a single table in the *Event Reaction Configurations* dialog.

The following information is displayed for each event:

- *Event Name*: The internal name of the event is shown.
- *Send an SNMP Trap*: This indicates whether an SNMP trap is sent when the event occurs.

The following settings can be changed for each event:

- *Send an E-mail*: If this option is activated, an e-mail will be sent when this event occurs (see Section 8.4.2.2, "E-Mail").
- *Associated Trace Profile*: You can assign one of the existing trace profiles to this event (see Section 8.4.2, "Events").
- *Start/Stop Trace Profile*: You can specify whether the selected trace profile should be started or stopped by this event.

Click *Apply* and *OK* in the confirmation dialog.

WBM path:

WBM **>** *Maintenance* **>**Traces & Events **>** *Events* **>** *Reaction Table* **>** selected event **>** *Event Reaction Configuration*

The *Event Reaction Configurations* mask is displayed. For descriptions of the individual fields, see Section 8.4.2.3, "Edit Event".

Edit Event

The following fields provide additional information:

- *Event Name*: The internal name of the event is shown.
- *Send an SNMP Trap*: This indicates whether an SNMP trap is sent when the event occurs.
- *Reboot Gateway*: This indicates whether the gateway must be restarted if the event occurs.
- *Notify OpenScape*: This indicates whether a message is sent to the OpenScape system if the event occurs.

You can edit the following fields:

- *Send an E-mail*: If this option is activated, an e-mail will be sent when this event occurs (see Section 8.4.2.2, "E-Mail").
- *Associated Trace Profile*: You can assign one of the existing trace profiles to this event (see Section 8.4.2, "Events").
- *Start/Stop Trace Profile*: You can specify whether the selected trace profile should be started or stopped by this event.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.3 Admin Log

The administration log is generated on the gateway machine. Logins are logged on the gateway machine. You can review and configure the protocol language. You can also download the log file from the STMIX/STMIY.

WBM path:

WBM > *Maintenance* > Traces & Events > *Admin Log*

Single-click the plus sign (+) next to *Admin Log* to display the following entries: *Configuration Load Admin Log Data*

8.4.3.1 Configuration

You can review and configure the administration log language on the STMIX/ STMIY.

WBM path:

WBM > *Maintenance* >Traces & Events > *Admin Log* > *Configuration* > *Admin Log Properties*

You can configure a different language for the administration log.

The *Admin Log Properties* mask is displayed. You can edit the following field:

- *Admin Log Language*: Select the required language. You can choose between English and German.

Click *Apply* followed by *OK* in the confirmation mask. Click Undo to discard the changes entered.

8.4.3.2 Load Admin Log Data

You can download the administration log from the STMIX.

WBM path:

WBM > *Maintenance* > *Admin Log* > Traces & Events > *Load Admin Log Data*

Load via HTTP

You can transfer the administration file from the STMIX/STMIY - SIP to the computer used to administer the gateway.

Once the file has been transferred it is shown immediately in the system editor.

8.5 Appl. Diagnostics

WBM path:

WBM > *Maintenance* > Appl. Diagnostics

The features in this area may only be used by developers.

9 Appendix: Traces and Events

This reference chapter contains:

- *Traces*, described according to individual trace components and trace profiles. Traces can be administered using the WBM (See Section 8.4, "Traces & Events", and in particular Section 8.4.2, "Events" and Section 8.4.2, "Events").
- *Events*, described according to individual event codes. Events can be administered using the WBM (See Section 8.4.2, "Events").

9.1 Traces

NOTICE: If traces are requested by the service, then the components and profiles to be traced are also notified.

9.1.1 Trace Components

The table is used for locating the trace components more quickly. The trace components are created in the same sequence as in WBM.

Overview of Trace Components
ADMIN
ASP
ASP_DSP
ASP_DSP_EVENT
ASP_DSP_IFTASK
ASP_DSP_INIT
ASP_DSP_IOCTL
ASP_DSP_STAT
ASP_FAX
ASP_PS
ASP_VMOD
ASP_VMUX
CARDADM
CFG_CODECS
CFG_H235
CFG_H323

Overview of Trace Components
CFG_H323ENDPOINT
CFG_H323GKI
CFG_H323GWI
CFG_H323I
CG
CMGMT
CNQ
CNQIWK
COMMUNITIES
CPMSG
CPUTRACE
CTS
DELIC_DRIVER
DEVMGR
DISPATCH
DLSC
DMC
DSP
DSP_TRACE
DSS1
EMAIL_MANAGER
EMIWK
EVTLOG
EVTLOGTRAP
FAXCONV_IF
FAXCONV_LOGT
FAXCONV_OS
FAXCONV_T30DOWN
FAXCONV_T30INT

Overview of Trace Components
FAXCONV_T30UP
FAXCONVERTER
FMSEM
GATEWAY
GWGLOBAL_DATA
GWGLOBAL_SI_DOWNL_PORTFUNC (HG 3500 only)
GWSI (HG 3500 only)
H323
H323_EPT
H323_GLOBAL_SI_DOWNLOADS
H323_SPE
H323IWK
H323MSG
HFAC (HG 3500 only)
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

Overview of Trace Components
IPSTACK_IPFILTER
IPSTACK_MACFILTER
IPSTACK_NAT
IPSTACK_ROUTE
IPSTACK_SNTPS
ISDN_FM
LAN
LICMGMT
LOCSERV
LOCSERV_CFG
LOCSERV_QUERY
LOCSERV_REG
LOG_MSG
LSDCL
LTUC
MANAGER
MAT_STREAM
MCP
MGAF_TBL
MIKEY
MMX (HG 3575 only)
MPH
MSC
MSC_DSP
MSC_QM
MSC_RTCP
MSC_SPECIFIC_STAT
MSC_TMT
MSP_CAPI_IF

Overview of Trace Components
MSP_HDLC
MSP_PPP_IF
MSP_RTP_MOD
NWRS
OAM
OAM_ACTIONLIST
OSF_PCS
PERFM_PL
PERFM_SIG
PLATFORM
PORT
PORT_MGR
PPP_CC
PPP_STACK_DBG_IF
PPP_STACK_PROC
PPPM_TBAS
PPPM_TEXT
PPPM_TSTD
PPTP_DBG_IF
PPTP_PROC
Q931
QDC
QDC_UDPPING
ROUTE98
RTPQM
SACCOB_DRV (HG 3500 only)
SCN
SCNPAY
SDR

Overview of Trace Components
SECURE_TRACE
SECURITY_SVC
SENDTMT
SENTA_API
SERVICE_TRACE
SESSION_MGMT
SI
SIP
SIP_CFG
SIP_CFG_INT
SIP_FM
SIP_GLOBAL_SI_DOWNLOADS
SIP_HT
SIP_REG
SIP_SA
SIP_TRK
SIP_TRK_FM
SIU_STARTUP
SLMO_HFA
SNMP
SPE_SVC
SPL
SS
SSL_UTIL
SSM
STACKTRACE
STATIC_ROUTES
STB (HG 3575 only)
STRC

Overview of Trace Components
STREAMS
SWCONF
SYSTEM
T90
TC (HG 3500 only)
TCP_IP_CONF (HG 3575 only)
TCPMOT_WT (HG 3575 only)
TCPSIG (HG 3575 only)
TCPSIG_WT (HG 3575 only)
TCPSUV (HG 3575 only)
TCPSUV_WT (HG 3575 only)
TESTLW
TIME_SYNC
TIME_SYNCH_TASK (HG 3575 only)
TOOLS
TRAP
TSA (HG 3500 only)
WAN
WEBAPPL
WEBSERVER
WEBSERVER_STATISTIC
WEBSRV_CLIENT_IF
WEBSRV_SYS_IF
X25
X75
XMLUTILS

ADMIN

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Incoming and outgoing admin messages with all details. This impacts the system performance.

Trace level **9** (DETAIL): Incoming and outgoing admin messages with all details, likewise internal admin messages such as poll information. This impacts the system performance significantly.

ASP

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Information on connection setup and cleardown.

Trace level **9** (DETAIL): Detailed information on connection setup and cleardown from MSP (with the exception of DSP-DD)

ASP_DSP

Configured default trace level: **0** (STATUS)

ASP_DSP_EVENT

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Information on detected tone selection or fax devices or modems.

ASP_DSP_IFTASK

Configured default trace level: **0** (STATUS)

ASP_DSP_INIT

Configured default trace level: **0** (STATUS)

ASP_DSP_IOCTL

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Detailed information on connection setup and cleardown (with all parameters).

ASP_DSP_STAT

Configured default trace level: **0** (STATUS)

Trace level **6** (INTRA): Information on data channel configuration following connection setup (fax, modem, V.110).

ASP_FAX

Configured default trace level: **0** (STATUS)

ASP_PS

Configured default trace level: **0** (STATUS)

ASP_VMOD

Configured default trace level: **0** (STATUS)

ASP_VMUX

Configured default trace level: **0** (STATUS)

CARDADM

Configured default trace level: **0** (STATUS)

CFG_CODECS

Configured default trace level: **0** (STATUS)

CFG_H235

Configured default trace level: **0** (STATUS)

CFG_H323

Configured default trace level: **0** (STATUS)

CFG_H323ENDPOINT

Configured Default Trace Level: 0 (STATUS)

CFG_H323GKI

Configured default trace level: **0** (STATUS)

CFG_H323GWI

Configured default trace level: **0** (STATUS)

CFG_H323I

Configured default trace level: **0** (STATUS)

CG

Configured default trace level: n/a

CMGMT

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status Output (0) Detailed Information (9) for CLI Actions
Please only use this trace component following consultation with Development!

CNQ

Configured default trace level: 3

Trace level **0**: ISDN trace

Trace level **1**:ISDN trace with data

Trace level **2**:Transport container trace

Trace level **3**:Trace of all parameters including the transport container

Trace level **4**:TMT trace

Trace level **5**:TMT trace and ISDN trace

Trace level **6**:TMT trace and ISDN trace with data

Trace level **7**:TMT-TMT trace and transport container

Trace level **8**:TMT-TMT trace and all parameters including the transport container

Trace level **9**:TMT-TMT trace and all parameters including the transport container and ASN.1 trace

CNQIWK

Configured default trace level: **3**

Trace level **0** - 9 see *CNQ*

COMMUNITIES

Configured default trace level: **0** (STATUS)

Trace level **6** (INTRA): Adding, deleting, modifying read, write or trap communities for SNMP. Receipt of SNMP trap destinations with automatic search.

CPMSG

Configured default trace level: **0** (STATUS)

CPUTRACE

Configured default trace level: **0** (STATUS)

CTS

Configured default trace level: **0** (STATUS)

DELIC_DRIVER

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the DELIC driver (SWC). For developers only.

DEVMGR

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Shows CP interface functions for connection setup and connection errors.

DISPATCH

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Listing of header data for all messages sent via the dispatcher. This impacts the system performance. The setting is preferred in order to get an idea of all messages sent via the dispatcher.

Trace level **6** (INTRA): This impacts the system performance quite significantly. The setting should only be used in order to get message details.

Trace level **6/9** (INTRA/DETAIL): Problems with the logical message queue (see comments above). Incorrectly coded component message handling, internal software problems: - Message not unregistered (incorrect RecvListType), - Message not registered (incorrect RecvListType), - Posting of message unsuccessful (incorrect RecvListType), - Sending of message unsuccessful (incorrect RecvListType), - Unregistered posting of message, - Unregistered sending of message.

DLSC

Configured default trace level: **0** (STATUS)

DMC

Configured default trace level: **0** (STATUS)

DSP

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used

Trace level 3-**9** : Messages output from the DSP and displayed by the DSB driver.

DSP_TRACE

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used

DSS1

Configured default trace level: **3**

Trace level **0** - 9 see *CNQ*

EMAIL_MANAGER

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Information on mail dispatch and connections to the mail server.

EMIWK

Configured default trace level: **0** (STATUS)

EVTLOG

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Make sure that events are also visible on the console / in the trace log / via LAN trace.

Trace level **6** (INTRA): Mutex blocking situations.

EVTLOGTRAP

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Activation/deactivation of a trace profile for a registered event.

FAXCONV_IF

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the CAPI interface actions of the fax converter. For developers only.

FAXCONV_LOGT

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Customer trace for displaying faulty fax transmissions.

FAXCONV_OS

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the OS interface actions of the fax converter. For developers only.

FAXCONV_T30DOWN

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the downstream interface actions of the fax converter T.30 module. For developers only.

FAXCONV_T30INT

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the actions of the fax converter T.30 module. For developers only.

FAXCONV_T30UP

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the upstream interface actions of the fax converter T.30 module. For developers only.

FAXCONVERTER

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the routines and data flow interface actions of the fax converter. For developers only.

FMSEM

Configured default trace level: **0** (STATUS)

GATEWAY

Configured default trace level: **0** (STATUS)

GWGLOBAL_DATA

Configured default trace level: **0** (STATUS)

GWGLOBAL_SI_DOWNL_PORTFUNC (HG 3500 only)

Configured default trace level: **3** (INTER)

Indicates if port/channel download data is received from the system interface containing information about the function type and the number of b channels for a port/channel.

GWSI (HG 3500 only)

Configured default trace level: **0** (STATUS)

H323

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): general information.

Trace level **3** (INTER): Receipt of dispatcher messages, admin recipients.

Trace level **6** (INTRA): Posting/sending of messages to other components.

Trace level **9** (DETAIL): Trace for function/parameter.

H323_EPT

Configured default trace level: **9** (DETAIL)

H323_GLOBAL_SI_DOWNLOADS

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Trace for download data.

H323_SPE

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): H.323 Protocol Manager: SPE 2 traces

Trace level 3 (INTER)

Trace level **6** (INTRA)

Trace level 9 (DETAIL)

H323IWK

Configured default trace level: **0** (STATUS)

H323MSG

Configured default trace level: **0** (STATUS)

H323STACK

Configured default trace level: 0 (STATUS)

HFAC (HG 3500 only)

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Status information about the HFAC component, component initialization.

Trace level **3** (INTER): Basic communication between the other components and the HFAC component, information about the basic-connected clients.

Trace level **6** (INTRA): Internal method calls and detailed information about the component.

Trace level **9** (DETAIL): Internal debugger information.

HSA_H225_CS

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): general information, H.323 stack API errors.

Trace level **3** (INTER): callbacks that caused a message to be sent to the H.323 Protocol Manager; stack API functions that triggered a LAN message.

Trace level **6** (INTRA): PVT use of the H.323 stack.

Trace level **9** (DETAIL): function/parameter trace.

HSA_H225_RAS

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): general information.

Trace level **3** (INTER): callbacks that caused a message to be sent to the H.323 Protocol Manager; stack API functions that triggered a LAN message.

Trace level **6** (INTRA): only used in exceptional situations.

Trace level **9** (DETAIL): function/parameter trace.

HSA_H245

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): general information.

Trace level **3** (INTER): callbacks that caused a message to be sent to the H.323 Protocol Manager; stack API functions that triggered a LAN message.

Trace level **6** (INTRA): callbacks that only collect parameter information.

Trace level **9** (DETAIL): function/parameter trace.

HSA_H323_NSD

Configured default trace level: **0** (STATUS)

Trace-Level **3** (INTER): No standard data traces.

Trace-Level **6** (INTRA):

HSA_RV_LOG

Configured default trace level: **6** (DETAIL)

Trace level **6** (INTRA): logging of RADVision stack traces.

HSA_SPE

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): H.323 stack adapter SPE2 traces

Trace level **3** (INTER)

Trace level 6 (INTRA)

Trace level 9 (DETAIL)

HSA_SYSTEM

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS), Trace level **3** (INTER), Trace level **6** (INTRA), Trace level **9** (DETAIL): Configuration and start issues as well as information not relating to the protocol.

ICC

Configured default trace level: **0** (STATUS)

IFTABLE

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Indicates errors.

Trace level **6** (INTRA): Indicates function calls with important parameters.

Trace level **9** (DETAIL): Not used.

IP_ROUTES

Configured default trace level: **0** (STATUS)

IPMONITOR

Configured default trace level: **0** (STATUS)

IPSTACK

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Error situation with IP accounting hash functions. For developers only.

IPSTACK_1LAN_IF

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Handling of configuration data.

IPSTACK_2LAN_IF

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Handling of configuration data.

IPSTACK_GLOBAL

Configured default trace level: **0** (STATUS)

IPSTACK_IPFILTER

Configured default trace level: **0** (STATUS)

IPSTACK_MACFILTER

Configured default trace level: **0** (STATUS)

IPSTACK_NAT

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Initialization.

Trace level **6** (INTRA): Detailed information about NAT processes.

Trace level **9** (DETAIL): Translated data.

IPSTACK_ROUTE

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Error situation with routing data.

IPSTACK_SNTPS

Configured default trace level: **0** (STATUS)

ISDN_FM

Configured default trace level: **3**

Trace level **3:** ISDN FM trace (default)

LAN

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): shows various normal operation procedures and errors.

Trace level **6** (INTRA): Displays interface functions with important parameters.

Trace level **9** (DETAIL): shows detailed information.

LICMGMT

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): not used

Trace level **3** (INTER): Messages received and sent via admin interface.

Trace level **6** (INTRA): Function terminations and results.

Trace level **9** (DETAIL): Other details.

LOCSERV

Configured default trace level: **0** (STATUS)

LOCSERV_CFG

Configured default trace level: **0** (STATUS)

LOCSERV_QUERY

Configured default trace level: **0** (STATUS)

LOCSERV_REG

Configured default trace level: **0** (STATUS)

LOG_MSG

Configured default trace level: **0** (STATUS)

LSDCL

Configured default trace level: n/a

LTUC

Configured default trace level: n/a

MANAGER

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Problems deleting, adding or changing manager objects.

MAT_STREAM

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used

Trace level 3-**9** : Internal messages from Materna storage management.

MCP

Configured default trace level: **0**

Trace level **0** (STATUS): Start and stop, errors received from other components.

Trace level **3** (INTER): Received/sent message or function entry, etc.

Trace level **6** (INTRA): Function-specific information.

Trace level **9** (DETAIL): Function-specific information with data.

MGAF_TBL

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Serious errors, for example missing parameters, invalid session ID, etc.

Trace level **3** (INTER): Status information on logins, logouts and connections.

Trace level **6** (INTRA): Detailed socket information.

MIKEY

Configured default trace level: **3** (INTER)

MMX (HG 3575 only)

Configured default trace level: **0** (STATUS)

MPH

Configured default trace level: **0** (STATUS)

MSC

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): API for Magic (function calls with parameters).

Trace level **3** (INTER): The input/output controls for the MSP are defined additionally.

Trace level **6** (INTRA): Tracking of internal MSC functions and handles/file descriptors.

Trace level **9** (DETAIL): Settings for configuration parameters (MSC, MSP/DSP) are defined. Detailed information on all MSC functions.

MSC_DSP

Configured default trace level: **0** (STATUS)

MSC_QM

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Detailed information on all MSC functions (only in RTCP context).

Trace level **3** (INTER): Information about quality surveillance

MSC_RTCP

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): General information on RTCP session, timer etc.

Trace level **3** (INTER): Callback function of MSP for RTCP events.

Trace level **6** (INTRA): Internal functions that were called during an RTCP session.

Trace level **9** (DETAIL): Detailed information on all MSC functions (though only in RTCP context).

MSC_SPECIFIC_STAT

Configured default trace level: **0** (STATUS)

MSC_TMT

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): MSC functions called by Magic are tracked.

Trace level **6** (INTRA): All input/output controls (interface to MSP) are tracked.

MSP_CAPI_IF

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used.

Trace level **3-9**: Internal messages from CAPI interface driver.

MSP_HDLC

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Detailed information on HDLC driver actions - only for developers.

MSP_PPP_IF

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used.

Trace level **3-9**: Internal messages from PPP interface driver.

MSP_RTP_MOD

Configured default trace level: **0** (STATUS)

NWRS

Configured default trace level: **0** (STATUS)

OAM

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Data flow from uploads and backup, export and upgrade actions (requires execution of the admin action).

Trace level **3** (INTER): Data flow of routing wizard actions (not relevant for HG 3500/3575).

Trace level **4**: Memory overrun information for all tasks.

Trace level **5**: Memory occupancy information for all tasks.

Trace level **5**: Execution of OAM threshold timer.

Trace level **6** (INTRA): Problems with OAM task queue (queue full, etc.).

Trace level **6** (INTRA): Problems when configuring SNTP time synchronization (not relevant for HG 3500/3575, moved to TIME_SYNC component).

OAM_ACTIONLIST

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Execution of automatic actions (garbage collection, gatekeeper switchback, etc.).

OSF_PCS

Configured default trace level: **3** (INTER)

PERFM_PL

Configured default trace level: **0** (STATUS)

PERFM_SIG

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Performance trace for signaling part.

PLATFORM

Configured default trace level: **0** (STATUS)

PORT

Configured default trace level: **0** (STATUS)

PORT_MGR

Configured default trace level: **0** (STATUS)

PPP_CC

Configured default trace level: **3** (INTER)

Trace level **0** (STATUS): Not used.

Trace level **3** (INTER): External interfaces for controlling PPP connections to other components, e.g. PPP Manager.

Trace level **6** (INTRA): External and internal PPP connection control interfaces.

Trace level **9** (DETAIL): External and internal interfaces as well as details of processes within PPP connection control.

PPP_STACK_DBG_IF

Configured default trace level: **0** (STATUS)

Trace level **6**-**9**: Other detailed information on call settings/connection cleardown.

Trace level **3** (INTER): PPP stack internal error messages.

PPP_STACK_PROC

Configured default trace level: **0** (STATUS)

Trace level **6**-**9**: PPP stack internal program flow.

Trace level **3** (INTER): Status of a PPP connection setup/cleardown.

PPPM_TBAS

Configured 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

Configured default trace level: **0** (STATUS)

Trace level **3**-**9**: Advanced information on internal processes in the PPP Manager.

PPPM_TSTD

Configured default trace level: **0** (STATUS)

Trace level **3**-**9**: Internal message flow of PPP Manager.

PPTP_DBG_IF

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used

Trace level 3-**9** : Internal error messages from PPTP for debugging.

PPTP_PROC

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Detailed information on MSC-specific quality data.

Trace level 3 (INTER): Information on setting up/clearing down calls at the PPP management interface.

Q931

Configured default trace level: **3**

Trace level **0** - 9 see *CNQ*

QDC

Configured default trace level: **0**

Trace level **0**: Status information on the QDC client; the traces are only displayed once.

- Information on starting/stopping the QDC client.
- Indicates if transmission to the QCU/NetMgr was started or interrupted.

Trace level **3**: Flowcharts and error messages at top level.

Trace level **6**: Flowcharts and traces are displayed when a function or class method is entered.

Trace level **9**: Detailed information about internal data and interface data.

- Buffer contents, for example QoS report from MSC/to QCU.
- Interface data

QDC_UDPPING

Configured default trace level: **0**

Trace level **0**: Status information about the QDC UDP ping. The traces are only displayed once:

1) Information on starting/stopping the QDC UDP ping.

2) • Indicates if the UDP listening task was started or interrupted.

Trace level **3**: Flowcharts and error messages at top level.

Trace level **6**: Flowcharts:

- Traces are displayed when a function or class method is entered.

Trace level **9**: Detailed information about internal data and interface data:

- Interface data

REMSURV

Configured default trace level: n/a

ROUTE98

Configured default trace level: **0** (STATUS)

RTPQM

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Trace for the function "Fallback to SCN".

Trace level **3** (INTER): Trace for the function "Fallback to SCN".

Trace level **6** (INTRA): Trace for the function "Fallback to SCN".

Trace level **9** (DETAIL): Trace for the function "Fallback to SCN".

SACCOB_DRV (HG 3500 only)

Configured default trace level: 0 (STATUS)

SCN

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Indicates different normal operational processes and errors.

Trace level **6** (INTRA): Indicates interface functions with important parameters.

Trace level **9** (DETAIL): Indicates detailed information.

SCNPAY

Configured default trace level: **0** (STATUS)

SDR

Configured default trace level: **0** (STATUS)

SECURE_TRACE

Configured default trace level: **0** (STATUS)

SECURITY_SVC

Configured default trace level: **0** (STATUS)

Trace level **0**: Fatal errors, for example missing parameters, invalid commands.

Trace level **3**: Status information and handling.

Trace level **6**: Detailed information, method calls.

SENDTMT

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Error sending or posting a message (extra info for TMT).

Trace level **3** (INTER): Receiving a message (extra info for TMT).

SENTA_API

Configured default trace level: **0**

Trace level **3** (INTER): An error has occurred.

Trace level **6** (INTRA): Functions and results exist.

Trace level **9** (DETAIL): Details.

SERVICE_TRACE

Configured default trace level: **0** (STATUS)

SESSION_MGMT

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Information on: GetUserInfo, SessionUpdate, SessionID-Verification

Trace level **6** (INTRA): Creation or verification of an admin session (only >= 2.1), updating of an admin session, deletion of an expired admin session, closing admin sessions, write authorization key/access handling (get/release).

Trace level **9** (DETAIL): Continuously updates admin session data with/without synchronization.

SI

Configured default trace level: **0** (STATUS)

SIP

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): SIP Protocol Manager: Status information trace Trace level **3** (INTER): Messages to other components Trace level **6** (INTRA): Messages after SSA Trace level **9** (DETAIL): All other actions

SIP_CFG

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Configuration data trace that can be accessed via WBM.

SIP_CFG_INT

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Internal configuration data trace.

SIP_FM

Configured default trace level: **3**

Trace level **0**: not used.

Trace level **3**: external interfaces of the SIP feature manager.

Trace level **6**: external and internal interfaces of the SIP feature manager.

Trace level **9**: external and internal interfaces and details of the processing method within the SIP feature manager.

SIP_GLOBAL_SI_DOWNLOADS

Configured default trace level: **0** (STATUS)

Trace level **9** (DETAIL): Trace for the system interface's download data.

SIP_HT

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): SIP for H.323 converter: SIP call signaling. Trace level **3** (INTER): Trace level **6** (INTRA): Trace level **9** (DETAIL):

SIP_REG

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): SIP stack adapter: REGISTER and OPTIONS Trace level **3** (INTER): Trace level **6** (INTRA): Trace level **9** (DETAIL):

SIP_SA

Configured 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

Configured default trace level: **0** (STATUS)

SIP_TRK_FM

Configured default trace level: **0** (STATUS)

SIU_STARTUP

Configured default trace level: n/a

SLMO_HFA

Configured default trace level: **0** (STATUS)

SMP

Configured default trace level: **0** (STATUS)

SNMP

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status output (0) detailed information (9) on the configuration data (via SNMP) and internal SNMP information and problems. Please only use this trace component following consultation with Development!

SPE_SVC

Configured default trace level: **0** (STATUS)

SPL

Configured default trace level: **0** (STATUS)

SS

Configured default trace level: **0** (STATUS)

SSL_UTIL

Configured default trace level: **0** (STATUS)

SSM

Configured default trace level: **0** (STATUS)

STACKTRACE

Configured default trace level: **0** (STATUS)

STATIC_ROUTES

Configured default trace level: **0** (STATUS)

STB (HG 3575 only)

Configured default trace level: **3** (INTER)

Trace level **0** (STATUS): Startup and shutdown; errors received from other components.

Trace level **3** (INTER): Received and sent messages, etc.

Trace level **6** (INTRA): Function-specific information.

Trace level **9** (DETAIL): Function-specific information with data.

STRC

Configured default trace level: **0** (STATUS)

STREAMS

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Not used

Trace level 3-**9**: Internal messages from streams storage management.

SWCONF

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Serious errors, for example missing parameters, invalid commands, etc.

Trace level **3** (INTER): Status information on job handling and process.

Trace level **6** (INTRA): Detailed information on all types of jobs, for example HTTP file transfers, MGAF, etc.

SYSTEM

Configured default trace level: **3** (INTER)

Trace level **3** (INTER): Always on; global system information (do not change!).

T90

Configured default trace level: **0** (STATUS)

Trace level **0**-**9**: Status information up to detailed information on the actions of the T.90 protocol. For developers only.

TC (HG 3500 only)

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Status information about the TC component, component initialization.

Trace level **3** (INTER): Basic communication between other components and the TC component.

Trace level **6** (INTRA): Internal method calls and detailed information about the component.

Trace level **9** (DETAIL): Internal debugger information.

TCP_IP_CONF (HG 3575 only)

Configured default trace level: **0** (STATUS)

TCPMOT_WT (HG 3575 only)

Configured default trace level: **0** (STATUS)

TCPSIG (HG 3575 only)

Configured default trace level: **0** (STATUS)

TCPSIG_WT (HG 3575 only)

Configured default trace level: **0** (STATUS)

TCPSUV (HG 3575 only)

Configured default trace level: **0** (STATUS)

TCPSUV_WT (HG 3575 only)

Configured default trace level: **0** (STATUS)

TESTLW

Configured default trace level: **0** (STATUS)

Trace level **0**-9: Detailed information on TESTLW actions - only for developers.

TIME_SYNC

Configured default trace level: **0** (STATUS)

Trace level **6** (INTRA): Problems when configuring SNTP time synchronization (not relevant for HG 3500/3575).

TIME_SYNCH_TASK (HG 3575 only)

Configured default trace level: **0** (STATUS)

TOOLS

Configured default trace level: **0** (STATUS)

Trace level **6** (INTRA): End of a thread in class *OSThread*.

TRAP

Configured default trace level: **0** (STATUS)

Trace level **3** (INTER): Important status information (IP address and port trap, SNMP trap version). Serious error receiving traps.

Trace level **6** (INTRA): Status information such as: - Receive trap OK, - Trap received from localhost or woanders, - Error information. Addition of a trap to the trap memory and deletion of a trap from the trap memory.

Trace level **9** (DETAIL): Detailed information.

TSA (HG 3500 only)

Configured default trace level: **0** (STATUS)

Trace level **0** (STATUS): Status information about the TSA component, component initialization.

Trace level **3** (INTER): Basic communication between other components and the TSA component.

Trace level **6** (INTRA): Internal method calls and detailed information about the component.

Trace level **9** (DETAIL): Internal debugger information.

WAN

Configured default trace level: **0** (STATUS)

WEBAPPL

Configured default trace level: **0** (STATUS)

Trace level **3/6** (INTER/INTRA): Input/output of important Web application functions and methods (for developers).

WEBSERVER

Configured default trace level: **0** (STATUS)

Trace level **6** (INTRA): Input/output of important Web server functions and methods (for developers).

WEBSERVER_STATISTIC

Configured default trace level: **0** (STATUS)

WEBSRV_CLIENT_IF

Configured default trace level: **0** (STATUS)

Trace level **1**: Trace of all URLS and URIs requested by a HTTP client (usually a browser). Only the name of the URI is output.

Trace level **3** (INTER): HTTP socket trace (without poll requests). HTTP data including the HTTP stack is output as sent from the browser. HTTP data including the HTTP stack's dynamic pages (XML) is output as sent to the browser.

Trace level **4**: As level 3, though additionally with poll requests.

Trace level **6** (INTRA): HTTP socket trace (without poll requests). HTTP data including the HTTP stack is output as sent from the browser. HTTP data including the HTTP stack's dynamic pages (XML) and generated/static pages (HTML) are output as sent to the browser.

WEBSRV_SYS_IF

Configured default trace level: **0** (STATUS)

Trace level **2**: Caution: This trace does not contain any trace information for poll requests. Data sent from and to the gatekeeper (gateway detection, automatic locating).

Trace level **3** (INTER): Administration interface trace. Data sent to the administration interface and XML data received from the administration interface.

Trace level **6** (INTRA): User and password information.

Trace level **9** (DETAIL): Login data sent to the administration interface, response sent to a client as well as internal parameter table information.

X25

Configured default trace level: **0** (STATUS)

Trace level **0**-**9**: Status information up to detailed information on the actions of the X.25 protocol. For developers only.

X75

Configured default trace level: **0** (STATUS)

Trace level **0-9**: Status information up to detailed information on the actions of the X.75 protocol. For developers only.

XMLUTILS

Configured default trace level: **0** (STATUS)

9.1.2 Trace Profiles

9.1.2.1 Profiles under Normal/Heavy Load

NOTICE: These profiles load the system in only a minor way and can therefore be started under normal/heavy load.

Overview of Profiles under Normal/Heavy Load
"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"
"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."

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - SIP, Level 9
  - SIP_REG, Level 9
  - SIP_SA, Level 9

"1.1.2(normal) SIP Trk. General problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - CNQ, Level 0
  - DSS1, Level 0
  - SIP, Level 9
  - SIP_SA, Level 9

"1.1.3(normal) SIP Trk. Payload problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - CNQ, Level 0
  - DSS1, Level 0
  - SIP, Level 9
  - SIP_SA, Level 9

"1.2.2(normal) SIP Sub. Payload problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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."

- Category: Can be activated under normal/heavy load.
- Additional: The following should also be activated:
  - A LAN trace (e.g. Wireshark)
  - The secure trace, to generate trace beacons for the LAN trace.
- Included trace components and assigned trace level:
  - DEVMGR, Level 9

"2.1.1(normal) H.323 Trk. General problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - CNQ, Level 0
  - DSS1, Level 0
  - HSA_SYSTEM, Level 1

"2.1.2(normal) H.323 Trk. Payload problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - HFAC, Level 6
  - SLMO_HFA, Level 6
  - TC, Level 6

"2.2.2(normal) HFA General problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.

- Included trace components and assigned trace level:
  - H323, Level 9
  - HSA_SYSTEM, Level 1
  - TSA, Level 9

"2.2.3(normal) HFA Payload problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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."

- Category: Can be activated under normal/heavy load.
- Additional: The following should also be activated:
  - A LAN trace (e.g. Wireshark)
  - The secure trace, to generate trace beacons for the LAN trace.
- Included trace components and assigned trace level:
  - HSA_SPE, Level 3

"3.1(normal) IPDA General problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - MPH, Level 3
  - MSC, Level 0

"3.2(normal) IPDA Payload problems"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: Can be activated under normal/heavy load.
- Additional: A LAN trace (e.g. Wireshark) should also be activated.

- Included trace components and assigned 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)"

- Category: Can be activated under normal/heavy load.
- Additional: The following should be carried out:
  - Activate a LAN trace (e.g. Wireshark)
  - Call "arpShow" and "mRouteShow" in the command shell
- Included trace components and assigned trace level:
  - MSC, Level 6
  - MSP_HDLC, Level 9

9.1.2.2 Profiles under Light Load

NOTICE: These profiles cause a heavy load on the system and must therefore only be started under light load!

Overview of Profiles under Light Load
"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"
"2.1.3(detail) H.323 Trk. Fax problems"
"2.2.1(detail) HFA Registration"
"2.2.2(detail) HFA General problems"

Overview of Profiles under Light Load
"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 problems"

"1.1.1(detail) SIP Reg. for Sub. and Trk."

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - SIP, Level 9
  - SIP_REG, Level 9
  - SIP_SA, Level 9

"1.1.2(detail) SIP Trk. General problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.

- Included trace components and assigned 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."

- Category: May only be activated under light load!
- Additional: The following should also be activated:
  - A LAN trace (e.g. Wireshark)
  - The secure trace, to generate trace beacons for the LAN trace.
- Included trace components and assigned trace level:
  - DEVMGR, Level 9

"2.1.1(detail) H.323 Trk. General problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.

- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - HFAC, Level 6
  - SLMO_HFA, Level 6
  - TC, Level 6

"2.2.2(detail) HFA General problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - H323, Level 9
  - HSA_SYSTEM, Level 1
  - TSA, Level 9

"2.2.3(detail) HFA Payload problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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."

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Additional: The following should also be activated:
  - A LAN trace (e.g. Wireshark)
  - The secure trace, to generate trace beacons for the LAN trace.
- Included trace components and assigned trace level:
  - DEVMGR, Level 9
  - H323_SPE, Level 9
  - HSA_SPE, Level 6

"3.1(detail) IPDA General problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned trace level:
  - ICC, Level 9
  - MCP, Level 9
  - MPH, Level 9
  - MSC, Level 9

"3.2(detail) IPDA Payload problems"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.
- Included trace components and assigned 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"

- Category: May only be activated under light load!
- Additional: A LAN trace (e.g. Wireshark) should also be activated.

- Included trace components and assigned 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)"

- Category: May only be activated under light load!
- Additional: The following should be carried out:
  - Activate a LAN trace (e.g. Wireshark)
  - Call "arpShow" and "mRouteShow" in the command shell
- Included trace components and assigned trace level:
  - MSC, Level 6
  - MSP_HDLC, Level 9

"4.2(detail) Signaling survivability problems"

- Category: May only be activated under light load!

"4.4(detail) NCUI reboots after TCP timeout"

- Category: May only be activated under light load!

9.2 Events

The sections below reflect the content of the original event templates.

An event type is assigned to each event. The following event types are available:

- **Information:** status message only, not an error message.
- **Warning:** message indicating a procedure or status that may be problematic; not an error message.
- **Minor:** error message. However, the error is not causing problems.
- **Major:** error message. This error could cause problems.
- **Critical:** error message. This error causes problems.
- **Cleared:** error message. The error has already been cleared by the system.
- **Indeterminate:** error message. The exact cause of the error cannot be established.

The descriptions contain the following information about each event:

- the event code,
- the message text in the log entry or at the user interface,
- the event type (see above),
- clarification of the causes, system responses and, if applicable, possible troubleshooting measures.

Some message texts (event texts) contain variable data. These are indicated as follows:

- %s means: character string
- %d and %I mean: positive decimal number
- %u means: positive or negative decimal number
- %f means: floating point number
- %p means: pointer (memory address)
- %x means: hexadecimal number (using lowercase letters)
- %X means: hexadecimal number (using uppercase letters)
- %c means: single character

9.2.1 Overview: Event Codes

The table is intended to help you find specific status and error messages faster. It has been sorted alphabetically according event codes. Since all event codes begin with MSG_, sorting effectively starts with the 5th character.

Event Code	Section
ASSERTION_FAILED_EVENT	9.2.3, "Reboot Events"
CCE_GENERAL_ERROR	9.2.49, "LAN Signaling Events - CCE"
CCE_PSS_STORE_ERROR	9.2.49, "LAN Signaling Events - CCE"
COMGA_NOK_UPGRADE_REG	9.2.2, "Status Events"
EXIT_REBOOT_EVENT	9.2.3, "Reboot Events"
FP_EVT_CRITICAL	9.2.3, "Reboot Events"
FP_EVT_INDETERMINATE	9.2.2, "Status Events"
FP_EVT_MAJOR	9.2.3, "Reboot Events"
FP_EVT_MINOR	9.2.2, "Status Events"
FP_EVT_SNMP_TRAP	9.2.2, "Status Events"
FP_EVT_INFORMATION	9.2.2, "Status Events"
FP_EVT_TRACE_START	9.2.2, "Status Events"
FP_EVT_TRACE_STOP	9.2.2, "Status Events"
FP_EVT_WARNING	9.2.3, "Reboot Events"
FW_NOK_UPGRADE_REG	9.2.2, "Status Events"
H323_NO_IP	9.2.8, "H.323 Events"
H323_SNMP_TRAP	9.2.8, "H.323 Events"
MSG_ADMIN_DIDN'T_GET_WRITE_ACCESS	9.2.29, "OAM Events"
MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS	9.2.29, "OAM Events"

Event Code	Section
MSG_ADMIN_GOT_WRITE_ACCESS	9.2.29, "OAM Events"
MSG_ADMIN_INVALID_LOGIN	9.2.29, "OAM Events"
MSG_ADMIN_LOGGED_IN	9.2.29, "OAM Events"
MSG_ADMIN_LOGGED_OUT	9.2.29, "OAM Events"
MSG_ADMIN_REBOOT	9.2.3, "Reboot Events"
MSG_ADMIN_RELEASED_WRITE_ACCESS	9.2.29, "OAM Events"
MSG_ADMIN_SESSION_CREATED	9.2.29, "OAM Events"
MSG_ADMIN_SESSION_EXPIRED	9.2.29, "OAM Events"
MSG_ASC_ERROR	9.2.35, "Major ASC Events"
MSG_ASP_ERROR	9.2.36, "Major ASP Events"
MSG_ASP_INFO	9.2.34, "Important Platform Software Status Events"
MSG_ASP_INFO	9.2.37, "Minor ASP Events"
MSG_ASP_REBOOT	9.2.3, "Reboot Events"
MSG_BSD44_ACCEPT_DGW_ERR	9.2.12, "DGW Events"
MSG_BSD44_ACCEPT_ERROR	9.2.23, "VCAPI Events"
MSG_BSD44_DGW_BIND_FAIL	9.2.12, "DGW Events"
MSG_BSD44_DGW_CONNECT_FAIL	9.2.12, "DGW Events"
MSG_BSD44_DGW_NO_LIST	9.2.12, "DGW Events"
MSG_BSD44_DGW_SOCKET_FAIL	9.2.12, "DGW Events"
MSG_BSD44_SELECT_ERROR	9.2.23, "VCAPI Events"
MSG_BSD44_VCAPI_NO_LIST	9.2.12, "DGW Events"
MSG_CAR_ALIVE_IP_CONNECTION_LOST	9.2.13, "CAR Events"
MSG_CAR_ALIVE_IP_CONNECTION_LOST	9.2.13, "CAR Events"
MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN	9.2.13, "CAR Events"
MSG_CAR_CALL_ADDR_REJECTED	9.2.29, "OAM Events"
MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB	9.2.13, "CAR Events"
MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS	9.2.13, "CAR Events"
MSG_CAR_CODEC_ENTRY_DELETED	9.2.13, "CAR Events"
MSG_CAR_CODECS_INCONSISTENT	9.2.13, "CAR Events"

Event Code	Section
MSG_CAR_DB_READ_NODE_TABLE_ERROR	9.2.13, "CAR Events"
MSG_CAR_DBF_SERVER_INCONSISTENT	9.2.13, "CAR Events"
MSG_CAR_DBFS_POSS_CONFLICT	9.2.13, "CAR Events"
MSG_CAR_ERROR_WITH_OAM_INTERFACE	9.2.13, "CAR Events"
MSG_CAR_FKT_GET_IPADR_FAILED	9.2.13, "CAR Events"
MSG_CAR_GENERAL_ERROR	9.2.13, "CAR Events"
MSG_CAR_MALLOC_FAILED	9.2.4, "Resource Monitoring Events"
MSG_CAR_NO_FREE_CODEC_TAB_ELE	9.2.13, "CAR Events"
MSG_CAR_NO_MAC_ADDRESS	9.2.13, "CAR Events"
MSG_CAR_NO_MEMORY	9.2.13, "CAR Events"
MSG_CAR_NODE_INFO_ALREADY_AVAILABLE	9.2.13, "CAR Events"
MSG_CAR_PARAM_NOT_FOUND	9.2.13, "CAR Events"
MSG_CAR_SENDING_UPDATE_REQUEST_-FAILED_NO_MEMORY	9.2.13, "CAR Events"
MSG_CAR_SENDING_UPDATE_REQUEST_-FAILED_SOH_ERROR	9.2.13, "CAR Events"
MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS	9.2.13, "CAR Events"
MSG_CAR_START_TCP_LISTENER_FAILED	9.2.13, "CAR Events"
MSG_CAR_UNAUTHORIZED_IP_ACCESS	9.2.13, "CAR Events"
MSG_CAR_UNEXPECTED_DATA_RECV	9.2.13, "CAR Events"
MSG_CAR_UNEXPECTED_MSG_RECV	9.2.13, "CAR Events"
MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CAU-LADDRTAB_TOO_BIG	9.2.13, "CAR Events"
MSG_CAR_WRONG_EVENT	9.2.13, "CAR Events"
MSG_CAR_WRONG_IP_ADDRESS	9.2.13, "CAR Events"
MSG_CAR_WRONG_LENGTH	9.2.13, "CAR Events"
MSG_CAR_WRONG_NODE_ID	9.2.13, "CAR Events"
MSG_CAR_WRONG_SERVICE	9.2.13, "CAR Events"
MSG_CAT_H235	9.2.9, "H.235 Events"
MSG_CAT_H323_REBOOT	9.2.3, "Reboot Events"

Event Code	Section
MSG_CAT_HSA_REBOOT	9.2.2, "Status Events"
MSG_CAT_NWRS	9.2.5, "Routing Events"
MSG_CLI_LOGGED_IN_FROM_TELNET	9.2.30, "CLI Events"
MSG_CLI_LOGGED_IN_FROM_V24	9.2.30, "CLI Events"
MSG_CLI_TELNET_ABORTED	9.2.30, "CLI Events"
MSG_DELIC_ERROR	9.2.41, "DELIC Events"
MSG_DEVM_BINDING_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CLOSE_LEG_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CONNECT_LEGS_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CONNECT_WRONG_LEGS	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CONNECT_WRONG_RES_STATE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_CREATE_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_DEVICEID_OUT_OF_RANGE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_DISCONNECT_LEGS_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_INTERROR_CHNID	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_INTERROR_DEVID	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_INTERROR_RESID	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_LAYER2_SERVICE_TRAP	9.2.33, "MAGIC/Device Manager Events"

Event Code	Section
MSG_DEVMGR_LISTEN_WRONG_RES_STATE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_MSCERROR_RESID	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_OPEN_LEG_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_OPEN_WRONG_RES_STATE	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_SCN_TASK_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DEVMGR_UPDATE_LEG_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_DGW_ABORT_SOCK_UNKN	9.2.12, "DGW Events"
MSG_DGW_ACCEPT_FAILED	9.2.12, "DGW Events"
MSG_DGW_ALLOC_CHN_CONN_FAIL	9.2.12, "DGW Events"
MSG_DGW_ALLOC_CHN_RUN_OUT	9.2.12, "DGW Events"
MSG_DGW_ALLOC_CONF_ERR	9.2.12, "DGW Events"
MSG_DGW_ALLOC_DISC_B3	9.2.12, "DGW Events"
MSG_DGW_ALLOC_REQ_ERR	9.2.12, "DGW Events"
MSG_DGW_BUFAVAIL_SOCK_UNKN	9.2.12, "DGW Events"
MSG_DGW_CONF_ALLOC_ERR	9.2.12, "DGW Events"
MSG_DGW_CONN_B3_ACT_IND	9.2.12, "DGW Events"
MSG_DGW_CONN_COMPL_ALLOC	9.2.12, "DGW Events"
MSG_DGW_CONN_OUT_OF_RANGE	9.2.12, "DGW Events"
MSG_DGW_CONN_RUN_OUT	9.2.12, "DGW Events"
MSG_DGW_CONNECT_FAILED	9.2.12, "DGW Events"
MSG_DGW_DATA_B3_ALLOC_ERR	9.2.12, "DGW Events"
MSG_DGW_DISC_B3_IND	9.2.12, "DGW Events"
MSG_DGW_DISC_B3_NOT_SEND	9.2.12, "DGW Events"

Event Code	Section
MSG_DGW_FREE_ALLOC_ERR	9.2.12, "DGW Events"
MSG_DGW_FREE_CHN_ALLOC_FAIL	9.2.12, "DGW Events"
MSG_DGW_FREE_NOT_SEND	9.2.12, "DGW Events"
MSG_DGW_FREE_UNKNOWN_ID	9.2.12, "DGW Events"
MSG_DGW_IND_ALLOC_ERR	9.2.12, "DGW Events"
MSG_DGW_INV_DATA_LEN	9.2.12, "DGW Events"
MSG_DGW_INV_MSG_LEN	9.2.12, "DGW Events"
MSG_DGW_INVALID_LENGTH	9.2.12, "DGW Events"
MSG_DGW_LISTENING_ERR	9.2.12, "DGW Events"
MSG_DGW_MGR_NOT_READY	9.2.12, "DGW Events"
MSG_DGW_MSG_IGNORED	9.2.12, "DGW Events"
MSG_DGW_MSG_RCV_FAIL	9.2.12, "DGW Events"
MSG_DGW_NO_PLCI	9.2.12, "DGW Events"
MSG_DGW_OPEN_CHN_ALLOC_FAIL	9.2.12, "DGW Events"
MSG_DGW_OPEN_CHN_UNKNOWN_ID	9.2.12, "DGW Events"
MSG_DGW_OPEN_CHN_WRONG	9.2.12, "DGW Events"
MSG_DGW_RCV_ALLOC_FAIL	9.2.12, "DGW Events"
MSG_DGW_RCV_FAILED	9.2.12, "DGW Events"
MSG_DGW_RCV_SOCK_UNKN	9.2.12, "DGW Events"
MSG_DGW_RECEIVE_ERR	9.2.12, "DGW Events"
MSG_DGW_SEC_ALLOC_FAIL	9.2.12, "DGW Events"
MSG_DGW_SEND_DATA_ERR	9.2.12, "DGW Events"
MSG_DGW_SEND_FAILED	9.2.12, "DGW Events"
MSG_DGW_SOCKET_BIND_ERR	9.2.12, "DGW Events"
MSG_DGW_SOCKET_NOT_OPEN	9.2.12, "DGW Events"
MSG_DGW_SOCKET_UNKNOWN	9.2.12, "DGW Events"
MSG_DGW_UNH_MSG_CAPI20_MGR	9.2.12, "DGW Events"
MSG_DGW_UNHANDLED_EVENT	9.2.12, "DGW Events"
MSG_DGW_UNHANDLED_MSG	9.2.12, "DGW Events"

Event Code	Section
MSG_DGW_UNKNOWN_ID_CHANNEL	9.2.12, "DGW Events"
MSG_DGW_UNKNOWN_NOTIFIC	9.2.12, "DGW Events"
MSG_DGW_UNKNOWN_PRIMITIVE	9.2.12, "DGW Events"
MSG_DGW_WRONG_EVENT_CAPI	9.2.12, "DGW Events"
MSG_DGW_WRONG_EVENT_CAPI20	9.2.12, "DGW Events"
MSG_DGW_WRONG_STATE	9.2.12, "DGW Events"
MSG_DLSC_BOOTSTRAP_OK	9.2.2, "Status Events"
MSG_DISP_SENDER_NOT_SET	9.2.29, "OAM Events"
MSG_ERH_ADMISSION_ERROR	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_ERROR	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_INFORMATION	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_NO_LICENSE	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_REGISTRATION_ERROR	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_SECURITY_DENIAL	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_ERH_SUB_OUT_OF_SERVICE	9.2.45, "Endpoint Registration Handler (ERH) Trace Events"
MSG_EXCEPTION_REBOOT	9.2.3, "Reboot Events"
MSG_FAXCONV_ERROR	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_FIREWALL_ALARM	9.2.2, "Status Events"
MSG_FAXCONV_INFO	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_GSA_SNMP	9.2.11, "GSA Events"

Event Code	Section
MSG_GW_OBJ_ALLOC_FAILED	9.2.3, "Reboot Events"
MSG_GW_OBJ_MEMORY_EXHAUSTED	9.2.3, "Reboot Events"
MSG_GW_OBJ_MEMORY_INCONSISTENT	9.2.3, "Reboot Events"
MSG_GW_SUCCESSFULLY_STARTED	9.2.2, "Status Events"
MSG_H323_INFORMATION	9.2.8, "H.323 Events"
MSG_H323_INVALID_CONFIGURATION	9.2.8, "H.323 Events"
MSG_H323_INVALID_PARAMETER_VALUE	9.2.8, "H.323 Events"
MSG_H323_INVALID_POINTER	9.2.8, "H.323 Events"
MSG_H323_LOGIC_ERROR	9.2.8, "H.323 Events"
MSG_H323_MISSING_PARAMETER	9.2.8, "H.323 Events"
MSG_H323_OSCAR_NSD_ERROR	9.2.8, "H.323 Events"
MSG_H323_PROTOCOL_ERROR	9.2.8, "H.323 Events"
MSG_H323_SNMP_TRAP	9.2.8, "H.323 Events"
MSG_H323_STACK_ERROR	9.2.8, "H.323 Events"
MSG_H323_UNEXPECTED_MESSAGE	9.2.8, "H.323 Events"
MSG_H323_UNEXPECTED_RETURN_VALUE	9.2.8, "H.323 Events"
MSG_H323CLIENT_INVALID_ADMIN_MSG	9.2.25, "H.323 Client Events"
MSG_H323CLIENT_INVALID_CLIENTID	9.2.25, "H.323 Client Events"
MSG_H323CLIENT_INVALID_PARAM	9.2.25, "H.323 Client Events"
MSG_H323CLIENT_MAPS_DIFFER	9.2.25, "H.323 Client Events"
MSG_H323CLIENT_NWRS_ENTRY_FAILED	9.2.25, "H.323 Client Events"
MSG_HBR_WARNING	9.2.2, "Status Events"
MSG_HACKER_ON_SNMP_PORT_TRAP	9.2.4, "Resource Monitoring Events"
MSG_HFAA_INTERNAL_ERROR	9.2.18, "HFA Adapter Events"
MSG_HFAA_INTERNAL_EVENT	9.2.18, "HFA Adapter Events"

Event Code	Section
MSG_HFAA_MEMORY_ERROR	9.2.18, "HFA Adapter Events"
MSG_HFAA_MESSAGE_ERROR	9.2.18, "HFA Adapter Events"
MSG_HFAA_PARAM_ERROR	9.2.18, "HFA Adapter Events"
MSG_HFAM_HAH_ALLOC_CHAN_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_HAH_ALLOC_CONF_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_ALGORITM_OBJID_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_BIND_REGISOCK_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_CREATE_REGISOCK_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_IPADR_TOO_LONG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_LISTEN_REGISOCK_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_MAX_CON_EXCEED_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_PROTOCOL_LIST_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_RETURNED_SOCKET_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR	9.2.17, "HFA Manager Events"

Event Code	Section
MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_LIH_UNEXP_CORNET_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_MAIN_ILLEG_PORTNO_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_MAIN_NO_LOGONTIMER_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_MON_NO_MON_TIMER_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_ESTAB_NOTREG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_INVAL_PWD_LEN_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_LOGIN_NOTREG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_LOGON_REJECT_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_MISSING_L2INFO_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_RELIN_NOTREG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_REG_SUBNO_TOO_LONG_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_SIH_CORNET_LONGER_28_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR	9.2.17, "HFA Manager Events"
MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR	9.2.17, "HFA Manager Events"
MSG_HIP_ALLOC_DEV_OBJ	9.2.31, "HIP Events"
MSG_HIP_ALLOC_MES_SI	9.2.31, "HIP Events"
MSG_HIP_NO_CLBLK	9.2.31, "HIP Events"

Event Code	Section
MSG_HIP_NO_CLPOOL_ID	9.2.31, "HIP Events"
MSG_HIP_NO_CLUSTER	9.2.31, "HIP Events"
MSG_HIP_NO_DEVLOAD	9.2.31, "HIP Events"
MSG_HIP_NO_DEVSTART	9.2.31, "HIP Events"
MSG_HIP_NO_MEM_CL	9.2.31, "HIP Events"
MSG_HIP_NO_MEM_CLBLK	9.2.31, "HIP Events"
MSG_HIP_NO_MEM_TO_SI	9.2.31, "HIP Events"
MSG_HIP_NO_NETPOOL_INIT	9.2.31, "HIP Events"
MSG_HIP_NO_OBJ_INIT	9.2.31, "HIP Events"
MSG_HIP_NO_PMBLK	9.2.31, "HIP Events"
MSG_HIP_PKTLEN_ZERO	9.2.31, "HIP Events"
MSG_HIP_PMBLK_ZERO	9.2.31, "HIP Events"
MSG_IP_LINK_FAILURE	9.2.4, "Resource Monitoring Events"
MSG_IP_LINK2_FAILURE	9.2.4, "Resource Monitoring Events"
MSG_IP_LINK_RESTORE	9.2.4, "Resource Monitoring Events"
MSG_IP_LINK2_RESTORE	9.2.4, "Resource Monitoring Events"
MSG_IP_LINK_SWITCHOVER	9.2.4, "Resource Monitoring Events"
MSG_IP_LINK2_SWITCHOVER	9.2.4, "Resource Monitoring Events"
MSG_IP_RTP_QUALITY_FAILURE	9.2.10, "RTPQM Events"
MSG_IP_RTP_QUALITY_WARNING	9.2.10, "RTPQM Events"
MSG_IPACCSRV_INTERNAL_ERROR	9.2.44, "IP Accounting Events"
MSG_IPACCSRV_LOGON	9.2.44, "IP Accounting Events"
MSG_IPACCSRV_MARK_REACHED	9.2.44, "IP Accounting Events"
MSG_IPACCSRV_MEMORY_ERROR	9.2.44, "IP Accounting Events"

Event Code	Section
MSG_IPACCSRV_MESSAGE_ERROR	9.2.44, "IP Accounting Events"
MSG_IPACCSRV_OVERFLOW	9.2.44, "IP Accounting Events"
MSG_IPACCSRV_SOCKET_ERROR	9.2.44, "IP Accounting Events"
MSG_IPF_ON_OFF	9.2.38, "IP Filter Events"
MSG_IPF_PARAMETER	9.2.38, "IP Filter Events"
MSG_IPF_STARTED	9.2.38, "IP Filter Events"
MSG_IPF_STOPPED	9.2.38, "IP Filter Events"
MSG_IPNC_CP_ASYNCH	9.2.26, "IPNC Events"
MSG_IPNC_INCONSISTENT_STATE	9.2.26, "IPNC Events"
MSG_IPNC_INTERNAL_ERROR	9.2.26, "IPNC Events"
MSG_IPNC_MESSAGE_DUMP	9.2.26, "IPNC Events"
MSG_IPNC_MESSAGE_ERROR	9.2.26, "IPNC Events"
MSG_IPNC_PARAM_ERROR	9.2.26, "IPNC Events"
MSG_IPNCA_ERROR	9.2.27, "IPNCA Events"
MSG_IPNCV_INTERNAL_ERROR	9.2.2, "Status Events"
MSG_IPNCV_MEMORY_ERROR	9.2.4, "Resource Monitoring Events"
MSG_IPNCV_SIGNALING_ERROR	9.2.46, "IPNCV Events"
MSG_IPNCV_STARTUP_ERROR	9.2.2, "Status Events"
MSG_IPNCV_STARTUP_SHUTDOWN	9.2.2, "Status Events"
MSG_IPSEC_REBOOT	9.2.3, "Reboot Events"
MSG_IPSTACK_INVALID_PARAM	9.2.40, "IP Stack Events"
MSG_IPSTACK_NAT_ERROR	9.2.40, "IP Stack Events"
MSG_IPSTACK_SOH_ERROR	9.2.40, "IP Stack Events"
MSG_ISDN_CMR_ADD_OBJECT_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_DEVICE_PTR_BAD	9.2.7, "SCN Protocol Events"

Event Code	Section
MSG_ISDN_CMR_GEN_CALL_REF_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_GENRIC_EVENT	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_INIT_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MAND_FIELDS_MISSING	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MESSAGE_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MSG_DECODE_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MSG_ENCODE_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MSG_SEND_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_MSG_UNEXPECTED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_NEW_OBJECT_FAILED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_OBJECT_NOT_FOUND	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_PROTOCOL_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_SEG_MSG_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_SESSION_NOT_FOUND	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_STATUS_MSG_RECEIVED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_TIMER_EXPIRED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_UNEXPECTED_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_UNEXPECTED_EVENT	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_UNEXPECTED_VALUE	9.2.7, "SCN Protocol Events"

Event Code	Section
MSG_ISDN_CMR_UNH_STATE_EVENT	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_UNIMPLEMENTED	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_WRONG_DEVICE_TYPE	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_WRONG_INTERFACE	9.2.7, "SCN Protocol Events"
MSG_ISDN_CMR_WRONG_PROTVAR	9.2.7, "SCN Protocol Events"
MSG_ISDN_DEVICE_PTR_NOT_FOUND	9.2.7, "SCN Protocol Events"
MSG_ISDN_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_NO_ERROR	9.2.7, "SCN Protocol Events"
MSG_ISDN_NULL_PTR	9.2.7, "SCN Protocol Events"
MSG_ISDN_OVERLOAD_CONDITION	9.2.7, "SCN Protocol Events"
MSG_ISDN_RESOURCE_IN_USE_BY_O_CALL	9.2.7, "SCN Protocol Events"
MSG_ISDN_RESOURCE_NOT_AVAILABLE	9.2.7, "SCN Protocol Events"
MSG_ISDN_RESOURCE_NOT_IN_SERVICE	9.2.7, "SCN Protocol Events"
MSG_ISDN_START_UP	9.2.7, "SCN Protocol Events"
MSG_ISDN_START_UP_ERROR	9.2.7, "SCN Protocol Events"
MSG_LDAP_ENCODE_DECODE_ERROR	9.2.4, "Resource Monitoring Events"
MSG_LDAP_GENERAL_ERROR	9.2.4, "Resource Monitoring Events"
MSG_LDAP_IP_LINK_ERROR	9.2.4, "Resource Monitoring Events"
MSG_LDAP_MEMORY_ERROR	9.2.4, "Resource Monitoring Events"

Event Code	Section
MSG_LDAP_SOCKET_ERROR	9.2.4, "Resource Monitoring Events"
MSG_LDAP_SUCCESSFULLY_STARTED	9.2.2, "Status Events"
MSG_LLC_EVENT_INVALID_PARAMETER_VALUE	9.2.50, "Events for LLC Operation"
MSG_LLC_EVENT_MISSING_PARAMETER	9.2.50, "Events for LLC Operation"
MSG_LLC_EVENT_MISSING_RESOURCE	9.2.50, "Events for LLC Operation"
MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE	9.2.50, "Events for LLC Operation"
MSG_MAF_ETHERNET_HEADER	9.2.39, "MAC Filter Events"
MSG_MAF_NETBUFFER	9.2.39, "MAC Filter Events"
MSG_MAF_NO_OF_RULES	9.2.39, "MAC Filter Events"
MSG_MAF_ON_OFF	9.2.39, "MAC Filter Events"
MSG_MAF_PARAMETER	9.2.39, "MAC Filter Events"
MSG_MAF_STARTED	9.2.39, "MAC Filter Events"
MSG_MAF_STOPPED	9.2.39, "MAC Filter Events"
MSG_MAND_PARAM_MISSING	9.2.6, "Call Control and Feature Events"
MSG_MIKEY_REBOOT	9.2.3, "Reboot Events"
MSG_MPH_INFO	9.2.28, "MPH Events"
MSG_MSP_FAX_OVERLONG_PKT	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_MSP_HDLC_ERROR	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_MSP_HDLC_INFO	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_NU_CAR_FAILED	9.2.15, "NU Events"
MSG_NU_CAR_RESP_INVALID	9.2.15, "NU Events"
MSG_NU_DEV_TAB_NOT_FOUND	9.2.15, "NU Events"
MSG_NU_EVENT_EXCEPTION	9.2.15, "NU Events"
MSG_NU_FREE_CHN_COMF_TOO_LATE	9.2.15, "NU Events"

Event Code	Section
MSG_NU_FREE_CHN_UNEXPECTED	9.2.15, "NU Events"
MSG_NU_GENERAL_ERROR	9.2.15, "NU Events"
MSG_NU_INTERNAL_ERROR	9.2.15, "NU Events"
MSG_NU_INVALID_CIDL	9.2.15, "NU Events"
MSG_NU_IP_ERROR	9.2.15, "NU Events"
MSG_NU_NO_FREE_TRANSACTION	9.2.15, "NU Events"
MSG_NU_NO_PORT_DATA	9.2.15, "NU Events"
MSG_NU_SOH_RESP_INVALID	9.2.15, "NU Events"
MSG_NU_SUPERFLUOS_MSG	9.2.15, "NU Events"
MSG_NU_TCP_LISTENER_FAILED	9.2.15, "NU Events"
MSG_NU_TOO_MUCH_DIGITS	9.2.15, "NU Events"
MSG_NU_TRANSPCONT_MISSING	9.2.15, "NU Events"
MSG_NU_UNEXPECTED_MSG	9.2.15, "NU Events"
MSG_NU_UNEXPECTED_SETUP	9.2.15, "NU Events"
MSG_NU_UNEXPECTED_TIMER	9.2.15, "NU Events"
MSG_NU_UNKNOWN_MESSAGE	9.2.15, "NU Events"
MSG_NU_WRONG_CALL_REF	9.2.15, "NU Events"
MSG_NULC_INTERNAL_ERROR	9.2.16, "NU Leg Control Events"
MSG_NULC_INTERNAL_EVENT	9.2.16, "NU Leg Control Events"
MSG_NULC_MEMORY_ERROR	9.2.16, "NU Leg Control Events"
MSG_NULC_MESSAGE_ERROR	9.2.16, "NU Leg Control Events"
MSG_NULC_PARAM_ERROR	9.2.16, "NU Leg Control Events"
MSG_NWRS_DEVICE_NOT_FOUND	9.2.5, "Routing Events"
MSG_NWRS_DEVICE_TABLE_NOT_FOUND	9.2.5, "Routing Events"
MSG_NWRS_DPLN_ENTRY_INVALID	9.2.5, "Routing Events"
MSG_NWRS_DPLN_NOT_FOUND	9.2.5, "Routing Events"

Event Code	Section
MSG_NWRS_EMPTY_FIELD_ECHOED	9.2.5, "Routing Events"
MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE	9.2.5, "Routing Events"
MSG_NWRS_ODR_COMMAND_UNKNOWN	9.2.5, "Routing Events"
MSG_NWRS_ODR_NOT_FOUND	9.2.5, "Routing Events"
MSG_NWRS_ROUTE_NOT_FOUND	9.2.5, "Routing Events"
MSG_NWRS_UNKNOWN_FIELD_ECHOED	9.2.5, "Routing Events"
MSG_NWRS_UNSPEC_ERROR	9.2.5, "Routing Events"
MSG_OAM_DMA_RAM_THRESHOLD_REACHED	9.2.4, "Resource Monitoring Events"
MSG_OAM_OVERLOAD_REACHED	9.2.4, "Resource Monitoring Events"
MSG_OAM_OVERLOAD_CLEARED	9.2.4, "Resource Monitoring Events"
MSG_OAM_FAN_OUT_OF_SERVICE	9.2.4, "Resource Monitoring Events"
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION	9.2.4, "Resource Monitoring Events"
MSG_OAM_INTERNAL_EVENT	9.2.29, "OAM Events"
MSG_OAM_PRIO_INCREASED	9.2.29, "OAM Events"
MSG_OAM_PRIO_SWITCHED_BACK	9.2.29, "OAM Events"
MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE	9.2.4, "Resource Monitoring Events"
MSG_OAM_PUT_TO_QUEUE_FAILED	9.2.29, "OAM Events"
MSG_OAM_QUEUE_BLOCKED	9.2.29, "OAM Events"
MSG_OAM_QUEUE_FULL	9.2.29, "OAM Events"
MSG_OAM_RAM_THRESHOLD_REACHED	9.2.4, "Resource Monitoring Events"
MSG_OAM_THRESHOLD_REACHED	9.2.4, "Resource Monitoring Events"
MSG_OAM_TIMESYNC	9.2.29, "OAM Events"
MSG_OAM_TIMESYNC_FAILED	9.2.29, "OAM Events"
MSG_OS_EXCEPTION_ERROR	9.2.3, "Reboot Events"
MSG_ERH_NO_LICENSE	9.2.48, "Error Events"

Event Code	Section
MSG_OSF_PCS_EXCEPTION	9.2.3, "Reboot Events"
MSG_PPP_STACK_PROC	9.2.21, "PPP Stack Events"
MSG_PPP_STACK_REBOOT	9.2.3, "Reboot Events"
MSG_PS_INVALID_STREAM_FROM_ADDRESS	9.2.2, "Status Events"
MSG_PS_INVALID_STREAM_FROM_PORT	9.2.2, "Status Events"
MSG_PPTP_STACK_REBOOT	9.2.3, "Reboot Events"
MSG_PPPM_ERR_CONFIG	9.2.20, "PPP MANAGER Events"
MSG_PPPM_ERR_OPERATION	9.2.20, "PPP MANAGER Events"
MSG_REG_ERROR_FROM_SOH	9.2.14, "REG Events"
MSG_REG_GLOBAL_ERROR	9.2.14, "REG Events"
MSG_REG_NIL_PTR_FROM_SOH	9.2.14, "REG Events"
MSG_REG_NO_MEMORY	9.2.14, "REG Events"
MSG_REG_NO_REGISTRATION_POSSIBLE	9.2.14, "REG Events"
MSG_REG_REQUEST_WITHIN_REGISTRATION	9.2.14, "REG Events"
MSG_REG_SOH_SEND_DATA_FAILED	9.2.14, "REG Events"
MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH	9.2.14, "REG Events"
MSG_RESTORE_CFG_REBOOT	9.2.3, "Reboot Events"
MSG_SCN_ADD_PARAMETER_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_BIND_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_DEV_NOT_IN_DEVLIST	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_ERROR_12_MSG	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_GET_ADMMSG_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_GET_LDAPMSG_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_OPEN_STREAM_FAILED	9.2.33, "MAGIC/Device Manager Events"

Event Code	Section
MSG_SCN_OPERATION_ON_STREAM_FAILED	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_POLL_FD	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_UNEXPECTED_L2_MSG	9.2.33, "MAGIC/Device Manager Events"
MSG_SCN_UNEXPECTED_POLL_EVENT	9.2.33, "MAGIC/Device Manager Events"
MSG_SDR_INIT	9.2.6, "Call Control and Feature Events"
MSG_SDR_UNEXPECTED_EVENT	9.2.6, "Call Control and Feature Events"
MSG_SI_L2STUB_COUDNT_OPEN_STREAM	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_ERROR_INIT_DRIVER	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_NO_ALLOC	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_NO_CLONE	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_OPEN_OTHER_STREAM_NOT_POSSIBLE	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_PORT_NOT_OPEN	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_STREAM_ALREADY_OPEN	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_UNEXPECTED_DB_TYPE	9.2.32, "SI Events (System Interface Events)"
MSG_SI_L2STUB_UNKNOWN_SOURCE_PID	9.2.32, "SI Events (System Interface Events)"
MSG_SIP_FM_INTERNAL_ERROR	9.2.2, "Status Events"
MSG_SIP_FM_MSG_INTERNAL_ERROR	9.2.2, "Status Events"
MSG_SIP_FM_MSG_NOT_PROCESSED	9.2.2, "Status Events"
MSG_SIP_FM_STARTUP_FAILURE	9.2.2, "Status Events"
MSG_SNCP_ADD_OBJECT_FAILED	9.2.6, "Call Control and Feature Events"

Event Code	Section
MSG_SNCP_CHANNEL_ID_MISSING	9.2.6, "Call Control and Feature Events"
MSG_SNCP_COULD_NOT_CREATE_OBJECT	9.2.6, "Call Control and Feature Events"
MSG_SNCP_COULD_NOT_DELETE_OBJECT	9.2.6, "Call Control and Feature Events"
MSG_SNCP_COULD_NOT_SET_FORW_ENC	9.2.6, "Call Control and Feature Events"
MSG_SNCP_COULD_NOT_SET_REV_ENC	9.2.6, "Call Control and Feature Events"
MSG_SNCP_DEVICE_ID_MISSING	9.2.6, "Call Control and Feature Events"
MSG_SNCP_ERROR	9.2.6, "Call Control and Feature Events"
MSG_SNCP_NEITHER_ENC_COULD_BE_SET	9.2.6, "Call Control and Feature Events"
MSG_SNCP_NO_RESOURCE_ID	9.2.6, "Call Control and Feature Events"
MSG_SNCP_UNANTICIPATED_MESSAGE	9.2.6, "Call Control and Feature Events"
MSG_SNMP_TRAP_COLLECTOR_START_ERROR	9.2.3, "Reboot Events"
MSG_SPE_CERT_MISSING	9.2.22, "SPE Events"
MSG_SPE_CERT_AVAIL	9.2.22, "SPE Events"
MSG_SPE_CERT_UPDATED	9.2.22, "SPE Events"
MSG_SPE_CERT_EXPIRED	9.2.22, "SPE Events"
MSG_SPE_CERT_TIMEREMAINING	9.2.22, "SPE Events"
MSG_SPE_CRL_EXPIRED	9.2.22, "SPE Events"
MSG_SPE_CRL_UPDATED	9.2.22, "SPE Events"
MSG_SPE_ALL_CRLS_UPTODATE	9.2.22, "SPE Events"
MSG_SPL_ADD_OBJECT_FAILED	9.2.6, "Call Control and Feature Events"
MSG_SPL_ERROR	9.2.6, "Call Control and Feature Events"
MSG_SPL_FMSEM_ERROR	9.2.6, "Call Control and Feature Events"

Event Code	Section
MSG_SPL_MISSING_CS_ID	9.2.6, "Call Control and Feature Events"
MSG_SPL_SESSION_NOT_FOUND	9.2.6, "Call Control and Feature Events"
MSG_SPL_UNANTICIPATED_MESSAGE	9.2.6, "Call Control and Feature Events"
MSG_SSM_BAD_NWRS_RESULT	9.2.6, "Call Control and Feature Events"
MSG_SSM_INVALID_PARAM	9.2.6, "Call Control and Feature Events"
MSG_SSM_NO_CSID	9.2.6, "Call Control and Feature Events"
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	9.2.3, "Reboot Events"
MSG_SSM_SESSION_CREATION_FAILED	9.2.3, "Reboot Events"
MSG_SSM_UNSPEC_ERROR	9.2.6, "Call Control and Feature Events"
MSG_SYSTEM_REBOOT	9.2.3, "Reboot Events"
MSG_STRC_STOP	9.2.2, "Status Events"
MSG_STRC_START	9.2.2, "Status Events"
MSG_T90_ERROR	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_T90_INFO	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_TESTLW_ERROR	9.2.42, "Test Loadware Events"
MSG_TESTLW_INFO	9.2.42, "Test Loadware Events"
MSG_TLS_MUTEX_BLOCKED	9.2.29, "OAM Events"
MSG_TLS_POOL_SIZE_EXCEEDED	9.2.3, "Reboot Events"
MSG_VCAPI_ACCEPT_ERROR	9.2.23, "VCAPI Events"
MSG_VCAPI_ADD_OBJECT_FAILED	9.2.24, "VCAPI Application Events"
MSG_VCAPI_BUF_NOT_CREATED	9.2.23, "VCAPI Events"
MSG_VCAPI_CONF_ALLOC_ERR	9.2.23, "VCAPI Events"

Event Code	Section
MSG_VCAPI_CONF_WITHOUT_REQ	9.2.24, "VCAPI Application Events"
MSG_VCAPI_CONV_H2N_ERROR	9.2.23, "VCAPI Events"
MSG_VCAPI_CONV_H2N_FAILED	9.2.23, "VCAPI Events"
MSG_VCAPI_CONV_N2H_FAILED	9.2.23, "VCAPI Events"
MSG_VCAPI_COULD_NOT_CREATE_OBJECT	9.2.24, "VCAPI Application Events"
MSG_VCAPI_COULD_NOT_DELETE_OBJECT	9.2.24, "VCAPI Application Events"
MSG_VCAPI_COULD_NOT_FIND_CSID	9.2.24, "VCAPI Application Events"
MSG_VCAPI_COULD_NOT_FIND_OBJECT	9.2.24, "VCAPI Application Events"
MSG_VCAPI_COULD_NOT_FIND_PLCI	9.2.24, "VCAPI Application Events"
MSG_VCAPI_COULD_NOT_STORE_REQ	9.2.24, "VCAPI Application Events"
MSG_VCAPI_CSID_MISSING	9.2.24, "VCAPI Application Events"
MSG_VCAPI_DATA_B3_ALLOC_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_DATA_NOT_STORED	9.2.23, "VCAPI Events"
MSG_VCAPI_DISP_NOT_READY	9.2.23, "VCAPI Events"
MSG_VCAPI_ILLEGAL_LINK_NUMBER	9.2.24, "VCAPI Application Events"
MSG_VCAPI_ILLEGAL_PARTNER_NUMBER	9.2.24, "VCAPI Application Events"
MSG_VCAPI_IND_ALLOC_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_LINK_TABLE_FULL	9.2.23, "VCAPI Events"
MSG_VCAPI_LISTENING_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT	9.2.24, "VCAPI Application Events"
MSG_VCAPI_MSG_NOT_SEND	9.2.23, "VCAPI Events"
MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG	9.2.24, "VCAPI Application Events"

Event Code	Section
MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG	9.2.24, "VCAPI Application Events"
MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG	9.2.24, "VCAPI Application Events"
MSG_VCAPI_NO_ALLOC_EXTENDED	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_ALLOC_MSG	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_ALLOC_SINGLE	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_CAPI_DATA	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_CLIENT	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_LIST_SOCKET	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_LNK_CONN	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_NEW_BUF	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_PLCI	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_PLCI_AVAILABLE	9.2.24, "VCAPI Application Events"
MSG_VCAPI_NO_PLCI_DATA_B3	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_PLCI_DISCONNECT	9.2.23, "VCAPI Events"
MSG_VCAPI_NO_RCV_BUFFER	9.2.23, "VCAPI Events"
MSG_VCAPI_PLCI_NOT_FOUND	9.2.23, "VCAPI Events"
MSG_VCAPI_RCV_LEN_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_RECEIVE_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_SERVER_ERROR	9.2.24, "VCAPI Application Events"
MSG_VCAPI_SOCK_NOT_AVAIL	9.2.23, "VCAPI Events"
MSG_VCAPI_SOCKET_BIND_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_SOCKET_NOT_OPEN	9.2.23, "VCAPI Events"
MSG_VCAPI_SOCKET_RCV_ERR	9.2.23, "VCAPI Events"
MSG_VCAPI_TOO_MANY_CLIENTS	9.2.23, "VCAPI Events"
MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE	9.2.24, "VCAPI Application Events"
MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE	9.2.24, "VCAPI Application Events"

Event Code	Section
MSG_VCAPI_UNANTICIPATED_MESSAGE	9.2.24, "VCAPI Application Events"
MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE	9.2.24, "VCAPI Application Events"
MSG_VCAPI_UNKNOWN_MSG_N2H	9.2.23, "VCAPI Events"
MSG_VCAPI_UNKNOWN_NTFY	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_BUF_LEN	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_CONV_H2N	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_CONV_N2H	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_EVENT_CAPI	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_EVENT_SRV	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_LENGTH_MSG	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_LINKNUM	9.2.23, "VCAPI Events"
MSG_VCAPI_WRONG_MSG_LENGTH	9.2.23, "VCAPI Events"
MSG_WEBSERVER_INTERNAL_ERROR	9.2.29, "OAM Events"
MSG_WEBSERVER_MAJOR_ERROR	9.2.3, "Reboot Events"
MSG_X25_ERROR	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_X25_INFO	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_X75_ERROR	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_X75_INFO	9.2.43, "Fax Converter, HDLC and X.25 Events"
MSG_XMLUTILS_ERROR	9.2.47, "XMLUTILS Events"
QDC_ERROR_IN_CLIENT	9.2.52, "QDC-CGWA-Related Events"
QDC_ ERROR_IN_COMMON_CLIENT	9.2.51, "Client-Related Events"
QDC_INVALID_CONFIGURATION	9.2.52, "QDC-CGWA-Related Events"
QDC_MSG_QUEUE_ERROR	9.2.51, "Client-Related Events"

Event Code	Section
QDC_PERSYSTENCY_ERROR	9.2.52, "QDC-CGWA-Related Events"
QDC_SIGNALLING_DATA_ERROR	9.2.51, "Client-Related Events"
QDC_SYSTEM_ERROR	9.2.51, "Client-Related Events"
QDC_VOIPSD_ERROR	9.2.53, "QDC VoIPSD Error Report Events"
SENTA_NOK_UPGRADE_REG	9.2.2, "Status Events"
SIP_INFORMATION	9.2.54, "SIP Events"
SIP_INVALID_PARAMETER_VALUE	9.2.54, "SIP Events"
SIP_INVALID_POINTER	9.2.54, "SIP Events"
SIP_REBOOT	9.2.3, "Reboot Events"
SIP_UNEXPECTED_RETURN_VALUE	9.2.54, "SIP Events"

9.2.2 Status Events

COMGA_NOK_UPGRADE_REG

Loading the COMGA Firmware via HTTP

FW_NOK_UPGRADE_REG

Loading the firmware

MSG_DLSC_BOOTSTRAP_OK

The bootstrapping of the deployment and licensing server clients was successful.

MSG_FIREWALL_ALARM

Alarm at firewall.

MSG_GW_SUCCESSFULLY_STARTED

`EventText: 11/21/2001 20:46:52`

Type: **Information**

Gateway was started successfully at given time. An SNMP trap is generated.

MSG_IPNCV_STARTUP_ERROR

`EventText: IPNCV Startup: %s`

Type: **Major**

IPNCV could not be started. An SNMP trap is generated. Create a TR/MR.

MSG_IPNCV_STARTUP_SHUTDOWN

`EventText: IPNCV start/stop: %s`

Type: **Information**

IPNCV was started or stopped successfully. An SNMP trap is generated.

MSG_IPNCV_INTERNAL_ERROR

`EventText: Internal IPNCV error: %s`

Type: **Warning**

Software error: invalid internal data found. An SNMP trap will be generated with the profile IPNCV-Detailed.

MSG_LDAP_SUCCESSFULLY_STARTED

`EventText: %s`

Type: **Information**

LDAP started successfully.

FP_EVT_INFORMATION

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

Type: **Information**

Internal SW event - for information only

FP_EVT_TRACE_STOP

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

Type: **Information**

Trace stop provided

FP_EVT_TRACE_START

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

Type: **Information**

Trace start provided

FP_EVT_SNMP_TRAP

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

Type: **Warning**

Important events with SNMP trap. Important events - SNMP trap is generated.

FP_EVT_MINOR

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

Type: **Minor**

Internal SW error with remote signaling

FP_EVT_INDETERMINATE

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

Type: **Information**

Internal software error with trace stop and remote signaling

MSG_PS_INVALID_STREAM_FROM_ADDRESS

Invalid data from a specific address.

MSG_PS_INVALID_STREAM_FROM_PORT

Invalid data from a specific port.

MSG_SIP_FM_MSG_INTERNAL_ERROR

`EventText: %p`

Type: **Major**

Software error within SIP_FM_MSG

MSG_SIP_FM_STARTUP_FAILURE

`EventText: SIP_FM startup failed: %s`

Type: **Major**

Software error during SIP_FM start

MSG_SIP_FM_INTERNAL_ERROR

`EventText: %p`

Type: **Major**

Software error within SIP_FM

MSG_SIP_FM_MSG_NOT_PROCESSED

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

Type: **Major**

SIP_FM could not send a "received" message.

MSG_STRC_STOP

STRC stopped.

MSG_STRC_START

STRC started.

MSG_HBR_WARNING

Warning of HiPath backup and restore.

SENTA_NOK_UPGRADE_REG

Loading the SENTA Firmware via HTTP

9.2.3 Reboot Events

MSG_CAT_H323_REBOOT

The H.323 stack adapter has no more internal resources and causes a reboot. The reboot is executed. An SNMP trap is generated.

MSG_CAT_HSA_REBOOT

`EventText: HSA (Reboot) Q931 cmCallNew() failed:reaching vtNodeCount limit`

Type: **Critical**

The H.323 stack adapter has run out of internal resources and causes a reboot. The reboot is executed. An SNMP trap is generated. Include the event log with the error report.

MSG_OSF_PCS_EXCEPTION

`EventText: "%p"`

Type: **Critical**

The OSF has registered a critical exception. The reboot will still be executed.

MSG_OS_EXCEPTION_ERROR

The OS has registered a critical exception. The reboot is executed.

MSG_WEBSERVER_MAJOR_ERROR

`EventText: %p`

Type: **Major**

Internal error on web server. As other activities on the part of the web server have been influenced, a reboot will be forced. The reboot is executed.

MSG_ADMIN_REBOOT

Type: **Information**

`EventText: Reboot initiated by Admin`

A restart forced by the administrator is executed. An SNMP trap is generated.

`EventText: Reboot initiated by Admin (SW Image Activation)`

A restart forced by the administrator by loading a new software image is executed. An SNMP trap is generated.

`EventText: Reboot initiated by Admin (SW Upgrade)`

A restart forced by the administrator by loading new data is executed. An SNMP trap is generated.

MSG_SYSTEM_REBOOT

`EventText: Reboot initiated by Garbage Collection. Available memory: xxxx`

Type: **Information**

A restart necessitated by an internal garbage collection is executed. An SNMP trap is generated.

MSG_EXCEPTION_REBOOT

```
EventText: Reboot initiated by VxWorks Task Exception
```

Type: **Information**

A restart is executed following a VxWorks task. An SNMP trap is generated.

MSG_RESTORE_CFG_REBOOT

```
EventText: Special reboot initiated by Admin (Backup
Service)
```

Type: **Information**

A restart necessitated by a HBS data restore procedure is executed. An SNMP trap is generated.

MSG_GW_OBJ_MEMORY_EXHAUSTED

```
EventText: Object memory has been exhausted. Last
allocation size: xxxx. Using failsafe areas to attempt a
graceful shutdown
```

Type: **Critical**

Possible memory problems: too much memory has been reserved, or not enough memory available. The necessary reboot is executed. An SNMP trap is generated.

MSG_GW_OBJ_ALLOC_FAILED

```
EventText: Memory allocation in partition xxx failed. xxx
Error. Last allocation size: xxxx. Rebooting ...
```

Type: **Critical**

Possible memory problems: too much memory has been reserved, or not enough memory available. The necessary reboot is executed. An SNMP trap is generated.

MSG_GW_OBJ_MEMORY_INCONSISTENT

```
EventText: Memory corruption in partition xxx XXX Error.
Invalid block address: xxxx. Rebooting ...
```

Type: **Critical**

Possible memory problems: memory was overwritten, or an attempt was made to free up memory that has already been freed up. The necessary reboot is executed. An SNMP trap is generated.

ASSERTION_FAILED_EVENT

```
EventText: Assertion failed ...
```

Type: **Information**

Internal software encoding problem. The necessary reboot is executed. An SNMP trap is generated. Create a TR/MR.

EXIT_REBOOT_EVENT

Type: **Information**

```
EventText: Rebooting due to Exit Event ...
```

Internal software encoding problem. The necessary reboot is executed. An SNMP trap is generated. Create a TR/MR.

`EventText: cannot create Task tV24CliI. ...`

Task generation on the V.24-CLI interface has failed. The necessary reboot is executed.

`EventText: internal error: not enough memory ...`

The reservation of memory has failed. The necessary reboot is executed.

`EventText: CLI: read operation from STD_IN has failed ...`

Input/output faulty. The necessary reboot is executed.

MSG_TLS_POOL_SIZE_EXCEEDED

`EventText: ?*?maximum number of elements exceeded`

Type: **Major**

Problem with internal pool size configuration. The necessary reboot is executed. An SNMP trap is generated. Create a TR/MR.

MSG_SSM_NUM_OF_CALL_LEGS_2BIG

`EventText: More than 2 call Legs: not supported! CSID: %x/ %x`

Type: **Major**

No more than two call Legs per session are permitted. This has caused the software to become unstable. The necessary reboot is executed. An SNMP trap is generated.

MSG_SSM_SESSION_CREATION_FAILED

`EventText: Session creation failed`

Type: **Major**

Signaling is no longer possible because a session could not be created. The necessary reboot is executed. An SNMP trap is generated.

MSG_SNMP_TRAP_COLLECTOR_START_ERROR

`EventText: Trap collector could not be started:%n%s`

Type: **Information**

The thread in the trace collector could not be started. Check whether trap port 162 has already been used elsewhere.

MSG_PPP_STACK_REBOOT

The reboot is executed.

MSG_PPTP_STACK_REBOOT

The reboot is executed.

MSG_ASP_REBOOT

The reboot is executed. An SNMP trap is generated.

MSG_DELIC_ERROR

A DELIC error has occurred. The reboot is executed. An SNMP trap is generated.

MSG_IPSEC_REBOOT

The reboot is executed.

FP_EVT_CRITICAL

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

Type: **Critical**

Reboot triggered by a software error.

FP_EVT_MAJOR

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

Type: **Major**

Reboot because resources are exhausted.

FP_EVT_WARNING

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

Type: **Warning**

Reboot initiated via the tool.

SIP_REBOOT

`EventText: InternalSetUserA`

Type: **csevMajor**

Configuration of the SIP stack failed. The reboot is executed.

MSG_MIKEY_REBOOT

The reboot is executed.

9.2.4 Resource Monitoring Events

MSG_IP_LINK_FAILURE

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

Type for this log entry: **Warning**

An IP network connection is not or is still not possible. An SNMP trap is generated. Check the terminal connections and cables

`EventText: IP Link no longer out of order`

Type for this log entry: **Cleared**

The IP network connection has become available again. An SNMP trap is generated.

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
```

Type for this log entry: **Warning**

The system memory limit has been reached. Details are listed in the event message (percentage limit value, current value and capacity utilization). This may be caused by a high volume of calls. An SNMP trap is generated.

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

Type for this log entry: **Cleared**

The problem with the system memory limit has been eliminated. Lower memory utilization may be caused by a lower call volume. An SNMP trap is generated.

MSG_OAM_DMA_RAM_THRESHOLD_REACHED

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

Type for this log entry: **Warning**

The DMA memory limit has been reached. Details are listed in the event message (percentage limit value, current value and capacity utilization). This may be caused by a high volume of calls. An SNMP trap is generated.

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

Type for this log entry: **Cleared**

The problem with the DMA memory limit has been eliminated. Lower memory utilization may be caused by a lower call volume. An SNMP trap is generated.

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
```

Type for this log entry: **Warning**

A threshold value has been reached (in the flash memory, in the file system memory capacity or in the netstack IP resources). Details are listed in the event message (percentage limit value, current value and capacity utilization). An SNMP trap is generated.

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

Type for this log entry: **Cleared**

The problem with the threshold value has been eliminated. An SNMP trap is generated.

MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE

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

Type for this log entry: **Warning**

There is (still) a problem with PSU or RPS. An SNMP trap is generated. Check the PSU and RPS and replace them if necessary.

```
EventText: PSU or RPS no longer out of Service
```

Type for this log entry: **Cleared**

The problem with the PSU or RPS has been eliminated. An SNMP trap is generated.

MSG_OAM_FAN_OUT_OF_SERVICE

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

Type for this log entry: **Warning**

There is (still) a problem with the fan. An SNMP trap is generated. Check the fan and replace it if necessary.

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

Type for this log entry: **Cleared**

The problem with the fan has been eliminated. An SNMP trap is generated.

MSG_OAM_HIGH_TEMPERATURE_EXCEPTION

```
EventText: High WaterMark "Temperature" reached:
Configured: xxx Current: xxx . Gateway stopped.
```

Type: **Warning**

A serious problem has occurred with the temperature. The gateway has been stopped. Check the environment and replace boards and/or fan if necessary.

MSG_CAR_MALLOC_FAILED

```
EventText: Malloc failed
```

Type: **Major**

The reservation of memory has failed.

MSG_IPNCV_MEMORY_ERROR

`EventText: IPNCV Memory: %s`

Type: **Major**

Memory overflow: an SNMP trap is generated. Restart the gateway. Create a TR/MR.

MSG_LDAP_IP_LINK_ERROR

`EventText: IP Link out of order`

Type: **Warning**

No network-IP connection.

MSG_LDAP_MEMORY_ERROR

`EventText: No Materna Buffer Available`

Type: **Major**

Not enough memory to send/receive a message.

MSG_LDAP_ENCODE_DECODE_ERROR

`EventText: Unable to Encode/Decode LDAP Msg`

Type: **Major**

BER encoding or decoding of a LDAP-ASN.1 message failed.

MSG_LDAP_SOCKET_ERROR

`EventText: LDAP Socket Failure`

Type: **Major**

An error has occurred with LDAP socket calls.

MSG_LDAP_GENERAL_ERROR

`EventText: LDAP Returns General Error`

Type: **Warning**

An error has occurred with LDAP function calls.

MSG_HACKER_ON_SNMP_PORT_TRAP

`EventText: %s has tried to connect with TCP port 7161`

Type: **Information**

The IP address specified has made an attempt to connect with the SNMP TCP port 7161.

9.2.5 Routing Events

MSG_CAT_NWRS

Type: **Warning/Major**

Invalid data for NPI or TONE value in an ODR command. The command is ignored. This message may also be displayed if an administrator switches

the ODR while the system is running. Check the ODR commands NPITYPE, TONTYPE (and CGNPITYPE, CGTONTYPE) for plausible values.

MSG_NWRS_DPLN_ENTRY_INVALID

`EventText: Dial Plan Entry invalid: Dpln=#, DplnEntry=#member`

Type: **Minor**

Syntax error in the numbering plan: characters other than `0123456789*#ANXZ-` are not allowed. Use permitted characters only. Do not use more than one separator in sequence and do not use separators at the beginning or at the end.

MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE

`EventText:` Dial Plan not found for Device #port

Type: **Major**

The specified port is not assigned to a specific numbering plan entry. Assign the specified port in the numbering plan and, if necessary, generate a new numbering plan first.

MSG_NWRS_EMPTY_FIELD_ECHOED

`EventText:` Empty field # echoed by Out Dial Rule #

Type: **Warning**

The echo command of an outdial rule for outgoing calls results in a blank or implausible sub-string. Check the digit string of the numbering plan entry in conjunction with the echo commands of the outdial rule for outgoing calls.

MSG_NWRS_UNKNOWN_FIELD_ECHOED

`EventText:` Unknown field # echoed by Out Dial Rule #

Type: **Minor**

The echo command of an outdial rule for outgoing calls results in a blank or implausible substring. Check the digit string of the numbering plan entry in conjunction with the echo commands of the outdial rule for outgoing calls.

MSG_NWRS_ODR_COMMAND_UNKNOWN

`EventText:` Unknown Command ...string in Out Dial Rule #

Type: **Minor**

An outdial rule for outgoing calls contains an unrecognizable command or an invalid value. Check the syntax of the outdial rule for keywords and separator characters (':' and ';') as well as all constants and limit values.

MSG_NWRS_ODR_NOT_FOUND

`EventText:` Out Dial Rule # not found"

Type: **Warning**

A gateway contains an index that cannot be resolved in outdial rules for outgoing calls. Use an outdial rule already configured for outgoing calls or create a new one.

MSG_NWRS_DEVICE_NOT_FOUND

`EventText:` Device # port not found

Type: **Major**

An invalid port has been assigned to a route member. Assign a valid destination port to the route member.

MSG_NWRS_DEVICE_TABLE_NOT_FOUND

`EventText:` Device Table not found

Type: **Major**

A port is not available. Try to resolve the problem by restarting the hardware.

MSG_NWRS_ROUTE_NOT_FOUND

`EventText:` Route # not found

Type: **Major**

A numbering plan member contains a route number that cannot be resolved. Use a route that has already been configured or create a new one.

MSG_NWRS_DPLN_NOT_FOUND

`EventText:` Dial Plan not found: Dpln %I

Type: **Major**

A numbering plan with the specified ID could not be found.

MSG_NWRS_UNSPEC_ERROR

`EventText:` %p

Type: **Major**

Inconsistent software status, for example, as a result of invalid data.

9.2.6 Call Control and Feature Events

MSG_SDR_INIT

`EventText:` SDR init %p

Type: **Major**

SDR could not be started (no files). An error occurred during initialization of SDR.

MSG_SDR_UNEXPECTED_EVENT

`EventText:` SDR: Unexpected event %n%M%n in state %s%n from %s - EXCEP: %n%e

Type: **Warning**

Unexpected or unregistered message.

MSG_SNCP_UNANTICIPATED_MESSAGE

`EventText:` SCN Payload: Unanticipated Message %s in state %s - EXCEP: %n%e

Type: **Warning**

An unknown message was received.

MSG_SNCP_DEVICE_ID_MISSING

`EventText:` SCN Payload: Mandatory field device ID missing in message 0x %X - EXCEP: %n%e

Type: **Major**

The mandatory field for the device ID, which is required for creating the resource ID, is missing from the specified message.

MSG_SNCP_CHANNEL_ID_MISSING

`EventText:` SCN Payload: Mandatory field device ID missing in message 0x %X - EXCEP: %n%e

Type: **Major**

The mandatory field for the channel ID, which is required for creating the resource ID, is missing from the specified message.

MSG_SNCP_NO_RESOURCE_ID

`EventText:` SCN Payload: No resource ID available in message 0x%X - EXCEP: %n%e

Type: **Major**

There is no resource ID in the specified message.

MSG_SNCP_COULD_NOT_DELETE_OBJECT

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

Type: **Major**

SCN payload object could not be deleted.

MSG_SNCP_COULD_NOT_CREATE_OBJECT

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

Type: **Major**

SCN payload object could not be deleted.

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

Type: **Major**

Could not set forward encoding.

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

Type: **Major**

Could not set reverse encoding.

MSG_SNCP_NEITHER_ENC_COULD_BE_SET

`EventText:` SCN Payload: Neither encoding could be set for CSID: (%s) and ResID: (%u) - EXCEP: %n%e

Type: **Major**

Neither encoding could be set.

MSG_SNCP_ADD_OBJECT_FAILED

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

Type: **Major**

SCN payload object could not be added.

MSG_SNCP_ERROR

`EventText:` SNCP Error: %p

Type: **Warning/Major**

Inconsistent software status in SNCP component.

MSG_SPL_SESSION_NOT_FOUND

`EventText:` No session for Session Payload Object found using CSID: %u) - EXCEP: %n%e

Type: **Major**

No session object found.

MSG_SPL_ADD_OBJECT_FAILED

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

Type: **Major**

Object could not be added

MSG_SPL_MISSING_CS_ID

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

Type: **Major**

Call and session ID missing.

MSG_SPL_UNANTICIPATED_MESSAGE

`EventText:` Session Payload: Unanticipated Message %s in state %s - EXCEP: %n%e

Type: **Warning**

Unanticipated message.

MSG_SPL_ERROR

`EventText: SPL Error: %p`

Type: **Warning/Major**

Inconsistent software status in SPL component.

MSG_SPL_FMSEM_ERROR

`EventText: FMSEM Error: %p`

Type: **Warning/Major**

Inconsistent software status in FMSEM component, which is part of SPL.

MSG_SSM_NO_CSID

`EventText:` Msg doesn't contain a CSID !

Type: **Major**

Call and session ID missing.

MSG_SSM_INVALID_PARAM

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

Type: **Major**

A parameter contained an invalid value.

MSG_SSM_UNSPEC_ERROR

`EventText: %p`

Type: **Major**

Inconsistent software status, for example, as a result of invalid data.

MSG_SSM_BAD_NWRS_RESULT

`EventText:` Bad result from NWRS

Type: **Major**

Probably a protocol loop was detected. Check configuration of the route from the signal source to the destination.

MSG_MAND_PARAM_MISSING

`EventText:` Mandatory parameter %s for construction of message missing

Type: **Major**

A CCP message could not be built from the message base because a mandatory parameter was missing.

9.2.7 SCN Protocol Events

MSG_ISDN_CMR_INIT_FAILED

`EventText: Initialization for protocol manager failed. %p`

Type: **Warning**

Initialization of the protocol manager failed.

MSG_ISDN_CMR_MAND_FIELDS_MISSING

`EventText: %pMandatory fields missing (ID %s)`

Type: **Warning**

Mandatory fields are missing from the message.

MSG_ISDN_CMR_OBJECT_NOT_FOUND

`EventText: %pThe object for Call and Session ID %s could not be found`

Type: **Critical**

The session object for a connection segment could not be found.

MSG_ISDN_CMR_UNIMPLEMENTED

`EventText: %pUnimplemented feature%s`

Type: **Warning**

The requested feature is not implemented.

MSG_ISDN_CMR_TIMER_EXPIRED

`EventText: %pTimer %S expired in state %S`

Type: **Information**

A timer has expired.

MSG_ISDN_CMR_WRONG_DEVICE_TYPE

`EventText: %p%Device Id %I is not a valid device type`

Type: **Warning**

A specified device type is invalid.

MSG_ISDN_CMR_MSG_DECODE_FAILED

`EventText: %pEvent decoding failed. %s %s %nEvent data: %b`

Type: **Warning**

Message decoding failed.

MSG_ISDN_CMR_NEW_OBJECT_FAILED

`EventText: %pThe object for this Call and Session ID could not be created`

Type: **Critical**

Creation of a session object for a call segment failed.

MSG_ISDN_CMR_ADD_OBJECT_FAILED

`EventText: %pThe object created for this Call and Session ID could not be added to the manager`

Type: **Critical**

A call segment object could not be linked to the protocol manager.

MSG_ISDN_CMR_UNEXPECTED_EVENT

`EventText: %pReceived unexpected event Message ID: %s`

Type: **Information**

An unexpected event was received.

MSG_ISDN_CMR_SESSION_NOT_FOUND

`EventText: %pThe session object for this Call and Session ID could not be found by the manager`

Type: **Critical**

The session object for the call segment was not found.

MSG_ISDN_CMR_STATUS_MSG_RECEIVED

`EventText: %pL3 Status message received in state %s`

Type: **Information**

A status message was received.

MSG_ISDN_CMR_WRONG_PROTVAR

`EventText: %pProtocol Variant %I, Key %x is not valid. Using default Timer Values !`

Type: **Critical**

A protocol variant is invalid.

MSG_ISDN_CMR_GENRIC_EVENT

`EventText: %p`

Type: **Information**

A general event.

MSG_ISDN_RESOURCE_NOT_IN_SERVICE

`EventText: %pResource not in service, Resource State %s`

Type: **Information**

Wrong resource status: the resource does not exist in this service.

MSG_ISDN_RESOURCE_NOT_AVAILABLE

`EventText: %pResource not available, Resource State %s`

Type: **Information**

Resource not available.

MSG_ISDN_RESOURCE_IN_USE_BY_O_CALL

`EventText: %pResource in use by other call. Resource not released, Resource State %s`

Type: **Information**

Resource reserved by another call (call collision).

MSG_ISDN_DEVICE_PTR_NOT_FOUND

`EventText: %pThe device ID could not be found`

Type: **Warning**

The device object could not be found.

MSG_ISDN_CMR_DEVICE_PTR_BAD

`EventText: %pNull device pointer`

Type: **Critical**

The device object pointer is pointing to NULL.

MSG_ISDN_CMR_MSG_ENCODE_FAILED

`EventText: %pEvent encoding failed. %s %s %nEvent data: %b`

Type: **Warning**

Encoding of message failed.

MSG_ISDN_CMR_MSG_SEND_FAILED

`EventText: %pL3 Message sending failed`

Type: **Critical**

Encoding of message failed.

MSG_ISDN_CMR_SEG_MSG_ERROR

`EventText: %pSegmented message error`

Type: **Minor**

Segmented message error.

MSG_ISDN_CMR_UNEXPECTED_ERROR

`EventText: %pUnexpected error`

Type: **Minor**

Unexpected error occurred.

MSG_ISDN_CMR_UNEXPECTED_VALUE

`EventText: %pUnexpected value for this Device ID`

Type: **Warning**

Unexpected value for device ID.

MSG_ISDN_CMR_MSG_UNEXPECTED

`EventText: %pUnexpected event`

Type: **Warning**

Message was unexpected in the current call status.

MSG_ISDN_CMR_GEN_CALL_REF_FAILED

`EventText: %pCould not generate a Call Reference`

Type: **Critical**

Generation of call reference failed.

MSG_ISDN_CMR_WRONG_INTERFACE

`EventText: %pWrong interface type %s`

Type: **Critical**

Wrong interface type.

MSG_ISDN_CMR_UNH_STATE_EVENT

`EventText: %pUnhandled event`

Type: **Warning**

Event was not handled in the appropriate call state.

MSG_ISDN_NULL_PTR

`EventText: %p%p`

Type: **Critical**

An attempt was made to use a pointer at NULL.

MSG_ISDN_ERROR

`EventText: %pError: %p`

Type: **Minor**

ISDN error.

MSG_ISDN_NO_ERROR

`EventText: %pNo Error`

Type: **Information**

No ISDN error.

MSG_ISDN_CMR_PROTOCOL_ERROR

`EventText: Protocol error: Device ID %d`

Type: **Warning**

Message did not comply with the present protocol.

MSG_ISDN_CMR_MESSAGE_ERROR

`EventText: Message Error 0x%X`

Type: **Minor**

Message contains an error.

MSG_ISDN_START_UP_ERROR

`EventText: %s: Start up error. %p`

Type: **Critical**

Error during startup of ISDN protocol.

MSG_ISDN_START_UP

`EventText: %s: Start up OK. %p`

Type: **Information**

ISDN startup concluded.

MSG_ISDN_OVERLOAD_CONDITION

`EventText: %pOverload Condition. SETUP received, RELEASE COMPLETE sent`

Type: **Information**

Overload reached: call cleared.

9.2.8 H.323 Events

H323_NO_IP

n/a

H323_SNMP_TRAP

n/a

MSG_H323_MISSING_PARAMETER

`EventText: ...`

Types: **Major, Minor, Warning, Information**

A parameter is missing from a message that was sent to a H.323 component. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_INVALID_PARAMETER_VALUE

`EventText: ...`

Types: **Major, Minor, Warning**

There is a parameter that exceeds the specified value range. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_INVALID_CONFIGURATION

`EventText: ...`

Types: **Major, Warning**

The configuration for H.323 is wrong. Activate an appropriate H.323 analysis trace profile and attach the trace, event log and gateway config data to the error report.

MSG_H323_UNEXPECTED_RETURN_VALUE

`EventText: ...`

Types: **Major, Minor, Warning**

The current function call returns an unexpected error. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_INVALID_POINTER

`EventText: ...`

Types: **Major, Minor, Warning, Information**

This pointer contains an invalid value. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_INFORMATION

`EventText: ...`

Type: **Information**

This is for information purposes only.

MSG_H323_UNEXPECTED_MESSAGE

`EventText: ...`

Types: **Major, Minor, Warning**

H.323 protocol received an unexpected message. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_LOGIC_ERROR

`EventText: ...`

Types: **Major, Warning, Information**

A logical error was detected during message processing. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_STACK_ERROR

`EventText: ...`

Types: **Major, Minor, Warning, Information**

An error occurred during a H.323 stack operation. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_PROTOCOL_ERROR

`EventText: ...`

Types: **Major, Minor, Warning, Information**

Protocol information missing or contains an error. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_OSCAR_NSD_ERROR

`EventText: ...`

Types: **Major, Minor, Warning, Information**

This error relates to non-standard data. Activate an appropriate H.323 analysis trace profile, and attach the trace and the event log to the error report.

MSG_H323_SNMP_TRAP

`EventText: ...`

Types: **Major, Minor, Warning, Information**

This event indicates a situation that requires the attention of a service engineer. The service department should take measures in accordance with the event text (for example, perform a network check).

9.2.9 H.235 Events

MSG_CAT_H235

`EventText: H.235...`

Types: **Major, Warning, Information**

H.235 security related events. Verify H.235 configuration in gateway, gatekeeper and clients.

9.2.10 RTPQM Events

MSG_IP_RTP_QUALITY_FAILURE

`EventText: ...`

Type for this log entry: **Major**

The LAN quality for the specified destination IP address is classified as "too bad for voice calls". As a result, all further calls to that destination are routed over the line network. Call attempts for this destination are rejected by the gateway. Check the packet loss setting for IP traffic to this IP address.

`EventText: ...`

Type for this log entry: **Cleared**

The time for rejecting LAN calls for the specified IP destination address has elapsed. LAN calls to this destination address can be established again.

MSG_IP_RTP_QUALITY_WARNING

`EventText: ...`

Type: **Major**

This is a warning that LAN quality is deteriorating. The route to the specified destination address may soon be blocked. Check the packet loss setting for IP traffic to this IP address.

9.2.11 GSA Events

MSG_GSA_SNMP

`EventText: %p`

Type: **Critical**

Critical error for GSA which generates an SNMP trap.

9.2.12 DGW Events

MSG_BSD44_VCAPI_NO_LIST

`EventText: No listening socket for VCAPI`

Type: **Major**

Not possible to create a listening socket for VCAPI. LAN traffic not possible.

MSG_BSD44_DGW_NO_LIST

`EventText: No listening socket for DATA-GW`

Type: **Major**

Not possible to create a listening socket for DATAGWI. LAN traffic not possible.

MSG_BSD44_ACCEPT_DGW_ERR

`EventText: accept error for DATAGW Dispatcher`

Type: **Major**

Not possible to set up a new connection for DATAGW.

MSG_BSD44_DGW_SOCKET_FAIL

`EventText: DGW socket() failed`

Type: **Minor**

Client cannot retrieve a socket.

MSG_BSD44_DGW_BIND_FAIL

`EventText: DGW bind() failed`

Type: **Minor**

Client cannot bind a socket.

MSG_BSD44_DGW_CONNECT_FAIL

`EventText: DGW connect() failed`

Type: **Minor**

Client cannot connect to the server.

MSG_DGW_CONN_OUT_OF_RANGE

`EventText: dg_capi_HandleCapi20Msg: connection_id=%D out of range!`

Type: **Minor**

Connection ID exceeds the maximum allowed channels.

MSG_DGW_WRONG_STATE

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

Type: **Minor**

Wrong state for DATAGW Dispatcher.

MSG_DGW_MSG_IGNORED

`EventText: %s from CAPI_PAYLOAD_IF ignored!`

Type: **Minor**

Message ignored because DGW Dispatcher in wrong state.

MSG_DGW_CONN_B3_ACT_IND

`EventText: ALLOC error: no more buffers`

Type: **Major**

Cannot allocate a buffer to send CONNECT_B3_ACTIVE_RESPONSE. The gateway performs an automatic restart.

MSG_DGW_DISC_B3_IND

`EventText: CAPI2_DISCONNECTB3_IND dreadful!: no more buffers`

Type: **Major**

Cannot allocate a buffer to send DGW_CLOSE_REQ. The gateway performs an automatic restart.

MSG_DGW_ALLOC_DISC_B3

`EventText: CAPI2_DISCONNECTB3_IND(2) dreadful!: no more buffers`

Type: **Major**

Cannot allocate a buffer to send DGW_FREE_REQ. The gateway performs an automatic restart.

MSG_DGW_UNHANDLED_MSG

`EventText: unhandled %s msg=%d from CAPI_PAYLOAD_IF`

Type: **Major**

Unknown message from CAPI_PAYLOAD_IF to DGW Dispatcher.

MSG_DGW_DATA_B3_ALLOC_ERR

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

Type: **Major**

Cannot allocate a buffer to send CMT_DATA_REQ to CAPI_PAYLOAD_IF. The gateway performs an automatic restart.

MSG_DGW_ALLOC_REQ_ERR

`EventText: DDGW_ALLOC_REQ received in wrong state!`

Type: **Minor**

DGW Dispatcher in wrong state when receiving DGW_ALLOC_REQ.

MSG_DGW_ALLOC_CONF_ERR

`EventText: DGW_ALLOC_CONF id=%d received in wrong state!`

Type: **Minor**

DGW Dispatcher in wrong state when receiving DGW_ALLOC_CONF.

MSG_DGW_FREE_ALLOC_ERR

`EventText: DGW_FREE_REQ: allocb failed!`

Type: **Major**

Cannot allocate a buffer to send DISCONNECT_B3_REQ. The gateway performs an automatic restart.

MSG_DGW_UNKNOWN_PRIMITIVE

`EventText: unknown capi primitive: %x`

Type: **Major**

Unknown message from CAPI_PAYLOAD_IF to DGW Dispatcher.

MSG_DGW_RECEIVE_ERR

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

Type: **Major**

Receive error.

MSG_DGW_UNHANDLED_EVENT

`EventText: Unhandled event for DGW-Dispatcher,received event:%D`

Type: **Warning**

Unhandled event received by DGW Dispatcher.

MSG_DGW_WRONG_EVENT_CAPI20

`EventText: wrong eventcode from CAPI20-Mgr`

Type: **Warning**

CAPI20 Manager received the wrong event code.

MSG_DGW_NO_PLCI

`EventText: Find connection ID by PLCI:PLCI %d not found`

Type: **Warning**

Not possible to find connection ID because of wrong PLCI.

MSG_DGW_IND_ALLOC_ERR

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

Type: **Major**

Not possible to allocate a buffer for CMT_DATA_IND. The gateway performs an automatic restart.

MSG_DGW_CONF_ALLOC_ERR

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

Type: **Major**

Not possible to allocate a buffer for CMT_DATA_CONF. The gateway performs an automatic restart.

MSG_DGW_WRONG_EVENT_CAPI

`EventText: wrong eventcode from CAPI_PAYLOAD_INTERFACE`

Type: **Warning**

Wrong event code from CAPI_PAYLOAD_INTERFACE.

MSG_DGW_ALLOC_CHN_RUN_OUT

`EventText: ALLOC_CHANNEL_REQ: run out of connection handles`

Type: **Minor**

Too many connections.

MSG_DGW_ALLOC_CHN_CONN_FAIL

`EventText: ALLOC_CHANNEL_REQ:connect failed`

Type: **Major**

Not possible to set up a new connection to the server.

MSG_DGW_OPEN_CHN_UNKNOWN_ID

`EventText: AOPEN_CHANNEL_REQ: unknown id`

Type: **Minor**

Connection ID not found using the channel ID.

MSG_DGW_OPEN_CHN_WRONG

`EventText: OPEN_CHANNEL_REQ:dreadful!: wrong state`

Type: **Minor**

Wrong state for message OPEN_CHANNEL_REQ.

MSG_DGW_OPEN_CHN_ALLOC_FAIL

`EventText: OPEN_CHANNEL_REQ:Alloc failed`

Type: **Major**

Not possible to allocate a buffer for DGW_OPEN_CONFIRM. The gateway performs an automatic restart.

MSG_DGW_FREE_UNKNOWN_ID

`EventText: FREE_CHANNEL_REQ : unknown connection_id`

Type: **Major**

FREE_CHANNEL_REQ with unknown ID.

MSG_DGW_FREE_CHN_ALLOC_FAIL

`EventText: FREE_CHANNEL_REQ : Alloc failed`

Type: **Major**

ALLOC for FREE_CHANNEL_REQ failed. Not possible to send DISCONNECT_B3_REQ. The gateway performs an automatic restart.

MSG_DGW_SEC_ALLOC_FAIL

`EventText: FREE_CHANNEL_REQ : second Alloc failed`

Type: **Major**

Second ALLOC for FREE_CHANNEL_REQ failed. Not possible to send DGW_FREE_REQ. The gateway performs an automatic restart.

MSG_DGW_UNH_MSG_CAPI20_MGR

`EventText: unhandled message %d from CAPI20-Mgr`

Type: **Warning**

Unknown message from CAPI2.0 Manager.

MSG_DGW_UNKNOWN_ID_CHANNEL

`EventText: find_conn_id_by_chn_id: unknown id %D`

Type: **Minor**

Connection ID cannot be found using channel ID.

MSG_DGW_FREE_NOT_SEND

`EventText: Alloc error: DGW_FREE_REQUEST not sent`

Type: **Major**

Alloc error: DGW_FREE_REQUEST not sent. The gateway performs an automatic restart.

MSG_DGW_DISC_B3_NOT_SEND

`EventText: Alloc error: DISCONNECT_B3_REQUEST not sent`

Type: **Major**

Alloc error: DISCONNECT_B3_REQUEST not sent. The gateway performs an automatic restart.

MSG_DGW_SOCKET_UNKNOWN

`EventText: SO_NTFY_CONN_COMPLETE: unknown socket!`

Type: **Minor**

SO_NTFY_CONN_COMPLETE: unknown socket. Connection will be closed.

MSG_DGW_CONNECT_FAILED

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

Type: **Major**

SO_NTFY_CONN_COMPLETE: connection error.

MSG_DGW_CONN_COMPL_ALLOC

`EventText: SO_NTFY_CONN_COMPLETE: Alloc failed`

Type: **Major**

No allocation request to remote.

MSG_DGW_CONN_RUN_OUT

`EventText: SO_NTFY_CONNECTION: run out of connection handles:cnt=%d`

Type: **Warning**

Too many connections.

MSG_DGW_MGR_NOT_READY

`EventText: SO_NTFY_CONNECTION: CAPI20Mgr not ready:DGW_Disp_State=0x%x`

Type: **Warning**

SO_NTFY_CONNECTION: CAPI2.0 Manager not ready. Start operation message from CAPI2.0 Manager not received.

MSG_DGW_BUFAVAIL_SOCK_UNKN

`EventText: SO_NTFY_BUFAVAIL: unknown socket`

Type: **Minor**

Send not possible because socket unknown.

MSG_DGW_RCV_SOCK_UNKN

`EventText: SO_NTFY_RCV_SDATA: unknown socket`

Type: **Minor**

Data cannot be received because socket unknown.

MSG_DGW_ABORT_SOCK_UNKN

`EventText: SO_NTFY_ABORT: unknown socket`

Type: **Minor**

Connection cannot be received because of unknown socket.

MSG_DGW_UNKNOWN_NOTIFIC

`EventText: Unknown notification 0x%x`

Type: **Minor**

Unknown notification.

MSG_DGW_RCV_FAILED

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

Type: **Minor**

Data not received correctly.

MSG_DGW_INV_MSG_LEN

`EventText: invalid message length: %d`

Type: **Minor**

Message with wrong length received from remote.

MSG_DGW_RCV_ALLOC_FAIL

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

Type: **Major**

Not possible to allocate a receive buffer.

MSG_DGW_MSG_RCV_FAIL

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

Type: **Minor**

Not possible to receive a message.

MSG_DGW_INVALID_LENGTH

`EventText: invalid length:%d %s`

Type: **Minor**

Wrong length received from remote.

MSG_DGW_INV_DATA_LEN

`EventText: invalid data length:%d`

Type: **Minor**

Wrong data length received from remote.

MSG_DGW_SEND_FAILED

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

Type: **Minor**

Not possible to send message to remote.

MSG_DGW_SEND_DATA_ERR

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

Type: **Minor**

Not possible to send data to remote.

MSG_DGW_SOCKET_NOT_OPEN

`EventText: DGW socket not opened`

Type: **Major**

DGW socket not opened. No connections possible.

MSG_DGW_SOCKET_BIND_ERR

`EventText: bind error for DGW socket %d`

Type: **Major**

Bind error in DGW socket. No connections possible.

MSG_DGW_LISTENING_ERR

`EventText: listening error for DGW socket %d`

Type: **Major**

Listening error in DGW socket. No connections possible.

MSG_DGW_ACCEPT_FAILED

`EventText: so_accept() failed`

Type: **Minor**

No new connections accepted.

9.2.13 CAR Events

MSG_CAR_GENERAL_ERROR

`EventText: CAR : General error : %s`

Type: **Minor**

A generic error occurred in the CAR subsystem.

MSG_CAR_NO_MEMORY

`EventText: CAR : no more memory available`

Type: **Minor**

`EventText:` CAR: there is no more memory available.

MSG_CAR_FKT_GET_IPADR_FAILED

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

Type: **Minor**

`Car_fkt_get_ipadr` returns an unsuccessful result due to the fact that `mat_allocb` cannot reserve any memory anymore.

MSG_CAR_START_TCP_LISTENER_FAILED

`EventText: CAR : SOH : start of TCP listener failed : returncode soh_api_start_tcp_listener = %d`

Type: **Critical**

`soh_api_send_tcp_listener` returns an incorrect value. Starting the TCP listener failed.

MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_SOH_ERROR

`EventText: CAR : SOH : sending update request failed : returncode soh_api_send_tcp_data = %d`

Type: **Critical**

`soh_api_send_tcp_listener` returns an incorrect value. Sending the update request failed.

MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_NO_MEMORY

`EventText: CAR : SOH : Start update failed due to lack of memory`

Type: **Minor**

CAR: SOH: sending the update request failed due to lack of memory.

MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CALLADDRTAB_TOO_BIG

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

Type: **Minor**

CAR: SOH: the number of entries received by the update is too big. Possible SOH error.

MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS

`EventText: CAR : SOH : received message is not from the Venus server. Received IP address = 0x%x`

Type: **Major**

CAR: SOH: received message is not from the Venus server.

MSG_CAR_DB_READ_NODE_TABLE_ERROR

`EventText: CAR : DB : Read of Node Table failed : table index = %d`

Type: **Major**

CAR: DB: reading node table failed.

MSG_CAR_ALIVE_IP_CONNECTION_LOST

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

Type: **Major**

`EventText:` CAR: Alive: IP connection lost.

MSG_CAR_ALIVE_IP_CONNECTION_LOST

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

Type: **Major**

CAR: Alive: IP connection lost.

MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN

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

Type: **Information**

CAR: Alive: IP connection ok again.

MSG_CAR_ERROR_WITH_OAM_INTERFACE

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

Type: **Minor**

CAR: An error occurred on the OAM interface.

MSG_CAR_NO_FREE_CODEC_TAB_ELE

`EventText: No free table element for CODECs found`

Type: **Minor**

No free table element found for codecs.

MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB

`EventText: Cannot arrange node table %d`

Type: **Major**

Node table cannot be arranged.

MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS

`EventText: Cannot sort MAC addresses %s`

Type: **Minor**

MAC addresses cannot be sorted.

MSG_CAR_CODECS_INCONSISTENT

`EventText: HSA CODEC tables inconsistent %s`

Type: **Major**

The HSA CODEC tables are inconsistent.

MSG_CAR_WRONG_NODE_ID

`EventText: Wrong node id %d`

Type: **Major**

Wrong node identification.

MSG_CAR_WRONG_SERVICE

`EventText: Wrong service %d`

Type: **Minor**

Wrong service.

MSG_CAR_NODE_INFO_ALREADY_AVAILABLE

`EventText: Node info already available for %d`

Type: **Minor**

Node information for specified nodes is already available.

MSG_CAR_DBF_SERVER_INCONSISTENT

`EventText: DB feature server inconsistent %s`

Type: **Major**

The DB feature server is in an inconsistent state.

MSG_CAR_UNEXPECTED_MSG_RECV

`EventText: Unexpected message received %s`

Type: **Minor**

An unexpected message was received.

MSG_CAR_UNEXPECTED_DATA_RECV

`EventText: Unexpected data received %s`

Type: **Minor**

Unexpected data was received.

MSG_CAR_PARAM_NOT_FOUND

`EventText: Parameter not found %s`

Type: **Major**

Parameter not found.

MSG_CAR_WRONG_EVENT

`EventText: Wrong event received %x`

Type: **Major**

A wrong event was received.

MSG_CAR_WRONG_LENGTH

`EventText: Wrong length %d`

Type: **Minor**

Wrong length.

MSG_CAR_WRONG_IP_ADDRESS

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

Type: **Major**

Wrong IP address.

MSG_CAR_UNAUTHORIZED_IP_ACCESS

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

Type: **Minor**

Unauthorized access from the specified IP address.

MSG_CAR_NO_MAC_ADDRESS

`EventText: No MAC address found`

Type: **Major**

MAC address not found.

MSG_CAR_DBFS_POSS_CONFLICT

`EventText: %s`

Type: **Warning**

Possible conflict.

MSG_CAR_CODEC_ENTRY_DELETED

`EventText: CODEC deleted for TableId %d, NodeId %d`

Type: **Major**

HSA CODEC Access deleted.

9.2.14 REG Events

MSG_REG_GLOBAL_ERROR

`EventText: REG : Global error : %s`

Type: **Minor**

REG: generic error.

MSG_REG_NO_MEMORY

`EventText: REG : No more memory available`

Type: **Minor**

REG: out of memory.

MSG_REG_SOH_SEND_DATA_FAILED

`EventText: REG : SOH : send data failed : returncode soh_api_send_tcp_data = %d`

Type: **Critical**

REG: SOH: send data failed: `soh_api_send_tcp_data` returned an incorrect return code.

MSG_REG_REQUEST_WITHIN_REGISTRATION

`EventText: REG : REG request within registration`

Type: **Minor**

REG: REG request within registration.

MSG_REG_NIL_PTR_FROM_SOH

`EventText: REG : NIL pointer received from SOH : Pointer = 0x%x`

Type: **Critical**

REG: NIL pointer (pointer with no address content) received from SOH.

MSG_REG_ERROR_FROM_SOH

`EventText: REG : SOH : error from SOH : errorcode = 0x%x`

Type: **Critical**

REG: SOH; error from SOH.

MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH

`EventText: REG : SOH : unknown event from SOH 0x%x`

Type: **Minor**

REG: SOH: unknown event from SOH.

MSG_REG_NO_REGISTRATION_POSSIBLE

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

Type: **Major**

REG: no registration possible (no response).

9.2.15 NU Events

MSG_NU_GENERAL_ERROR

`EventText: General error %s`

Type: **Warning**

Only as a temporary dummy.

MSG_NU_TRANSPCONT_MISSING

`EventText: Transport container missing`

Type: **Major**

Transport container missing.

MSG_NU_NO_FREE_TRANSACTION

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

Type: **Warning**

No free transaction store found in a function.

MSG_NU_INVALID_CIDL

`EventText: NCIDL invalid`

Type: **Major**

The CIDL sent in the message is invalid.

MSG_NU_CAR_FAILED

`EventText: Call to CAR function failed`

Type: **Major**

Call to CAR function failed. Wrong return code returned.

MSG_NU_CAR_RESP_INVALID

`EventText: Invalid Response from CAR: 0x%x`

Type: **Major**

Invalid response from CAR.

MSG_NU_UNEXPECTED_MSG

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

Type: **Major**

Unexpected message in a certain NU state.

MSG_NU_UNEXPECTED_TIMER

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

Type: **Minor**

Unexpected timer event in a certain NU state.

MSG_NU_FREE_CHN_UNEXPECTED

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

Type: **Major**

Free channel unexpected in a certain NU state.

MSG_NU_FREE_CHN_COMF_TOO_LATE

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

Type: **Major**

Free channel confirmation from the NU Leg control too late in certain NU state.

MSG_NU_EVENT_EXCEPTION

`EventText: Event exception: State: %d, Event:0x%x, Data:0x %x`

Type: **Minor**

Event exception in a certain NU state.

MSG_NU_WRONG_CALL_REF

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

Type: **Major**

Wrong call reference from system or LAN.

MSG_NU_UNEXPECTED_SETUP

`EventText: Unexpected SETUP: State:%d, Lwport/IPAddr:0x%x, CR:%d, Direction:%d`

Type: **Warning**

Unexpected SETUP on active transaction in a certain NU state. Might be caused by glare situations.

MSG_NU_NO_PORT_DATA

`EventText: No data for port_%d found in %s`

Type: **Major**

No data for a port found in a certain function.

MSG_NU_SUPERFLUOS_MSG

`EventText: Superfluous message: Event:0x%x, Lwport:%d, Channel:%d, Data:0x%x`

Type: **Minor**

Superfluous message sent to NU. Might be caused by asynchronous behavior of the two nodes.

MSG_NU_IP_ERROR

`EventText: IP Error: IPAddress:0x%x, Error: 0x%x`

Type: **Minor**

IP error.

MSG_NU_UNKNOWN_MESSAGE

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

Type: **Minor**

Unknown message sent to NU.

MSG_NU_INTERNAL_ERROR

`EventText: NU internal error: %s`

Type: **Minor**

NU Internal software error.

MSG_NU_TOO_MUCH_DIGITS

`EventText: ?*?Too many digits sent at a time`

Type: **Minor**

Too many digits sent at a time.

MSG_NU_TCP_LISTENER_FAILED

`EventText: Start_tcp_listener failed`

Type: **Critical**

The Socket Handler couldn't start a listener function.

MSG_NU_SOH_RESP_INVALID

`EventText: SOH call back response invalid. Event:0x%x, Reason:%s`

Type: **Minor**

Parameters returned in the Socket Handler callback function invalid, or SOH error.

MSG_NU_DEV_TAB_NOT_FOUND

`EventText: Device table not found`

Type: **Major**

Access to the device table not ok.

9.2.16 NU Leg Control Events

MSG_NULC_MESSAGE_ERROR

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

Type: **Warning**

Received unexpected or unknown message.

MSG_NULC_PARAM_ERROR

```
EventText: Missing/not valid parameter %s in message %s
           %s = name of either parameter or message
```

Type: **Major**

Mandatory parameter missing or contains an invalid value.

MSG_NULC_MEMORY_ERROR

```
EventText: EventText: ?*?Can't access/allocate memory
```

Type: **Major**

Application did not receive the requested memory, or another operation returned a null pointer.

MSG_NULC_INTERNAL_ERROR

```
EventText: %s
```

Type: **Major**

Internal error in NU Leg control.

MSG_NULC_INTERNAL_EVENT

```
EventText: %s
```

Type: **Information**

Successful startup or shutdown of application.

9.2.17 HFA Manager Events

MSG_HFAM_HAH_ALLOC_CHAN_ERR

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

Type: **Major**

An attempt was made to seize a channel for a client that is not idle. Internal error in HFA Manager.

MSG_HFAM_HAH_ALLOC_CONF_ERR

```
EventText: HFAM_ALLOCATE_CHANNEL_CONF received from client
that is not in allocating or opening state
```

Type: **Major**

HFAM_OPEN_CHANNEL_CONF received from client that is not in opening state. HFAA error.

MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR

EventText: unknown/unexpected event code received: lw_event

Type: **Major**

Unknown/unexpected event code received: lw_event. System-side DH/CP error.

MSG_HFAM_MAIN_ILLEG_PORTNO_ERR

EventText: Illegal port no with event code

Type: **Major**

Illegal port number with event code. Check system.

MSG_HFAM_MAIN_NO_LOGONTIMER_ERR

EventText: No logon timer started for that client

Type: **Major**

A logon timer was not started for the client. Internal error in the HFA Manager.

MSG_HFAM_LIH_CREATE_REGISOCK_ERR

EventText: Could not create registration socket

Type: **Critical**

Could not create registration socket. LAN-side error.

MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR

EventText: Could not set socket option 'reuse address

Type: **Critical**

Could not set socket option "reuse Address". LAN-side error.

MSG_HFAM_LIH_BIND_REGISOCK_ERR

EventText: Could not bind registration socket

Type: **Critical**

Could not bind registration socket. LAN-side error.

MSG_HFAM_LIH_LISTEN_REGISOCK_ERR

EventText: Could not listen at registration socket

Type: **Critical**

Could not listen at registration socket. LAN-side error.

MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR

EventText: Could not accept TCP/IP connection from client

Type: **Critical**

Could not accept TCP/IP connection from client. LAN-side error. Check client setup.

MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR

`EventText: Could not accept TCP/IP connection from client`

Type: **Major**

Connection from client not accepted. LAN-side error. Check client setup.

MSG_HFAM_LIH_MAX_CON_EXCEED_ERR

`EventText: max no.(HFAM_MAX_CONNECTIONS) of TCP/IP connections exceeded`

Type: **Major**

Maximum number (`HFAM_MAX_CONNECTIONS`) of TCP/IP connections exceeded. Internal error in the HFA Manager.

MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR

`EventText: Cannot accept connection from client`

Type: **Major**

Cannot accept connection from client. LAN-side error. Check client setup.

MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR

`EventText: CSocket would block: no data -> ignore`

Type: **Minor**

Socket would block: no data. Ignore. LAN-side error.

MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR

`EventText: TC_DATAGRAM received from client->subscriber_no while not in logged_in state, discarded`

Type: **Minor**

TC_DATAGRAM received from client->subscriber number, although not logged on. Discarded. LAN-side error. Check client setup.

MSG_HFAM_LIH_UNEXP_CORNET_ERR

`EventText: unknown/unexpected Cornet-TS message received from client`

Type: **Minor**

Unknown/unexpected Cornet-TS message received from client. Check client

MSG_HFAM_LIH_IPADR_TOO_LONG_ERR

`EventText: IP-address too long, cut !`

Type: **Major**

IP address was too long and was cut. Check client setup.

MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR

`EventText: SubNo too long, cut !`

Type: **Major**

Subscriber number was too long and was cut. Check client setup.

MSG_HFAM_LIH_ALGORITM_OBJID_ERR

`EventText: SubNo too long, cut !`

Type: **Major**

Algorithm object ID was too long and was cut. Check client setup.

MSG_HFAM_LIH_PROTOCOL_LIST_ERR

`EventText: too many elements in protocol list`

Type: **Major**

Too many elements in the protocol list. Check client setup.

MSG_HFAM_LIH_RETURNED_SOCKET_ERR

`EventText: returned socket error`

Type: **Major**

Returned socket error. LAN-side error.

MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR

`EventText: timeslot is valid`

Type: **Major**

Login timer for a client could not be started. Start HFA Manager.

MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR

`EventText: Input Parameter for hfam_sih_send_ts invalid`

Type: **Major**

Input parameter for `hfam_sih_send_ts` invalid. System-side error.

MSG_HFAM_SIH_CORNET_LONGER_28_ERR

`EventText: cannot synthesize CorNet-TS message longer than 28 bytes`

Type: **Major**

Cannot synthesize CorNet-TS messages longer than 28 bytes. System-side error.

MSG_HFAM_MON_NO_MON_TIMER_ERR

`EventText: No monitor timer !`

Type: **Minor**

No monitor timer. Start HFA Manager.

MSG_HFAM_REG_LOGIN_NOTREG_ERR

`EventText: DL_LOGON_IN received for client not in not_registered state, subno`

Type: **Minor**

`DL_LOGON_IN` received for client not in registered state. HFA Manager-internal.

MSG_HFAM_REG_SUBNO_TOO_LONG_ERR

`EventText: DL_LOGON_IN received for client not in not_registered state`

Type: **Major**

SubNo in `DL_LOGON_IN` too long and was cut. Check client setup in system.

MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR

`EventText: SubNo from System I/F not found in config data`

Type: **Minor**

SubNo from system I/F not found in config data. Check client setup in system.

MSG_HFAM_REG_ESTAB_NOTREG_ERR

`EventText: DL_EST_IN arrived for client not in registered state`

Type: **Minor**

`DL_EST_IN` received for the client not in registered state. Check system setup or WBM.

MSG_HFAM_REG_RELIN_NOTREG_ERR

`EventText: DL_REL_IN arrived for client not in registered state`

Type: **Minor**

`DL_REL_IN` received for the client not in registered state. Check system setup or WBM.

MSG_HFAM_REG_MISSING_L2INFO_ERR

`EventText: missing L2addr-InfoElem, no IP address`

Type: **Minor**

`L2addr-InfoElem` missing, no IP address. Check system setup or WBM.

MSG_HFAM_REG_LOGON_REJECT_ERR

`EventText: logon of client->subscriber_no rejected`

Type: **Information**

Logon of client subscriber number was rejected. Check system setup.

MSG_HFAM_REG_INVAL_PWD_LEN_ERR

`EventText: invalid password length of <sub_number>, no hash`

Type: **Minor**

Invalid password length for <sub_number>, no hash. Check client setup or WBM.

9.2.18 HFA Adapter Events

MSG_HFAA_MESSAGE_ERROR

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

Type: **Warning**

Received unexpected or unknown message.

MSG_HFAA_PARAM_ERROR

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

Type: **Major**

Mandatory parameter missing or contains an invalid value.

MSG_HFAA_MEMORY_ERROR

`EventText: ?*?Can't access/allocate memory`

Type: **Major**

Application doesn't get requested memory or constructor returns null pointer.

MSG_HFAA_INTERNAL_ERROR

`EventText: %s`

Type: **Major**

Internal error in HFA Adapter.

MSG_HFAA_INTERNAL_EVENT

`EventText: %s`

Type: **Information**

Successful startup or shutdown of application.

9.2.19 PPP Call Control Events

None implemented at the moment.

9.2.20 PPP MANAGER Events

MSG_PPPM_ERR_CONFIG

`EventText: %p`

Types: **Critical, Major, Minor**

Inconsistency in configuration data. Error in Admin receiver. Examine configuration data for PPP systematically. Inform Software Development Department, provide the trace files (PPPM_TBAS, PPPM_TSTD, PPPM_TEXT Level 9) that document this corrupt behavior.

MSG_PPPM_ERR_OPERATION

`EventText: %p`

Types: **Critical, Major, Minor**

Unexpected condition during operation. Inform Software Development Department, provide the trace files (PPPM_TBAS, PPPM_TSTD, PPPM_TEXT Level 9) that document this corrupt behavior.

9.2.21 PPP Stack Events

MSG_PPP_STACK_PROC

`EventText: %p`

Types: **Major, Minor, Warning**

Internal PPP stack processing error. Inform Software Development Department, provide the trace files (PPP_STACK_PROC Level 6 and PPP_STACK_DBG_IF Level 9) that document this corrupt behavior.

9.2.22 SPE Events

MSG_SPE_CERT_MISSING

Certificate for Signaling and Payload Encryption (SPE) is not available.

MSG_SPE_CERT_AVAIL

Certificate for Signaling and Payload Encryption is available.

MSG_SPE_CERT_UPDATED

Certificate for Signaling and Payload Encryption was updated.

MSG_SPE_CERT_EXPIRED

Certificate for Signaling and Payload Encryption has expired.

MSG_SPE_CERT_TIMEREMAINING

Certificate for Signaling and Payload Encryption, remaining time

MSG_SPE_CRL_EXPIRED

Certificate revocation list for SPE has expired.

MSG_SPE_CRL_UPDATED

Certificate revocation list for SPE was updated.

MSG_SPE_ALL_CRLS_UPTODATE

All certificate revocation lists for SPE are up to date.

9.2.23 VCAPI Events

MSG_BSD44_SELECT_ERROR

`EventText: Select error for VCAPI & DATAGW Dispatcher`

Type: **Major**

Sockets for VCAPI and DATAGW clients not working anymore.

MSG_BSD44_ACCEPT_ERROR

`EventText: Accept error for VCAPI Dispatcher`

Type: **Major**

Not possible to set up a new connection for VCAPI.

MSG_VCAPI_NO_CAPI_DATA

`EventText: No CAPI data in message with event 0x%x`

Type: **Minor**

No data in the message received from VCAPI server or from `CAPI_PAYLOAD_INT`.

MSG_VCAPI_WRONG_LINKNUM

`EventText: Wrong link number %d in message %s`

Type: **Minor**

Wrong link number in the message received from VCAPI server or from `CAPI_PAYLOAD_INT`.

MSG_VCAPI_LINK_TABLE_FULL

`EventText: No free element found in VS_Plci_Link table`

Type: **Major**

Too many physical link connections are not released correctly.

MSG_VCAPI_NO_PLCI

`EventText: PLCI not found in VS_Plci_Link table (to find message_nbr)`

Type: **Major**

PLCI not found in `VS_Plci_Link` (needed to find `message_nbr`).

MSG_VCAPI_CONV_H2N_ERROR

`EventText: Conversion error:%d`

Type: **Minor**

Message to client is not converted correctly.

MSG_VCAPI_CONV_H2N_FAILED

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

Type: **Minor**

Conversion returns wrong value.

MSG_VCAPI_WRONG_CONV_H2N

`EventText: Wrong conversion for %s`

Type: **Minor**

Message not converted (wrong message).

MSG_VCAPI_WRONG_MSG_LENGTH

`EventText: Wrong message length %d`

Type: **Minor**

The total length of the CAPI message is wrong.

MSG_VCAPI_CONV_N2H_FAILED

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

Type: **Minor**

Conversion returns wrong value.

MSG_VCAPI_WRONG_CONV_N2H

`EventText: Wrong conversion for %s`

Type: **Minor**

Message not converted (wrong message).

MSG_VCAPI_UNKNOWN_MSG_N2H

`EventText: unknown msg %s`

Type: **Minor**

Wrong subcommand in message.

MSG_VCAPI_TOO_MANY_CLIENTS

`EventText: Too many clients connected`

Type: **Warning**

No free element found in the connection table. Connection will be closed.

MSG_VCAPI_ACCEPT_ERROR

`EventText: Accept error for VCAPI Dispatcher`

Type: **Major**

Not possible to set up a new connection for VCAPI.

MSG_VCAPI_DISP_NOT_READY

`EventText: VCAPI Dispatcher not ready`

Type: **Major**

The VCAPI server did not send `VCAPI_EVENT_START_OPERATION_REQ` to the dispatcher.

MSG_VCAPI_NO_CLIENT

`EventText: no client address`

Type: **Minor**

No client address.

MSG_VCAPI_WRONG_BUF_LEN

`EventText: Wrong buffer length %d`

Type: **Minor**

Buffer length not within the message limits.

MSG_VCAPI_NO_RCV_BUFFER

`EventText: rcvBufPP=0x%x null`

Type: **Minor**

Receive buffer either already cleared or not possible to allocate memory.

MSG_VCAPI_NO_ALLOC_SINGLE

`EventText: Not possible to allocate a single buffer`

Type: **Minor**

Not possible to get a single receive buffer (allocation error).

MSG_VCAPI_NO_ALLOC_EXTENDED

`EventText: Not possible to allocate an extended buffer`

Type: **Major**

Not possible to get an extended receive buffer (allocation error). The gateway performs an automatic restart.

MSG_VCAPI_BUF_NOT_CREATED

`EventText: Not possible to create buffer with size:%d`

Type: **Major**

Not possible to create buffer with the expected length.

MSG_VCAPI_NO_NEW_BUF

`EventText: No new buffer created by vs_bputd`

Type: **Major**

Not possible to create a new buffer to store the received data (allocation error). The gateway performs an automatic restart.

MSG_VCAPI_DATA_NOT_STORED

`EventText: Not possible to get a receive buffer,data not stored`

Type: **Major**

Received data not stored because new buffer could not be allocated (allocation error). The gateway performs an automatic restart.

MSG_VCAPI_SOCKET_NOT_OPEN

`EventText: VCAPI-Socket not opened`

Type: **Major**

Socket couldn't be opened (connections with clients not possible).

MSG_VCAPI_SOCKET_BIND_ERR

`EventText: bind error for socket %d`

Type: **Major**

Bind error for VCAPI socket (connections with clients not possible).

MSG_VCAPI_LISTENING_ERR

`EventText: listening error for socket %d`

Type: **Major**

Not possible to create a listening VCAPI socket (connections with clients not possible).

MSG_VCAPI_RECEIVE_ERR

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

Type: **Minor**

Error while receiving message for VCAPI Dispatcher.

MSG_VCAPI_NO_ALLOC_MSG

`EventText: Not possible to allocate a buffer`

Type: **Major**

Not possible to send a message to VCAPI Dispatcher because no buffer could be allocated (allocation error). The gateway performs an automatic restart.

MSG_VCAPI_WRONG_EVENT_SRV

`EventText: wrong eventcode from VCAPI_SERVER`

Type: **Warning**

VCAPI Dispatcher has received wrong event from VCAPI server.

MSG_VCAPI_PLCI_NOT_FOUND

`EventText: PLCI not found in VS_Plci_Link table`

Type: **Minor**

PLCI not found in `VS_Plci_Link` table when receiving a message from `CAPI_PAYLOAD_IF`.

MSG_VCAPI_IND_ALLOC_ERR

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

Type: **Major**

Not possible to allocate a buffer for `CMT_DATA_IND`. Message cannot be sent to client. The gateway performs an automatic restart.

MSG_VCAPI_CONF_ALLOC_ERR

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

Type: **Major**

Not possible to allocate a buffer for CMT_DATA_CONF. Message cannot be sent to client. The gateway performs an automatic restart.

MSG_VCAPI_WRONG_EVENT_CAPI

EventText: Nwrong eventcode from CAPI_PAYLOAD_INTERFACE

Type: **Warning**

VCAPI Dispatcher has received wrong event from CAPI_PAYLOAD_IF.

MSG_VCAPI_WRONG_LENGTH_MSG

EventText: Wrong message length %d

Type: **Warning**

Length of message from client to VCAPI server/CAPI_PAYLOAD_IF is incorrect.

MSG_VCAPI_NO_PLCI_DATA_B3

EventText: PLCI not found in VS_Plci_Link table (for DATA_B3_REQ)

Type: **Minor**

PLCI not found in VS_Plci_Link table (for DATA_B3_REQ). Message cannot be sent to CAPI_PAYLOAD_IF.

MSG_VCAPI_DATA_B3_ALLOC_ERR

EventText: ALLOC ERROR: returncode %x

Type: **Major**

Not possible to get a buffer to send the DATA_B3_REQ message to CAPI_PAYLOAD_IF (allocation error). The gateway performs an automatic restart.

MSG_VCAPI_NO_PLCI_DISCONNECT

EventText: PLCI Element not found in VS_Plci_Link table for DISCONNECT_RESPONSE

Type: **Minor**

PLCI element not found in VS_Plci_Link table for the DISCONNECT_RESPONSE message.

MSG_VCAPI_MSG_NOT_SEND

EventText: not possible to send message

Type: **Warning**

Not possible to send a message. Interface to CAPI_PAYLOAD returns -1.

MSG_VCAPI_NO_LIST_SOCKET

EventText: no listening socket stored in connection table

Type: **Major**

No listening socket stored in connection table. A new connection cannot be opened.

MSG_VCAPI_RCV_LEN_ERR

`EventText: Wrong message length at receive data from client`

Type: **Warning**

Wrong message length on receipt of data from client. Connection will be closed. Message is not sent to VCAPI server.

MSG_VCAPI_SOCKET_RCV_ERR

`EventText: Error on receiving data from the Socket (connection interrupted)`

Type: **Warning**

Connection has been interrupted causing an error on receipt of data.

MSG_VCAPI_SOCK_NOT_AVAIL

`EventText: connected socket not stored in connection table`

Type: **Minor**

Connected socket not stored in connection table. Not possible to receive data.

MSG_VCAPI_UNKNOWN_NTFY

`EventText: Unknown notification. Used value:%d`

Type: **Warning**

Unknown notification.

MSG_VCAPI_NO_LNK_CONN

`EventText: Link number not found in connection table`

Type: **Minor**

Link number not found in connection table.

9.2.24 VCAPI Application Events

MSG_VCAPI_SERVER_ERROR

`EventText: VCAPI Server error: %p`

Type: **Warning**

Various VCAPI Server errors from the HXG2 code.

MSG_VCAPI_UNANTICIPATED_MESSAGE

`EventText: Unanticipated Message %s for CSID %s in state %s`

Type: **Warning**

The CAPI Manager has received an unanticipated message for the current state of the relevant CAPI object.

MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE

`EventText: Unanticipated CAPI message %s`

Type: **Warning**

The CAPI Manager has received an unanticipated CAPI message with an unknown command and subcommand.

MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE

`EventText: Unanticipated VCAPI Dispatcher message %d`

Type: **Warning**

The VCAPI Server has received a VCAPI Dispatcher message with an unknown event.

MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE

`EventText: Unanticipated Message Base %m`

Type: **Warning**

The VCAPI Server, the VCAPI Interface or CAPI Manager has received a message base with an unanticipated ID.

MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT

`EventText: Part of the CAPI Message is missing (%d > %d)`

Type: **Warning**

The length of the CAPI message is greater than the size of the VB string containing this CAPI message.

MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG

`EventText: Message Base without CAPI message`

Type: **Warning**

The VCAPI Server, the VCAPI Interface or the CAPI Manager has received a `CapiInd` or `CapiReq` not containing the required CAPI message.

MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG

`EventText: MMessage Base without Data GW message`

Type: **Warning**

The CAPI Manager has received a message base not containing the required VCAPI Dispatcher message from NU or from the Data GW dispatcher.

MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG

`EventText: Message Base without VCAPI Dispatcher message`

Type: **Warning**

The VCAPI Server has received a message base not containing the required VCAPI Dispatcher message from the VCAPI Dispatcher.

MSG_VCAPI_ILLEGAL_LINK_NUMBER

`EventText: Illegal link number: %d`

Type: **Warning**

An attempt was made to address a member of the dynamic link table with an illegal index.

MSG_VCAPI_ILLEGAL_PARTNER_NUMBER

```
EventText: Illegal partner number: %d
```

Type: **Warning**

An attempt was made to address the info of a non-allocated VCAPI partner.

MSG_VCAPI_ADD_OBJECT_FAILED

```
EventText: Could not add a CAPI object to the managed
object list
```

Type: **Major**

A newly created CAPI object could not be added to the managed object list. The gateway performs an automatic restart.

MSG_VCAPI_COULD_NOT_CREATE_OBJECT

```
EventText: Could not create a CAPI object
```

Type: **Warning**

A new CAPI object could not be created.

MSG_VCAPI_COULD_NOT_DELETE_OBJECT

```
EventText: Could not delete a CAPI object
```

Type: **Major**

The specified CAPI object could not be deleted. The gateway performs an automatic restart.

MSG_VCAPI_NO_PLCI_AVAILABLE

```
EventText: No PLCI available
```

Type: **Warning**

All available PLCIs are seized.

MSG_VCAPI_CSID_MISSING

```
EventText: CSID is missing
```

Type: **Warning**

The CAPI Manager has received a message from NU or from CCP that doesn't contain a call and session ID.

MSG_VCAPI_COULD_NOT_FIND_PLCI

```
EventText: Could not find the corresponding PLCI
```

Type: **Warning**

The PLCI belonging to a given call and session ID or to a given channel ID could not be found.

MSG_VCAPI_COULD_NOT_FIND_OBJECT

```
EventText: Could not find the corresponding CAPI Object
```

Type: **Warning**

The CAPI object belonging to a given call and session ID could not be found.

MSG_VCAPI_COULD_NOT_FIND_CSID

`EventText: Could not find the corresponding CSID`

Type: **Warning**

The call and session ID belonging to a given PLCI could not be found.

MSG_VCAPI_COULD_NOT_STORE_REQ

`EventText: Could not store the request %x %x for PLCI %d`

Type: **Major**

No more space available in the CAPI interface to store the request. The gateway performs an automatic restart.

MSG_VCAPI_CONF_WITHOUT_REQ

`EventText: Confirmation %x %x for PLCI %d without stored Request`

Type: **Warning**

The CAPI interface has received a confirmation without the relevant stored request.

9.2.25 H.323 Client Events

MSG_H323CLIENT_INVALID_CLIENTID

`EventText: invalid Peer ID: %d`

Type: **Major**

Software error: index of client table incorrect. Stop the H323Client-Internal trace profile.

MSG_H323CLIENT_INVALID_ADMIN_MSG

`EventText: invalid admin message for file %s received`

Type: **Minor**

Error received while reading/writing configuration files. Stop the H323Client-Internal trace profile.

MSG_H323CLIENT_NWRS_ENTRY_FAILED

`EventText: create %s entry failed for client (%I, %I)`

Type: **Major**

Creation of the NWRS entry failed. Stop the H323Client-Internal trace profile.

MSG_H323CLIENT_INVALID_PARAM

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

Type: **Major**

Software error: invalid parameter. Stop the H323Client-Internal trace profile.

MSG_H323CLIENT_MAPS_DIFFER

`EventText: size of maps differ (call no: %I, IP: %I)`

Type: **Major**

Software error: invalid parameter. Stop the H323Client-Internal trace profile.

9.2.26 IPNC Events

MSG_IPNC_MESSAGE_ERROR

`EventText: message error: %s`

Type: **Major**

Unexpected message received - will be ignored. Stop the IPNC-Std trace profile.

MSG_IPNC_MESSAGE_DUMP

`EventText: message error: %s% M`

Type: **Major**

Unexpected message received - will be ignored. Stop the IPNC-Std trace profile.

MSG_IPNC_PARAM_ERROR

`EventText: message parameter error: %s %x`

Type: **Major**

Message with invalid parameter received - will be ignored. Stop the IPNC-Std trace profile.

MSG_IPNC_INTERNAL_ERROR

`EventText: internal error: %I`

Type: **Major**

Software error: invalid internal data detected. Stop the IPNC-Detailed trace profile.

MSG_IPNC_INCONSISTENT_STATE

`EventText: inconsistent internal state: %s %x`

Type: **Major**

Software error: data became inconsistent during processing. Stop the IPNC-Std trace profile.

MSG_IPNC_CP_ASYNCH

`EventText: CP and IPNC asynchronous: %s %s`

Type: **Major**

Asynchronism between states of HiPath-CP and IPNC detected. Stop the IPNC-Std trace profile.

9.2.27 IPNCA Events

MSG_IPNCA_ERROR

`EventText: IPNC Adapter: (some) Error description ("IPNC Adapter: %s")`

Type: **Minor**

A minor error has occurred.

9.2.28 MPH Events

MSG_MPH_INFO

`EventText: %p SGP Message not sent`

Type: **Information**

Event log for all MPH events. SGP message cannot be sent to IPNC.

9.2.29 OAM Events

MSG_TLS_MUTEX_BLOCKED

`EventText: Mutex blocked`

Type: **Major**

Software error: deadlock. Reboot the gateway; create error report.

MSG_DISP_SENDER_NOT_SET

`EventText: Sender not set in message: %n%M`

Type: **Critical**

Internal software error. Message header not set. Event is always followed by an ASSERT event, which causes an automatic reboot.

MSG_OAM_TIMESYNC

`EventText: Time Synchronization from %s to %s`

Type: **Information**

Time synchronization took place.

MSG_OAM_TIMESYNC_FAILED

`EventText: Time Synchronization failed`

Type: **Warning**

Time synchronization not performed.

MSG_OAM_PRIO_INCREASED

`EventText: Priority of %s increased`

Type: **Warning**

Priority of an OAM task (trace, event, OAM) was increased because of heavy load. This is still valid behavior.

MSG_OAM_PRIO_SWITCHED_BACK

`EventText: Priority of %s switched back. OAM Msg Queue OK`

Type: **Cleared**

Priority of an OAM task (trace, event, OAM) was decreased because the heavy load no longer exists. This is still valid behavior.

MSG_OAM_QUEUE_FULL

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

Type: **Major**

Queue of OAM tasks (trace, event, OAM) full. All messages are removed.

MSG_OAM_PUT_TO_QUEUE_FAILED

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

Type: **Major**

The addition of OAM tasks (trace, event, OAM) to the message queue failed for no apparent reason. All messages are removed.

MSG_OAM_QUEUE_BLOCKED

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

Type: **Major**

The addition of OAM tasks (trace, event, OAM) to the message queue failed. Reason: queue blocked. All messages are removed.

MSG_OAM_INTERNAL_EVENT

`EventText: %p`

Type: **Warning**

Execution of an automatic action failed.

MSG_ADMIN_LOGGED_IN

`EventText: %s user \"%s\" (session id = %d) logged in`

Type: **Information**

Information about successful administrator login.

MSG_ADMIN_SESSION_CREATED

`EventText: %s session created for user \"%s\" (session id = %d)`

Type: **Information**

A session for an administrator or an automatic login procedure (such as AutoDiscovery or data transfer from OpenScape 4000 V10 to HG 3500/3575) was created.

MSG_ADMIN_LOGGED_OUT

```
EventText: %s user \"%s\" (session id = %d) logged out
```

Type: **Information**

Information about successful administrator login.

MSG_ADMIN_INVALID_LOGIN

```
EventText: Invalid login from %s (user \"%s\")
```

Type: **Information**

Invalid login attempt.

MSG_ADMIN_SESSION_EXPIRED

```
EventText: Session id = %d of user \"%s\" expired
```

Type: **Information**

Session expired (session timeout reached). New login necessary.

MSG_ADMIN_GOT_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) got write
access
```

Type: **Information**

Administrator has write access. He can therefore change the gateway configuration.

MSG_ADMIN_DIDN'T_GET_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) didn't get
write access
```

Type: **Information**

Administrator has not been granted write access. Another administrator already has write access. Wait for or force write access (for example, via WBM).

MSG_ADMIN_RELEASED_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) released write
access
```

Type: **Information**

An administrator has released write access and cannot perform any more changes on the gateway configuration. Now other administrators can be granted write access.

MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS

```
EventText: %s user \"%s\" (session id = %d) released write
access
```

Type: **Information**

The current administrator was forced to release write access because another administrator took over write access. The gateway can now be changed by the other administrator only.

MSG_CAR_CALL_ADDR_REJECTED

`EventText: Call address rejected %s`

Type: **Minor**

The specified call address was rejected.

MSG_WEBSERVER_INTERNAL_ERROR

`EventText: %p`

Type: **Warning**

Internal error on the web server, internal exception situation which does not impact other web server activities however.

9.2.30 CLI Events

MSG_CLI_TELNET_ABORTED

`EventText: Telnet client \"%s\" aborted`

Type: **Warning**

Telnet client disconnected before logging in.

MSG_CLI_LOGGED_IN_FROM_TELNET

`EventText: User \"%s\" logged in (session id = %d) from telnet CLI with IP address %s`

Type: **Information**

Telnet client successfully logged in.

MSG_CLI_LOGGED_IN_FROM_V24

`EventText: User \"%s\" logged in (session id = %d) from V24 CLI`

Type: **Information**

A user has successfully logged in via the V.24 inferface.

9.2.31 HIP Events

MSG_HIP_ALLOC_DEV_OBJ

`EventText: hi_main: Device allocation memory not possible`

Type: **Warning**

No heap space for device data. Check available memory.

MSG_HIP_NO_MEM_CLBLK

`EventText: hi_main: No memory for Cluster block available`

Type: **Warning**

No space available for cluster block. Check why no allocatable memory is available in the gateway.

MSG_HIP_NO_MEM_CL

`EventText: hi_main: No memory for Cluster %d available`

Type: **Warning**

No space available for cluster. Check why no allocatable memory is available in the gateway.

MSG_HIP_NO_NETPOOL_INIT

`EventText: NETPOOL INIT not possible: Return value %d`

Type: **Warning**

Initialization of netpool for HIP not possible. Check return value %d and take appropriate measures.

MSG_HIP_NO_OBJ_INIT

`EventText: No initialization of END_OBJ Structure possible`

Type: **Warning**

Initialization of `END_OBJ` for HIP not possible. Check `END_OBJ` pointer and memory.

MSG_HIP_NO_DEVLOAD

`EventText: hi_main:Loading device into MUX not possible, unit = %d, pendLoad = %X,Pinitstring = %X, Loaning = %d,pBSP = %X`

Type: **Warning**

Loading HIP device in MUX not possible. Check parameters transferred to `muxDevLoad`.

MSG_HIP_NO_DEVSTART

`EventText: I_main: Start HIP device not Possible, return value = %X`

Type: **Warning**

Starting HIP device in MUX not possible. Check return value %X and take appropriate measures.

MSG_HIP_NO_MEM_TO_SI

`EventText: SI_main: allocating of memory for message to SI not possible`

Type: **Warning**

Allocation of memory for message to system interface not possible. Check why no allocatable memory available at gateway.

MSG_HIP_NO_CLPOOL_ID

`EventText: hi_main: No clusterpool ID available`

Type: **Warning**

No cluster pool ID available for sending a packet to an IP via MUX. Check for problem.

MSG_HIP_NO_CLUSTER

`EventText: I_main:No cluster available to make packet,packet_len = %d`

Type: **Warning**

Cluster of requested length not available. The problem may be that not enough clusters of a certain length are free or that the clusters have not been released.

MSG_HIP_NO_CLBLK

`EventText: No clusterblock for netpool available`

Type: **Warning**

No more cluster blocks. Number of defined cluster blocks too low.

MSG_HIP_NO_PMBLK

`EventText: No memory block for incoming messages from MUX`

Type: **Warning**

MUX calls HIP without a pointer to a memory block. Check the interface IP > MUX -> HIP.

MSG_HIP_PKTLEN_ZERO

`EventText: Packet length from MUX = zero`

Type: **Warning**

Length of packet from MUX is 0. Inform person responsible for IP about this message.

MSG_HIP_ALLOC_MES_SI

`EventText: No allocation for message SI possible`

Type: **Warning**

Could not send message from HIP to system interface. Check available memory.

MSG_HIP_PMBLK_ZERO

`EventText: Length of packet from Mux is zero`

Type: **Warning**

Length of packet from MUX is 0. Inform person responsible for IP/MUX about this message.

9.2.32 SI Events (System Interface Events)

MSG_SI_L2STUB_STREAM_ALREADY_OPEN

`EventText: Stream already open for device %X`

Type: **Warning**

Device has already been opened using the `SI_open` procedure. Check MAL to determine why it calls `SI_open` twice.

MSG_SI_L2STUB_COUDNT_OPEN_STREAM

`EventText: Stream couldn't be opened for device %X`

Type: **Warning**

Error in Vxworks-Costream for opening a data channel for a device. Check maximum number of devices and interpret the error code.

MSG_SI_L2STUB_ERROR_INIT_DRIVER

`EventText: Critical Error in Initializing L2 driver`

Type: **Critical**

Initialization of L2 not possible. Check error code in Vxworks.

MSG_SI_L2STUB_NO_CLONE

`EventText: Unsupported non-Clone open!`

Type: **Warning**

A non-clone entity not supported has been opened.

MSG_SI_L2STUB_OPEN_OTHER_STREAM_NOT_POSSIBLE

`EventText: Unable to open another L2 stream`

Type: **Warning**

Check the Vxworks error code.

MSG_SI_L2STUB_UNEXPECTED_DB_TYPE

`EventText: Unexpected db_type (0x%x)"`

Type: **Warning**

The message type is not allowed for DLPI.

MSG_SI_L2STUB_NO_ALLOC

`EventText: Unable to allocb(%d)`

Type: **Critical**

Out of memory. The gateway performs an automatic restart. An SNMP trap is generated. Further measures not required.

MSG_SI_L2STUB_PORT_NOT_OPEN

`EventText: Port has not been opened`

Type: **Warning**

Port must be opened before transfer can be performed. Check why port is closed.

MSG_SI_L2STUB_UNKNOWN_SOURCE_PID

`EventText: PSource PID not known (0x%x)`

Type: **Warning**

Message from unknown PID. Check who has sent this message.

MSG_SI_L2STUB_UNEXPECTED_EVENT_CODE

`EventText: Unexpected event code (%d) from SWU`

Type: **Warning**

Event code sent from HiPath 3000 not known. Check DH in HiPath 3000.

9.2.33 MAGIC/Device Manager Events

9.2.33.1 Startup and Internal Messages

MSG_DEVM_NO_PROTOCOL_FOR_DEVICE

```
EventText: Device %u could not be bound to protocol %d.
Device has been taken out of service
```

Type: **Major**

Specified device couldn't be assigned to a protocol and is therefore "out-of-service". Check and correct content of file 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
```

Type: **Major**

Specified device couldn't be assigned to a protocol and is therefore "out-of-service". Check and correct content of persistent file devmgr.txt.

MSG_DEVM_BINDING_FAILED

```
EventText: Protocol rejected. Device '%u' will be taken out
of service
```

Type: **Major**

Invalid protocol specified in persistent file. Check and correct content of persistent file devmgr.txt.

MSG_DEVMGR_DEVICEID_OUT_OF_RANGE

`EventText: The current DeviceId: %d is out of range`

Type: **Major**

Specified device ID is outside valid range. Check and correct content of persistent file devmgr.txt.

MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE

```
EventText: No Device Type for %s Device available in
persistency
```

Type: **Major**

Invalid device type in persistent file. Check and correct content of persistent file devmgr.txt.

MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE

`EventText: No Device Type for %s Device available in persistency`

Type: **Major**

No entry found in persistent file for specified device type. Check and correct content of persistent file devmgr.txt.

MSG_DEVMGR_CREATE_FAILED

`EventText: %s create failed`

Type: **Major**

Device object entity of specified class could not be created. Not enough memory. Restart system.

MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY

`EventText: Can not read %s persistency file`

Type: **Major**

Specified persistent file cannot be read. Check persistent files. Restart system.

MSG_DEVMGR_SCN_TASK_FAILED

`EventText: SCN Task create failed`

Type: **Major**

Class entity of `SCN_TASK` cannot be created; startup interrupted. Restart system.

MSG_DEVMGR_INTERROR_DEVID

Type for following event texts: **Major**

`EventText: SCN Task create failed`

Could not find a valid device pointer in the global device table.

`EventText: DeviceId (%x): Got NULL pointer instead of Resource!`

A null pointer to a resource occurred.

`EventText: DeviceId (%x): No container object found!`

Could not find a valid object pointer in the global table.

`EventText: DeviceId (%x): No protocol manager found!`

Could not find a valid protocol manager.

`EventText: DeviceId (%x): No protocolId in message!`

Could not read protocol ID from persistent file. Check and correct content of persistent file devmgr.txt.

`EventText: DeviceId (%x): If Table init failed, DVMGR not initialized!`

Error in system startup. Could not create IF tables. Restart system. If problem persists, a new APS will be required.

`EventText: DeviceId (%x): Startup failed, DVMGR not initialized!`

Error in system startup. Could not start device manager. Restart system. If problem persists, a new APS will be required.

`EventText: DeviceId (%x): is not a fax deviceId. Could not set fax status.`

Got a wrong device ID.

`EventText: DeviceId (%x): Got NULL pointer !!!`

Received a null pointer.

`EventText: DeviceId (%x): No free channel found!`

Could not find a free channel.

`EventText: DeviceId (%x): Unknown Device Type!`

Unknown device type received. Check and correct content of persistent file devmgr.txt.

`EventText: DeviceId (%x): Device %d can't be created!`

Could not create device. No connections possible for this device.

`EventText: DeviceId (%x): Insert in global Device Table failed!`

Inserting in global device table failed. This device will not be known to the system.

Type for following event text: **Minor**

`EventText:` DeviceId (%x): Not enough memory to create Resource object!!

Not enough memory to create a resource.

Type for following event texts: **Warning**

`EventText: DeviceId (%x): Amount of configured resources exceeds overall limit.`

The number of total resources is less than the number of resources assigned to this device. Check configuration of resources in devmgr.txt.

`EventText: DeviceId (%x): Unexpected SUSY id !!!`

Got an unexpected SUSY ID.

`EventText: DeviceId (%x): iAdmCommand: Unexpected value received`

Got an unexpected command.

`EventText: DeviceId (%x): id >= MAX_RESOURCE_NUMBER!`

Got wrong resource.

`EventText: DeviceId (%x): Wrong param from persistency file gwglobal.txt!`

Could not read parameter from persistent file. Check and correct content of persistent file gwglobal.txt.

`EventText: DeviceId (%x): BChannel not found in resources!`

Could not find B channel in resources.

`EventText: DeviceId (%x): Got a LOGON_TRK_IND msg for wrong device!`

Got a message for wrong device.

`EventText: DeviceId (%x): Unknown resource state!`

Resource state unknown.

`EventText: DeviceId (%x): Configured Trunk Channels exceed physical Limit!`

The configured trunk channels (Manager E) exceed the number of physical B channels.

Type for following event texts: **Information**

`EventText: DeviceId (%x): Unknown AdminState! AdminState set to AStateDown`

Unknown admin state.

`EventText: DeviceId (%x): Shutdown of SCN_Task failed! Continue with Shutdown.`

Shutdown of `SCN_TASK` failed. Shutdown will be continued anyway.

MSG_DEVMGR_INTERROR_RESID

Type for following event texts: **Warning**

`EventText: ResourceId (%x): Fax Indication received from wrong device`

Wrong device type.

`EventText: ResourceId (%x): No ASCII character defined for digit %d`

Wrong digit.

`EventText: ResourceId (%x): G711TransparentChannel Indication not from SCN-side`

Wrong indication.

`EventText: ResourceId (%x): State RESOURCE_IN_USE not set!`

Could not change state.

`EventText: ResourceId (%x): State RESOURCE_IDLE not set!`

Could not change state.

`EventText: ResourceId (%x): DecreaseResourceCounter() failed`

Decrease of the resource counter failed.

`EventText: ResourceId (%x): Leg not opened`

Leg is not opened yet.

`EventText: ResourceId (%x): No Codecs available!`

Did not find a codec. Calls not possible.

`EventText: ResourceId (%x): Codec value out of range!`

Unknown codec.

`EventText: ResourceId (%x): Number of licenses out of range!`

Unknown codec quantity.

`EventText: ResourceId (%x): new state not expected!`

Got unexpected state.

`EventText: ResourceId (%x): Leg already in a connection`

The system's own Leg or the partner Leg is already connected. Reject command.

`EventText: ResourceId (%x): ChangeState(%d): N/A in state %s`

State cannot be changed due to wrong state.

`EventText: ResourceId (%x): Resource not in state RESOURCE_IN_USE`

Wrong state.

`EventText: ResourceId (%x): No Dtmf tone defined for character %c`

Wrong character.

Type for following event texts: **Major**

`EventText: ResourceId (%x): GOT NULL POINTER !!!`

Received a null pointer.

MSG_DEVMGR_INTERROR_CHNID

`EventText: ChannelId (%x): Channel out of range!`

Type: **Warning**

Wrong channel number.

MSG_DEVMGR_MSCERROR_RESID

Type for following event texts: **Warning**

`EventText: Could not connect Legs. TIMEOUT, Faxstatus not changed from MSC`

Legs could not be connected because of timeout.

`EventText: DCould not connect Legs; FAX_STATUS_ERROR from MSC`

Legs could not be connected because of `FAX_STATUS_ERROR` from MSC.

9.2.33.2 LEG Management Messages

MSG_DEVMGR_OPEN_LEG_FAILED

`EventText: Open of %s Leg failed; MSC Error Code %d`

Type: **Warning**

Payload Leg couldn't be opened; MSC responds with specified error code.

MSG_DEVMGR_OPEN_WRONG_RES_STATE

`EventText: Open of %s Leg failed; Resource State %d`

Type: **Warning**

Resource state unexpected. State not changed, but returns `false` to the caller.

MSG_DEVMGR_UPDATE_LEG_FAILED

`EventText: Update of %s Leg failed; MSC Error Code %d`

Type: **Warning**

Data of payload Leg could not be changed; MSC responds with specified error code.

MSG_DEVMGR_CONNECT_WRONG_LEGS

`EventText: Connect of %s Leg failed; Partner not a %s Leg`

Type: **Warning**

Partner Leg has a wrong Leg type, which is why the connection cannot be established.

MSG_DEVMGR_CONNECT_LEGS_FAILED

`EventText: Connect of %s Leg failed; MSC Error Code %d`

Type: **Warning**

Connection to specified Leg failed; MSC created specified error code.

MSG_DEVMGR_LISTEN_WRONG_RES_STATE

`EventText: ListenForConnect on %s Leg failed; State %d Mode %d`

Type: **Warning**

Listening on the fax channel failed due to either false state or false mode.

MSG_DEVMGR_CONNECT_WRONG_RES_STATE

`EventText: Connect on %s Leg failed; State %d Mode %d`

Type: **Warning**

Connection on the fax channel failed due to either false state or false mode.

MSG_DEVMGR_DISCONNECT_LEGS_FAILED

`EventText: Disconnect of %S Leg failed; MSC Error Code %d`

Type: **Warning**

Disconnect of payload Legs failed; MSC responds with specified error code.

MSG_DEVMGR_CLOSE_LEG_FAILED

`EventText: Close of %s Leg failed; MSC Error Code %d`

Type: **Warning**

Proper closing of payload Leg failed; closed anyway.

9.2.33.3 Layer2 Communication Messages

MSG_SCN_ERROR_12_MSG

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

Type: **Major**

Layer2 has sent an error message; logged only.

MSG_SCN_ADD_PARAMETER_FAILED

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

Type: **Major**

Add parameter failed.

MSG_SCN_DEV_NOT_IN_DEVLIST

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

Type: **Major**

Specified device not found in device list.

MSG_SCN_GET_ADMMSG_FAILED

`EventText: Reading message from admin stream failed`

Type: **Major**

A message cannot be read from the admin stream.

MSG_SCN_GET_LDAPMSG_FAILED

`EventText: Reading message for device %d failed`

Type: **Major**

A message cannot be read from the admin stream.

MSG_SCN_UNEXPECTED_L2_MSG

`EventText: Unexpected layer2 message on device %d`

Type: **Major**

Layer2 has sent an unexpected DLPI message; logging only.

MSG_SCN_OPERATION_ON_STREAM_FAILED

`EventText:` Operation on stream failed for device %u

Type: **Major**

Operation on specified stream failed.

MSG_SCN_POLL_FD

`EventText: Poll returned unexpected value -1`

Type: **Major**

Polling failed.

MSG_SCN_OPEN_STREAM_FAILED

`EventText: Open stream failed on device %d`

Type: **Major**

Opening communication path to Layer2 failed. Restart system.

MSG_SCN_UNEXPECTED_POLL_EVENT

`EventText: Unexpected poll event on device %u`

Type: **Major**

Got an unexpected event on the specified device.

MSG_SCN_BIND_FAILED

`EventText: Bind for device: %d failed`

Type: **Major**

Binding layer2 communication path failed. Restart system.

MSG_DEVMGR_LAYER2_SERVICE_TRAP

Type for following event texts: **Critical**

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Waiting for DL_CONNECT_IND`

Message from SI missing; layer2 not ready. An SNMP trap is generated.

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Initiated by Layer2`

SI takes layer2 out of service. No more calls possible for this device. An SNMP trap is generated.

`EventText: DEVMGR DevId: %d Layer2 Out-Of-Service; Initiated by Application/Operator`

Administrator takes Layer2 out of service. No more calls possible for this device. An SNMP trap is generated.

Type for following event text: **Information**

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

Layer2 is ready. Connections to this device possible. An SNMP trap is generated.

9.2.34 Important Platform Software Status Events

MSG_ASP_INFO

Type for following event texts: **Information**

`EventText: Booting DSP module #<nr> with <DSP SW Version > from < date>`

This message appears at startup and marks the beginning of the boot procedure of the DSP module.

`EventText: Loading ...`

This message is displayed at startup and marks the beginning of the DSP software download.

`EventText: Booting DSP Modules #<nr> done`

This message appears at startup and marks the successful conclusion of the boot procedure of the DSP module.

9.2.35 Major ASC Events

MSG_ASC_ERROR

`EventText: DSP channel not initialized`

Type: **Indeterminate**

Possibly a configuration problem. Verify the ASC configuration in the gateway.

9.2.36 Major ASP Events

MSG_ASP_ERROR

Type for following event texts: **Critical**

`EventText: Hardware Configuration invalid: <error string>`

Different DSP modules (DDM1, DDM2) plugged in. Check the DSP modules on the main board.

`EventText: DSP Error 7,<nr>,0,0,0,0...`

An RTP packet of invalid length may have been received from the LAN. Displayed on console only.

`EventText: DSP Error 9,<nr>,0,0,0,0...`

Space problem: something is blocked on the DSP side. Displayed on console only.

9.2.37 Minor ASP Events

MSG_ASP_INFO

`EventText: fec restarts because of high traffic on LAN - Restart counter <nr>`

Type: **Information**

This message appears every tenth time that the FEC sender is blocked by a collision or by high-volume traffic. Some packets are lost when FEC is restarted automatically. Monitor LAN traffic.

9.2.38 IP Filter Events

MSG_IPF_STARTED

`EventText: IP Filter started`

Type: **Information**

An IP filter object has been created.

MSG_IPF_STOPPED

`EventText: IP Filter stopped`

Type: **Information**

An IP filter object has been destroyed.

MSG_IPF_ON_OFF

`EventText: IP Filter is switched %s`

Type: **Information**

IP filter was switched ON/OFF.

MSG_IPF_PARAMETER

`EventText: Rule number %d: missing parameter %s`

Type: **Critical**

When reading the specified filter rule, could not read specified parameter.

9.2.39 MAC Filter Events

MSG_MAF_STARTED

`EventText: MAC Address Filter started`

Type: **Information**

A MAC address filter object has been created.

MSG_MAF_STOPPED

`EventText: MAC Address Filter stopped`

Type: **Information**

A MAC address filter object has been destroyed.

MSG_MAF_ON_OFF

`EventText: MAC Address Filter is switched %s`

Type: **Information**

MAC address filter was switched ON/OFF.

MSG_MAF_PARAMETER

`EventText: Rule number %d: missing parameter %s`

Type: **Critical**

When reading the specified filter rule, could not read specified parameter.

MSG_MAF_NO_OF_RULES

`EventText: Number of rules is bigger than the maximum of %d`

Type: **Critical**

The number of rules entered is greater than the predefined maximum.

MSG_MAF_NETBUFFER

`EventText: IP packet seems to be corrupt`

Type: **Critical**

An error occurred when trying to access the memory area where the IP packet should be.

MSG_MAF_ETHERNET_HEADER

`EventText: Cannot find ethernet header of IP packet`

Type: **Critical**

An error occurred when trying to access the Ethernet header of an IP packet.

9.2.40 IP Stack Events

MSG_IPSTACK_NAT_ERROR

`EventText: CNAT Error: %s`

Type: **Critical**

Critical error occurred during net address translation (NAT).

MSG_IPSTACK_SOH_ERROR

`EventText: Error occurred in Socket Handler`

Type: **Critical**

Error occurred in Socket Handler.

MSG_IPSTACK_INVALID_PARAM

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

Type: **Minor**

IP Stack receives invalid parameter.

9.2.41 DELIC Events

MSG_DELIC_ERROR

`EventText: delic mailbox fatal error; reboot delic`

Type: **Critical**

Reboot after a critical DELIC mailbox error. Reboot will be executed automatically. HiPath not informed.

9.2.42 Test Loadware Events

MSG_TESTLW_INFO

`EventText: Info: %p`

Type: **Information**

Information about TESTLW functions (successful initialization, etc.).

MSG_TESTLW_ERROR

`EventText: Error: %p`

Type: **Major**

Errors during initialization due to receipt of an unknown message, or with buffer and timer errors.

9.2.43 Fax Converter, HDLC and X.25 Events

MSG_FAXCONV_INFO

`EventText: Info: %p`

Type: **Information**

Information about Fax Converter module (successful initialization, operations, etc.).

MSG_FAXCONV_ERROR

`EventText: Error: %p`

Type for following errors: **Warning**

Errors during initialization, receiving an unknown message, buffer errors.

Type for following errors: **Major**

Errors opening Fax Converter module.

MSG_MSP_FAX_OVERLONG_PKT

n/a

MSG_T90_INFO

`EventText: Info: %p`

Type: **Information**

Information about T.90 protocol module (successful initialization, operations, etc.).

MSG_T90_ERROR

`EventText: Error: %p`

Type: **Warning/Major**

Errors during initialization, receiving an unknown message, buffer errors.

MSG_X25_INFO

`EventText: Info: %p`

Type: **Information**

Information about X.25 protocol module (successful initialization, operations, etc.).

MSG_X25_ERROR

`EventText: Error: %p`

Type: **Warning/Major**

Errors during initialization, receiving an unknown message, buffer errors.

MSG_X75_INFO

`EventText: Info: %p`

Type: **Information**

Information about X.75 protocol module (successful initialization, operations, etc.).

MSG_X75_ERROR

`EventText: Error: %p`

Type: **Warning/Major**

Errors during initialization, receiving an unknown message, buffer errors.

MSG_MSP_HDLC_INFO

`EventText: Info: %p`

Type: **Information**

Information about HDLC driver (successful initialization, operations, etc.).

MSG_MSP_HDLC_ERROR

`EventText: Error: %p`

Type: **Warning/Major**

Errors during initialization, receiving unknown messages, buffer errors and errors when opening HDLC driver.

9.2.44 IP Accounting Events

MSG_IPACCSRV_SOCKET_ERROR

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

Type: **Major**

A fatal error occurred at the socket interface. The gateway performs an automatic restart.

MSG_IPACCSRV_MEMORY_ERROR

`EventText: Memory allocation failed`

Type: **Major**

Application doesn't get requested memory. The gateway performs an automatic restart.

MSG_IPACCSRV_INTERNAL_ERROR

`EventText: Internal Error in IP Accounting (code: %d %s)`

Type: **Major**

Various errors, for example, when OAM returns an error code. The message is displayed.

MSG_IPACCSRV_MESSAGE_ERROR

`EventText: Wrong internal message (origin: %s, code %d)`

Type: **Warning**

Received unknown message from IP Counting or IP Accounting client. The message is displayed.

MSG_IPACCSRV_MARK_REACHED

`EventText: WIP Accounting data reached upper mark, it shall be read`

Type: **Warning**

Upper level in IP Counting table reached. An SNMP trap is generated. If IP Accounting information is to be processed, log onto the IP Accounting client.

MSG_IPACCSRV_OVERFLOW

`EventText: IP Accounting data has overflown`

Type: **Warning**

Upper level in IP Counting table reached. Data will be lost. An SNMP trap is generated. If IP Accounting information is to be processed, log onto the IP Accounting client.

MSG_IPACCSRV_LOGON

`EventText: Login of IP Accounting client: %s`

Type: **Information**

Depending on the dummy %s, provides information on whether logon was successful or not. The message is displayed. If logon was unsuccessful, check reason.

9.2.45 Endpoint Registration Handler (ERH) Trace Events

MSG_ERH_INFORMATION

`EventText: %p`

Type: **Information**

Important ERH information. Check this event in connection with other ERH events if necessary.

MSG_ERH_ERROR

`EventText: %p`

Type: **Warning**

Errors, which occurred during an ERH operation (if not classified in other event classes). To get more information create a trace with ERH_REGISTRATION, ERH_ADMISSION and ERH_CONFIGURATION and trace level 6.

MSG_ERH_REGISTRATION_ERROR

`EventText: %p`

Type: **Warning**

Errors, which occurred during ERH registration. To get more information create a trace with ERH_REGISTRATION, ERH_CONFIGURATION and trace level 6. Very often this error is caused by a corrupt configuration. In addition, read messages of type MSG_ERH_INFORMATION.

MSG_ERH_ADMISSION_ERROR

`EventText: %p`

Type: **Warning**

Errors, which occurred when endpoints were being set up or cleared down. To get more information create a trace with ERH_ADMISSION and trace level 6. Check the endpoints that are not working.

MSG_ERH_SECURITY_DENIAL

`EventText: %p`

Type: **Critical**

This indicates that the ERH has rejected a request for registration, de-registration, setup or cleardown of endpoints for security reasons. Check carefully whether this message was caused by a faulty configuration in the network, or whether it is the result of attacks from a network hacker.

MSG_ERH_SUB_OUT_OF_SERVICE

n/a

MSG_ERH_NO_LICENSE

`EventText: %p`

Type: **Warning**

Indicates that there are no ComScendo licenses for registering a H.323 endpoint. More licenses need to be configured in the license manager (Manager E).

9.2.46 IPNCV Events

MSG_IPNCV_SIGNALING_ERROR

`EventText: IPNCV Signaling Error: %s`

Type: **Warning**

Software error: invalid internal data found.

9.2.47 XMLUTILS Events

MSG_XMLUTILS_ERROR

`EventText: %d`

Type: **Major**

An error has occurred in the XMLUTILS component.

9.2.48 Error Events

MSG_OSF_PCS_ERROR

`EventText: %p`

Type: **Major**

OSF has discovered a major error.

9.2.49 LAN Signaling Events - CCE

CCE_GENERAL_ERROR

`EventText: ...`

Type: **Major, Minor, Warning, Information**

CCE error not resolved through interaction with PSS saving (e. g. interaction with a QDC client).

CCE_PSS_STORE_ERROR

`EventText: ...`

Type: **Major, Minor, Warning, Information**

CCE error resolved through interaction with PSS saving (e. g. interaction with a QDC client).

9.2.50 Events for LLC Operation

MSG_LLC_EVENT_MISSING_RESOURCE

`EventText: %p`

Type: **Information**

Important information about an LLC operation.

MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE

`EventText: %p`

Type: **Critical**

In the case of errors that arise during an LLC operation (provided they are not already classified in other event classes).

MSG_LLC_EVENT_MISSING_PARAMETER

`EventText: %p`

Type: **Critical**

Mandatory element missing from message.

MSG_LLC_EVENT_INVALID_PARAMETER_VALUE

`EventText: %p`

Type: **Warning**

Invalid message.

9.2.51 Client-Related Events

(Events in the QoS Data Collection category)

QDC_SIGNALLING_DATA_ERROR

`EventText: Signaling data could not be completely retrieved for the QDC report`

Type: **Information**

Signaling data could not be completely retrieved for the QDC report.

QDC_MSG_QUEUE_ERROR

`EventText: QDC message queue is full.`

Type: **Major**

QDC message storage is full. Messages may be lost.

QDC_SYSTEM_ERROR

`EventText: QDC software failure`

Type: **Major**

QDC is not running correctly.

QDC_ ERROR_IN_COMMON_CLIENT

`EventText: Error in QDC Common Client: %s`

Type: **Warning**

General error message; Reason described in specific text represented instead of %s.

9.2.52 QDC-CGWA-Related Events

(Events in the QoS Data Collection category)

QDC_INVALID_CONFIGURATION

`EventText: Invalid QDC configuration`

Type: **Warning**

The administrator is attempting to use an invalid QDC configuration.

QDC_PERSYSTENCY_ERROR

`EventText: QDC default configuration could not be read from the persistency`

Type: **Warning**

The default QDC configuration could not be read from the persistency.

QDC_ERROR_IN_CLIENT

`EventText: Error in QDC Client: %s`

Type: **Warning**

General error message; Cause of error in plain text instead of %s.

9.2.53 QDC VoIPSD Error Report Events

QDC_VOIPSD_ERROR

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

Type: **Information**

One of the components reports an error with "secure" data transmission: %s

9.2.54 SIP Events

SIP_INFORMATION

`EventText: ...`

Type: **Major, Minor, Warning, Information**

Just informationSHT: startup/shutdown.

SIP_INVALID_PARAMETER_VALUE

`EventText: ...`

Type: **Major, Minor, Warning**

There is a parameter that exceeds the specified value range.

SIP_UNEXPECTED_RETURN_VALUE

`EventText: ...`

Type: **Major, Minor, Warning**

The current function returns an unexpected result.

SIP_INVALID_POINTER

`EventText: ...`

Type: **Major, Minor, Warning, Information**

This pointer has got an invalid value.

10 Appendix: WAN/LAN Management

The administration of linked networks in WAN/LAN is a highly technical procedure. When performing this task, configuration problems will always crop up which need to be corrected quickly and efficiently. The information provided in the following sections is intended to help you in such cases.

10.1 Utility Programs for TCP/IP Diagnostics

Any operating system provides tools designed for finding faults in a TCP/IP environment which do not have an obvious explanation. As each operating system includes its own tools and corresponding command parameters, only the main Microsoft operating system functions are described here. Other tools for UNIX-based operating systems are described in detail in RFC 1147. Special parameters are contained in the Help for the corresponding operating system and can normally be queried by entering `<Command> -?`.

10.1.1 ping

The tool most often used is probably the `ping` command. This command allows you to check whether a computer in the network can be reached, that is whether communication with that computer is possible. An ICMP ECHO message is sent to the computer and then returned to the sender. If the answer reaches the sending computer, communication with the specified computer is possible. Most variants of the PING command produce connection statistics.

Syntax for Windows operating systems:

:

`ping <Host> [<Parameter>]`	
The following entries are possible for `<Parameter>`:	
`<Host>`	Contains the destination address or the host name of the destination computer
`-t`	Uninterrupted transfer of test packets to the computer. Normally only 4 test packets are transferred.
`-a`	IP addresses are resolved to host names.
`-n <number>`	Sends <Number> test packets to the computer.
`-l <size>`	Sends test packets with <Size> bytes
`-I <TTL>`	Number of router hops allowed for one packet. The counter is set to a starting value by the sender and decremented by each router that forwards the packet.

-w <Timeout>	Timeout in milliseconds to wait for each reply. If this time elapses, a timeout message appears. This value is set by default to 1000 (1s). It is advisable to set this value to 5000 (5s) or 10000 (10s) in the case of slow connections such as via modem or GSM. If the reply takes more than 1 second, a timeout message will be received even though a connection is possible.

Example:

Check connection to local computer. The local computer can normally be reached under the loopback address `127.0.0.1` and the name `localhost`.

```
C:\>ping localhost

PING is executed for the local host [127.0.0.1] with 32
bytes of data:

Reply from 127.0.0.1: bytes=32 time<10msec TTL=128

Reply from 127.0.0.1: bytes=32 time<10msec TTL=128

Reply from 127.0.0.1: bytes=32 time<10msec TTL=128

Reply from 127.0.0.1: bytes=32 time<10msec TTL=128
```

Messages:

If the remote computer does not reply, the error can be deduced from the messages.

- Invalid IP address (unknown host): The host name could not be converted to a valid IP address. This message is generated when the DNS server cannot be reached or is out of service. This message is only output when the host is addressed using a name.
- Destination host not available (network unreachable): There are no valid routes to the destination system. The destination address could not be reached, as a gateway is out of service or was not correctly specified on the local host.
- (Timeout): The computer has a route to the destination computer but there is no reply. The message reaches the destination host, but cannot be returned. This error is caused by incorrect routing of the destination computer.

10.1.2 ipconfig

The `ipconfig` program is a quick way of querying the TCP/IP network configuration. In this way you can display IP addresses, netmasks, gateways and network card statistics. It also enables IP addresses assigned via DHCP to be released or renewed.

Syntax for Windows operating systems:

`ipconfig [<Parameter>]`
The following entries are possible for `<Parameter>`:

`/all`	Shows details of the network configuration. This includes the host name, DNS servers used, MAC addresses of each network adapter and DHCP information.
`/release [Adapter]`	Releases the IP address assigned via DHCP at the adapter.
`/renew [Adapter]`	Assigns a new IP address to the adapter via DHCP.

If no adapter is specified under the parameters `release` and `renew`, all IP addresses at all adapters assigned via DHCP will be released or re-assigned.

Example:

Detailed query of current configuration:

```
C:\>ipconfig /all

Windows NT IP Configuration

        Host Name ..............: myhost.unify.de
        DNS Server..............: 192.168.50.23
                                  192.168.50.160
        Node Type ..............: Broadcast
        NetBIOS Scope ID .....:
        IP Routing Enabled.....: No
        WINS Proxy Enabled.....: No
        NetBIOS Resolution Uses
        DNS:                      Yes

Ethernet adapter El90x2:

        Description.............: 3Com 3C90x Ethernet
                                  adapter
        Physical Address.........: 00-10-5A-DD-56-55
        DHCP Enabled.............: No
        IP Address..............: 192.168.129.1
        Netmask..................: 255.255.255.0
        Default Gateway.........:

Ethernet adapter El90x1:
```

	Description.....:	3Com 3C90x Ethernet adapter
	Physical Address.....:	00-10-5A-37-26-B1
	DHCP Enabled.....:	Yes
	IP Address.....:	192.168.14.6
	Netmask.....:	255.255.255.0
	Default Gateway.....:	192.168.14.1
	DHCP Server.....:	192.168.11.103
	Lease Supplied..... ...:	Tue, 17.08.1999 08:43:30
	Lease Expires.....:	Tue, 19.01.2038 04:14:07

10.1.3 nslookup

An IP address can be assigned via a host name. This assignment of name and IP address is stored in the DNS server (DNS = Domain Name Server). The command `nslookup` can be used to query data that was saved for a specific host in the DNS server. By entering the command `nslookup` in the MS-DOS prompt, the program tries to contact the DNS server provided in the network. If a name is queried, the corresponding IP address is returned. Conversely, if an IP address is queried, the host name is returned. If neither the IP address nor the host name is stored in the DNS server, a corresponding error message is output.

The `nslookup` command message `Invalid IP address` indicates that the host name specified cannot be converted into an IP address. This occurs when the DNS server is out of service or the entry does not exist. This requires that the DNS servers are entered in the network configuration and can be addressed via network.

`nslookup` can be used to query various entries (records) on the DNS server. Once the program has been started, the following entries can be used to query the corresponding data.

`set Type=<Type>`	
The following entries are possible for `<Type>`:	
`a`	Address entries
`any`	All entries
`mx`	Mail Exchanger entries
`ns`	Name Server entries
`soa`	Start of Authority entries
`hinfo`	Host Info entries

axfr	All entries in a single area
txt	Text entries

Syntax for Windows operating systems:

nslookup <Host>

<Host>	Contains the destination address or the host name of the destination computer

Example:

```
C:\>nslookup localhost
Server: ns.domain.com
Address: 192.168.0.1
Name: localhost
Address: 127.0.0.1
```

The host "localhost" has the IP address 127.0.0.1.

10.1.4 hostname

The command hostname returns the name of the local computer. Unlike other operating systems, in Microsoft operating systems the host name cannot be changed using this command.

Example:

```
C:\>hostname
localhost
```

10.1.5 netstat

The command netstat is used to check existing connections and configured routes, and returns detailed statistics and information on individual network interfaces. Besides the routing table, the most frequently used netstat function is the query feature, which ascertains which connections exist at the local computer as well as the status of these connections.

Syntax for Windows operating systems:

netstat [<Parameter>] [<Interval>]

The following entries are possible for <Parameter>:	
-a	Displays all connections. This means that listening applications such as a Telnet server are also displayed.
-e	Displays Ethernet statistics
-n	Displays IP addresses instead of host names

`-p <Proto>`	Displays connections established via the `<Proto>` protocol
`-r`	Displays the routing table, which can also be displayed using `route print`.
`-s`	Displays statistics for each protocol
`<Interval>`	Repeats the display after <Interval> seconds

Example:

Queries all connections in IP address format (abbreviated)

```
C:\>netstat -a -n
```

Active Connections

Proto	Local address	Remote address	State
....			
....			
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	*:*	
....			

IP connections and their statuses can be displayed using this table. Before explaining this example in more detail, we will briefly discuss the variables.

`<Proto>`	Indicates the protocol used for the communication. In this case, Windows only distinguishes between TCP and UDP. Unfortunately, certain servers which only operate via a single protocol are displayed both as TCP and as UDP servers. This prevents accurate determination of the actual protocol in use.

<Local address>	This indicates the local address which has established a connection or is listening for a connection. The local address and the remote address are displayed in the format <IP address>:<Port number>.
<Remote address>	This indicates the remote address which has established a connection or to which a connection has been established.
<State>	
Shows the current state of the connections:	
ESTABLISHED	The local computer has set up a connection to a server. In this case the local computer is a client.
LISTENING	The local computer is ready to accept a connection. In this case the local computer is a server.
SYN_SENT	The local computer signals to the server that it would like to establish a connection.
SYN_RECEIVED	The local computer where the server is running has received a "SYN_SENT" signal, that is the client would like a connection to be established.
FIN_WAIT_1	The local computer would like to clear down the connection to the server.
TIME_WAIT	The local computer is waiting for server confirmation that the connection is to be terminated.
CLOSE_WAIT	The local computer where the server is running has received a "FIN_WAIT_1" signal, that is the client would like a connection to be cleared down.
FIN_WAIT_2	The local computer has received confirmation from the server to clear down the connection.
LAST_ACK	The server has sent confirmation that the connection is to be cleared down.
CLOSED	The server has received client confirmation that the connection has been cleared down.

A computer can be both a client and a server at the same time. This is the case, for example, where the local computer is connected to its own server. This is possible using the loopback interface 127.0.0.1. If, for example, a Telnet server is running on the local computer, a Telnet session can be opened on the local computer using the command `telnet localhost`.

In order to determine which data can be collated using the above example, we will now explain the procedure step by step.

Proto	Local address	Remote address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

Proto	Local address	Remote address	State
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING

The first two entries are in the "LISTENING" state, that is two programs (servers) have been started on the local computer, both of which are waiting for a client to establish a connection with them. Both are connected to the IP address "0.0.0.0". This IP address indicates that the server is connected to all available network interfaces. Even if only one network card is installed, this already has two interfaces, that is the local network card (192.168.129.3) and the loopback interface "127.0.0.1" which is installed as standard by Windows. In this example, a HTTP server (Port 80) and an SMTP server (Port 25) are running on the local computer. In order to determine whether the network card is working correctly, send a test ping from the local computer, e.g. `ping 192.168.129.3`. Any error message triggered by this test indicates an incorrectly configured network interface. If you wish to test the connection to the local HTTP server for example , simply use your Web browser and enter the URL `https://127.0.0.1` or `https://192.168.129.3`. Entering "telnet localhost 25" or "telnet 192.168.129.3 25" allows a connection to be established to the local SMTP server. In this case, the port (that is the application) is specified using 25.

The next three entries are all active connections. These can be established either from the local to the remote computer, or from the remote to the local computer.

Proto	Local address	Remote address	State
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

In order to distinguish between an incoming and an outgoing connection, the entries contained in the "LISTENING" state (server) are required. To do this, you need to check whether the port specified for the local computer is running on the local computer itself. The first line shows port "1037". This port is not running as a server (LISTENING) on the local computer (192.168.129.3). Thus this must be a connection from the local computer to a remote computer (192.168.129.1) with the port "110" (POP3). In other words, the local computer is in the process of downloading its e-mails from the POP3 server.

The second entry must also be an outgoing connection, as it is also not in the "LISTENING" state on the local computer. The local computer has therefore set up a connection to the computer "192.168.129.2" and port "23" (Telnet). This means that the local computer has opened a Telnet session on the remote PC.

In the third entry, the local port "80" (HTTP) corresponds to that of a server. Thus the remote computer 192.168.129.1 is in the process of opening Web pages on the local computer.

10.1.6 nbtstat

This utility program allows connections which use the "NetBIOS over TCP/IP protocol" (WINS-Client(TCP/IP)) to be tested. In the "NetBIOS over TCP/

IP protocol", the NetBIOS packet is packaged in a TCP/IP packet and then unpacked again on the remote side. This is necessary because NetBIOS cannot be routed like TCP/IP. As Windows drives can only be enabled via NetBIOS, such enablements must be packaged in TCP/IP in order to be transferred to other physical networks. For this purpose, Windows creates a NetBIOS name cache which can also be created manually. IP addresses are resolved in a table as computer names. This file is called `lmhosts` and is located in either the system directory or a system subdirectory, depending on the operating system

Win95/98/ME:	*%systemroot%*
WinNT/2000/XP:	*%systemroot%\system32\drivers\etc*

In these directories, Windows provides various test files which can be used as samples. The structure of each test file is explained. These files have the extension *sam*. In this case, the file is called *lmhosts.sam*. If this *lmhosts* file does not already exist, it can simply be copied to *lmhosts* and edited.

Syntax for Windows operating systems:

`nbtstat [<Parameter>]`	
The following entries are possible for `<Parameter>`:	
`-a <Host Name>`	Returns the name table for the computer specified under <Host Name>
`-A<IP address>`	Returns the name table for the computer specified under <IP Address>
`-c`	The NetBIOS Name Cache is listed with NetBIOS names and corresponding IP addresses
`-n`	Lists all local NetBIOS names used
`-R`	Deletes the NetBIOS Name Cache and reloads the file `LMHOST`.
`-r`	Lists the names which have been resolved for the Windows networks
`-S`	Shows client and server connections as IP addresses.
`-s`	Shows client and server connections and resolves the IP addresses into names.

10.1.7 pathping

This command (available in Windows 2000 and later) traces routes and offers additional information as well as `ping` and `tracert` command features. The `pathping` command sends data packets to each router on the way to a destination over a specific time frame. Specific statistics are then calculated using the data packets returned by each segment. The `pathping` command displays

packet loss information for every router and every connection so you can see which router or connection is causing network problems.

Win 2000:	*%systemroot%\system32*

Syntax for Windows operating systems:

`pathping [<Parameter>] destination name`	
The following entries are possible for `<Parameter>`:	
`-n`	Prevents addresses from being resolved to form host names.
`-h <section>`	Specifies the maximum number of segments to be transited when searching for a destination. The default value is 30.
`-c <host list>`	Separates concatenated computers through the implementation of intermediate gateways (loose source route) based on the host list.
`-p <interval>`	Specifies (in milliseconds) the interval between sequential ping commands. The default value is 250 milliseconds (1/4 seconds).
`-q <number>`	Specifies the number of requests for each PC on the path. The default value is 100.
`-w <timeout>`	Specifies how long (in milliseconds) the system must wait for individual answers. The default value is 3000 milliseconds (3 seconds).
`-T`	Adds a layer-2 priority ID to the ping packets (for example, for 802.1) and sends this ID to all network devices on the route. This is a quick and easy way to establish which network devices are not correctly configured for the layer-2 priority. This parameter must be entered in capital letters.
`-R`	Checks whether the individual network devices on the route support the Resource Reservation Setup Protocol (RSVP). This protocol allows the host computer to reserve a certain bandwidth for a data flow. This parameter must be entered in capital letters.
`Destination name`	Specifies the destination computer (terminal) which is identified either by an IP address or a host name.

10.1.8 route

In order to interconnect several TCP/IP networks, you will need to configure routing. Without routing, it is impossible to leave the local network. Note when routing that the gateway which connects the local network to other networks must be located in the same TCP/IP network as the local computer.

Syntax for Windows operating systems:

route <command> <target> <subnet mask> <gateway> [metric <hops>] [<parameter>]

The following entries are possible for <command>:	
print	Displays the current routing table
add	Adds a new route
delete	Deletes an existing route
change	Modifies an existing route
<Destination>	Indicates the destination host or destination network reachable via the <Gateway>.
<Subnet>	Specifies the subnet mask.
<Gateway>	Indicates the IP address of the gateway via which the IP address specified under <Destination> can be reached.
<Hops>	Indicates the number of gateways located between the sender and the destination. This parameter is only relevant when several routes exist for one destination. Certain routes can be assigned priority using this parameter. However, since there is usually only one gateway, the value "1" can be set here.
The following entries are possible for <Parameter>:	
-f	Deletes all routing entries in the routing table
-p	Creates a permanent entry. This parameter can only be specified using the command add. Normally routes are only set statically with the route command. This means that routes set in this way will be deleted by a system reboot. The parameter -p sets the entry permanently, so that it will not be deleted by a system reboot.

Example 1:

Adding a permanent default route

```
C:\cmd>route add 0.0.0.0 mask 0.0.0.0 192.168.0.199 -p
```

Example 2:

Querying a routing table

```
C:\>route print

Active Routes:
```

Network Address	Netmask	Gateway Address	Interface	Number
0.0.0.0	0.0.0.0	192.168.128.1	192.168.128.1	14
10.2.0.0	255.255.0.0	192.168.128.1	192.168.128.1	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	1
224.0.0.0	224.0.0.0	192.168.128.14	192.168.128.14	1
255.255.255.255	255.255.255.255	192.168.128.14	192.168.128.14	1

The last two entries are multicast or broadcast entries which will not be described in detail here.

10.1.9 tracert

The command `tracert` (trace route) is used to trace the route from the local computer to the destination host. It indicates all gateways located on the route to the destination host.

Syntax for Windows operating systems:

`tracert <Host> [<Parameter>]`	
`<Host>`	Contains the destination address or the host name of the destination computer
The following entries are possible for `<Parameter>`:	
`-d`	IP addresses are not resolved to host names
`-h <number>`	Indicates the maximum number of gateways to the destination host
`-j <list>`	Suggests a gateway route
`-w <timeout>`	Wait <Timeout> milliseconds for each reply

Example:

```
C:\cmd>tracert localhost

Tracing route to localhost [127.0.0.1] over a maximum of 30
hops:

1 <10 msec <10 msec <10 msec localhost [127.0.0.1]

Trace complete.
```

10.1.10 arp

Before a packet can be sent from one host to another, the hardware address (MAC address) of the destination host's network card must be determined. For this purpose, each computer which communicates via the TCP/IP protocol has an ARP table. "ARP" (Address Resolution Protocol) is used for resolving the IP address to the hardware address (MAC address). Before a connection is

established, the ARP table is searched for the required destination host. If the host is not contained in the table, an ARP request with the IP address of the destination host is sent via the network. When the destination host receives this request, it sends its hardware address to the requesting computer. This in turn enters the hardware address in its local ARP table. The next time this connection is set up, the hardware address of the destination host is known and can be applied as usual. If a hardware address located outside the logical TCP/IP network is requested, the only hardware address necessary is that of the router via which the destination host can be reached.

Syntax for Windows operating systems:

arp <Parameter>

The following entries are possible for `<Parameter>`:	
a	Displays the ARP table
`-d`	Deletes an entry from the ARP table
`-s`	Adds a host entry to the ARP table

Example 1:

Entering a new MAC address into the ARP table

```
C:\>arp -s 192.168.0.199 02-60-8c-f1-3e-6b
```

Example 2:

Querying the ARP table

```
C:\>arp -a

Interface: 192.168.0.1 on Interface 1
```

Internet Address	Physical Address	Type
192.168.0.1	00-00-5a-42-66-60	dynamic
192.168.0.10	00-60-70-cd-59-22	dynamic
192.168.0.199	02-60-8c-f1-3e-6b	static

10.1.11 Telnet

Telnet enables the user to log onto a remote computer. By default, the program uses port 23 for this. If you wish to log onto a computer with another port, you must additionally specify the port number.

Syntax for Windows operating systems:

telnet [<Host> [<Port>]]

<Host>	Contains the destination address or the host name of the destination computer

<Port>	Port number which identifies the application on the destination computer

Example:

```
C:\>telnet localhost 110
```

10.2 IP Addressing: Subnets

To circumvent the scarcity of official IP addresses and to divide an IP network into separate sub-networks, the "sub-netting" procedure can be used.

For the allocation of official IP addresses, for example, sub-netting makes it possible to generate additional independent IP networks by using existing Class A, B and C network addresses.

Various classes and standard network masks have been agreed upon for networks:

Table 3: Network Classes and Standard Network Masks

Class	Subnet mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Division into independent subnets also offers the considerable advantage that local network traffic remains in its own subnet. Access to third-party networks is only possible via a router.

The basic functionality of sub-netting is relatively simple and is based on the "netmask". This mask is used for defining bits which represent either the network or the host segment within an IP address. Set bits (1) represent the network segment, while deleted bits (0) represent the host segment.

The best way to analyze a netmask is in binary format. The Class C standard netmask "255.255.255.0" is a good example.

Table 4: Example of a Class C Standard Network Mask

	Network			Host
Bytes	1st byte	2nd byte	3rd byte	4th byte
Netmask	255	255	255	0
Binary format	1111 1111	1111 1111	1111 1111	0000 0000

In netmask "255.255.255.0", the first 3 bytes represent the network segment (all bits 1) and the last byte represents the host segment (all bits 0).

The host (router, workstation, etc.) uses this netmask to determine whether the IP address being addressed is located in the local network. If the destination

host is not located in the same network, packets are forwarded to this address via suitably defined routing mechanisms.

To create customized subnets, you will first need to determine the number of sub-networks to be established within a class-based network (Class A, B, C). When a network is divided, 2n subnets are always created as a result. An example will illustrate this more clearly.

The Class C network "192.168.1.0" is to be divided into 4 subnets. A Class C network has the default netmask "255.255.255.0". Two bits are required for four different combinations in the binary system. The following table illustrates the interdependency between the bit number and the number of networks.

Table 5: Bit Number Depending on Number of Networks

Bits	Combinations	Bits	Combinations
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
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

So that no gaps are left in the address range, additional 1s are added from left to right to the existing 1s of the netmask.

Table 6: Example of a Subnet Mask Binary Format

Class C	Network			Host
Bytes	1st byte	2nd byte	3rd byte	4th byte
Netmask	255	255	255	0

Class C	Network			Host	
Binary format	1111 1111	1111 1111	1111 1111	0000 0000	
New	**Network**			**Host**	
Bytes	1st byte	2nd byte	3rd byte	4th byte	
Binary format	1111 1111	1111 1111	1111 1111	**11**	00 0000
Netmask	255	255	255	192	

If the new subnet is converted from binary to decimal form, the result is the subnet mask "255.255.255.192". Now 26 bits are available for the network segment and 6 for the host segment. Computers with a network segment with the same bit pattern can communicate directly in a physical network. Other networks can only be reached via a gateway. If the modified 4th byte is viewed in terms of the two new network bits (25 and 26), the newly created subnets can now be calculated.

Table 7: Calculating New Subnets

4th byte	Decimal	New networks	Broadcast address	Host addresses
0000 0000	0	192.168.1.0	192.168.1.63	1 - 62
0100 0000	64	192.168.1.64	192.168.1.127	65 - 126
1000 0000	128	192.168.1.128	192.168.1.191	129 - 190
1100 0000	192	192.168.1.192	192.168.1.255	193 - 254

Thus sub-netting essentially involves the extension of the network segment of an IP address by reducing the host segment. The number of available subnets and hosts depends on the following conditions:

The number of available host addresses depends largely on the length of the host segment of the IP address. Viewed mathematically, a 6-bit host segment provides for 64 addresses. However, as each IP network and thus each individual subnet has two reserved addresses, the maximum number of addresses is reduced by two. These are the host addresses which contain either zeros or ones. The former is used for addressing a network, while the latter is used for broadcasts in the network in question.

As mentioned above, the new network segment bits are added from left to right to the existing bits. The reasons for this are described below. For example, if you use subnet mask "255.255.255.3" for the network "192.168.1.0", the host segment is located in the middle of the network segment.

Table 8: Host Segment in a Network Segment

	Network			Host	Network
Bytes	1st byte	2nd byte	3rd byte	4th byte	

	Network			Host	Network
Netmask	255	255	255	3	
Binary format	1111 1111	1111 1111	1111 1111	0000 00	**11**

No associated IP address areas are provided for by this subnet as only the hosts which have set the last two bits are located in a network. The resulting addresses are listed in the following table.

Table 9: Network Addresses Depending on Last Two Bit Digits

4th byte	Decima	New networks	Broadcast address	Host addresses
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

The host addresses indicate that the individual hosts are not located in associated areas. This type of sub-netting makes it difficult to maintain an overview for administration. This is why this type of sub-netting should not be used.

Up to now we have described how sub-networks are created. We will now explain how the IP addresses of computers are assigned to the respective subnets.

The following table shows four IP addresses for a network (Class C) and their connection to the netmask being used 255.255.255.224.

Table 10: Allocating IP Addresses to Class C Networks

	Network	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

The binary illustration of masks and addresses shows quite clearly which subnet the IP addresses in question belong to. Addresses 1 and 4 are in subnet ".32" (00100000), address 2 belongs to subnet ".96" (01100000) and address 3 is located in subnet ".128" (10000000).

If the example is based on the standard mask "255.255.255.0" of a Class C network, the length of the network segment is 24 bits, while the host segment is 8 bits long. Based on netmask "255.255.255.224" the network segment of an IP

address in the network is exactly 27 bits long. Accordingly the host segment is just 5 bits long.

The following overview provides the most commonly-used Class C masks as a reference, together with the corresponding network and host allocations.

Table 11: Overview of the Most Commonly-Used Class C Masks

Subnet mask	Number of networks	Hosts per subnet	Subne	Broadcast Address	Hosts
255.255.255.0	1	253	0	255	1 - 254
255.255.255.128	2	126	0	127	1 - 126
			128	255	129 - 254
255.255.255.192	4	62	0	63	1 - 62
			64	127	65 - 126
			128	191	129 - 190
			192	255	193 - 254
255.255.255.224	8	30	0	31	1 - 30
			32	63	33 - 62
			64	95	65 - 94
			96	127	97 - 126
			128	159	129 - 158
			160	191	161 - 190
			192	223	193 - 222
			224	255	225 - 254
255.255.255.240	16	16	0	15	1 - 14
			16	31	17 - 30
			32	47	33 - 46
			48	63	47 - 62
			64	79	65 - 78
			80	95	81 - 94
			96	111	97 - 110
			112	127	113 - 126
			128	143	129 - 142
			144	159	145 - 158

Subnet mask	Number of networks	Hosts per subnet	Subne	Broadcast Address	Hosts
			160	175	161 - 174
			176	191	177 - 190
			192	207	193 - 206
			208	223	209 - 222
			224	239	225 - 238
			240	255	241 - 254

Example:

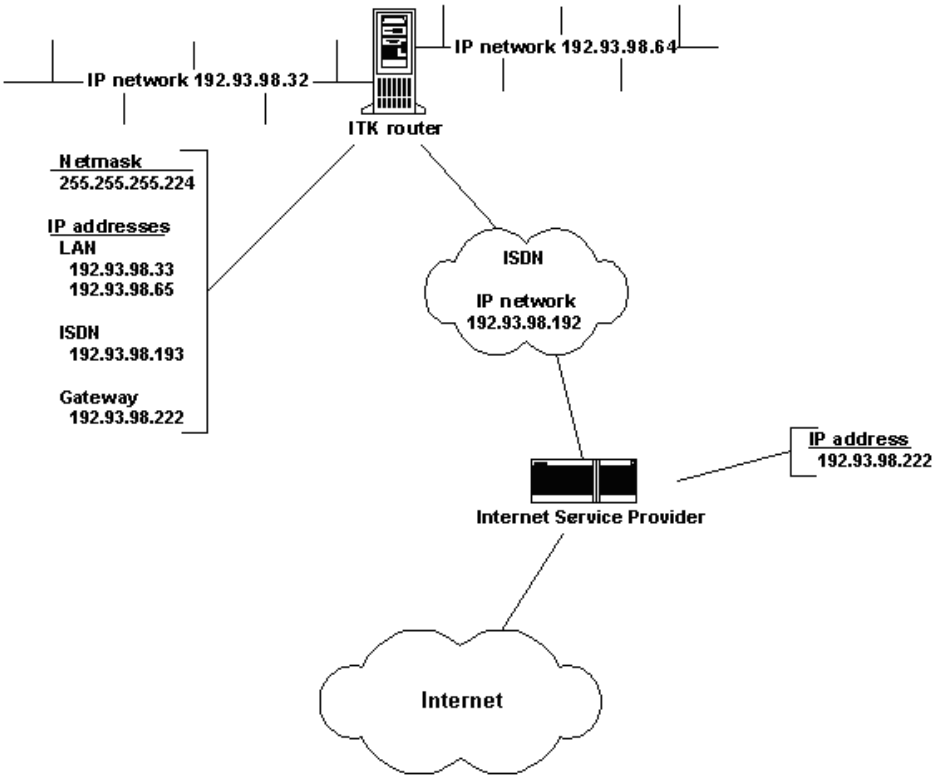
A LAN with two Ethernet networks is to be connected to the Internet via ISDN access. All stations in the local Ethernet are to have Internet access and also be directly accessible from the Internet. Based on the corresponding structures of a Class C address, a complete Class C network would normally have to be provided for each of the two Ethernet networks and for the ISDN network. However, as the maximum number of stations in a Thin Ethernet segment is limited to thirty, 223 host addresses per network would be lost here alone.

This is where sub-netting is of particular significance: With a corresponding netmask, just one Class C network is required to achieve a complete LAN connection, without the loss of host addresses.

For this purpose, an Internet Service Provider provides a Class C network with the following basic data:

Provider IP address:	192.93.98.222
Gateway IP address:	192.93.98.222
Networks IP address:	192.93.98.0
Netmask:	255.255.255.0

The following diagram shows the corresponding configuration:



Connection of BNC Network at Twisted Pair to HG 3500/3575

"255.255.255.224" is available as a netmask, as this mask provides 8 subnets with 30 hosts each. The number of hosts in each subnet is thus equivalent to the maximum number of stations in an Ethernet segment.

This illustration shows that two subnets, in this case "192.93.98.32" and "192.93.98.64", have been assigned to the two LAN boards of the ITK router. One of the LAN boards is assigned the IP address "192.93.98.33" and the other is assigned "192.93.98.65". In this way each board can supply 29 additional stations with IP addresses.

10.3 Port Numbers

10.3.1 Port Numbers on the OpenScape 4000 V10

Table 12: Port numbers on OpenScape 4000 V10

Client/Server	Protocol	Server	Client	Application
H.323 (H.225/ Q931)	TCP	1720	ephemeral	Voice over IP for system clients, H.323 clients, AllServe and IP networking
RTP/RTCP	UDP	1500	ephemeral	

Client/Server	Protocol	Server	Client	Application
H.245	TCP	ephemeral	ephemeral	
Accounting Server	TCP	13042		
SNMP (Get/Set)	UDP	161		SNMP browser, OpenScape FM
RTCP/MSC	UDP	162		

10.4 PC Sound Settings for Voice over IP

A number of special PC sound card configurations must be observed when using Voice over IP to make calls via networks and PCs. Faults such as poor sound quality and one-sided or non-existent connections can often be corrected by modifying your settings. The following chapter suggests solutions which should help when configuring a voice client. This help is kept rather general, since the exact settings depend on the hardware and software and on the environment where the PC is located. A detailed description would be too extensive and therefore unclear.

Poor sound quality is not always an indication of a configuration error or of hardware/software faults. For example, crackling noises, which signify brief interruptions (lost voice packets), could also be an indication that the LAN load is too high. It may be possible to improve the quality of the Voice over IP connection by restructuring the LAN, migrating to 100BaseT or using a switch. If the G.711 audio standard is used (64 kbps) rather than G.723 (5 kbps), a considerably higher LAN load may result. For a small number of voice applications, G.711 has no noticeable effect on the LAN load. However, if Voice over IP is used intensively when the LAN is already overloaded, the voice quality may deteriorate significantly.

Configuration options

1) Simultaneous talking and listening is not possible

- The sound card driver is not fully duplex-compatible, an update must be installed to correct this.
- Incorrect configuration of the voice application, activate full duplex functionality in the software.

2) Full duplex functionality of the sound card driver can be tested with Netmeeting. Under **Options** #→ **Audio** you can activate/deactivate full duplex functionality. If this item cannot be modified, a fully-duplex driver must be installed for the sound card.

3) One-sided voice connections

- Full duplex functionality activated
- Microphone connected
- Microphone activated for voice application
- Check PC volume setting, activate **Microphone** under Record

4) You hear your own voice, either immediately or after a delay.

- Check PC volume setting, deactivate **Microphone** under Playback and deactivate **Wave** under Record

5) Call partner has difficulty hearing you

- Check volume setting of PC or voice application, increase volume
- If available, activate Microphone Booster under **Volume** > **Playback** > **Advanced Settings**

6) The called party hears loud background noise (over-modulation).

- If available, deactivate microphone booster under **Volume** > **Playback**> **Advanced Settings**
- Adjust microphone sensitivity in the voice application, for example in Netmeeting under **Options** > **Audio Microphone**, activate "Set manually" and adjust sensitivity
- Adjust recording volume, for example in Netmeeting go to **Options**> **Audio** and activate the Audio Wizard
- Change the audio standard, for example in Netmeeting go to **Options** > **Audio** > **Extended, and switch from G.723 Audio Codec** to **G.711 Audio Codec** (increases the LAN load)

11 Appendix: Internet References

The following Internet sources provide original or detailed information on technical standards used in HG 3500/3575.

11.1 RFCs

RFCs (Requests for Comments) are official Internet descriptions of relevant network standards.

http://tools.ietf.org/html/rfc793

1) RFC for the TCP protocol

http://tools.ietf.org/html/rfc791

RFC for the IP protocol

http://tools.ietf.org/html/rfc768

RFC for the UDP protocol

http://tools.ietf.org/html/rfc2616

RFC for the HTTP protocol

http://tools.ietf.org/html/rfc2821

RFC for the SMTP protocol

http://tools.ietf.org/html/rfc1157

RFC for the SNMP protocol

http://tools.ietf.org/html/rfc959

Standard for the FTP protocol

http://tools.ietf.org/html/rfc3550

RFC for the RTP protocol (Real-Time Application Protocol)

http://tools.ietf.org/html/rfc1994

PPP Challenge Handshake Authentication Protocol (CHAP)

http://tools.ietf.org/html/rfc2030

RFC for the SNTP protocol

http://tools.ietf.org/html/rfc1340

RFC for "Assigned Numbers" (protocol and port numbers)

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

Telephone number mapping (ENUM) service registration for H.323

http://tools.ietf.org/html/rfc3508

H.323 Uniform Resource Locator (URL) Scheme Registration

http://tools.ietf.org/html/rfc3709

Internet X.509 Public Key Infrastructure

http://tools.ietf.org/html/rfc3647

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

http://tools.ietf.org/html/rfc3279

Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

http://tools.ietf.org/html/rfc3280

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

http://tools.ietf.org/html/rfc3394

Advanced Encryption Standard (AES) Key Wrap Algorithm

http://tools.ietf.org/html/rfc3670

Information Model for Describing Network Device QoS Datapath Mechanisms

http://tools.ietf.org/html/rfc3644

Policy Quality of Service (QoS) Information Model

http://tools.ietf.org/html/rfc3555

MIME Type Registration of RTP Payload Formats

http://tools.ietf.org/html/rfc3387

Considerations from the Service Management Research Group (SMRG) on Quality of Service (QoS) in the IP Network

11.2 Other Sources

http://www.protocols.com/pbook/VoIP.htm

1) Voice Over IP Reference Page

http://en.wikipedia.org/wiki/Voice_over_IP

Wikipedia article on "Voice over IP".

12 Glossary

Numbers

3DES

Triple DES. Improved version of the symmetrical DES encryption procedure in which the DES algorithm is applied three times to achieve a higher level of security.

A

AES

The Advanced Encryption Standard is the successor of the DES or 3DES encryption standard.

AF

Assured Forwarding. Procedure for controlling broadband for Quality of Service.

ARP

The Address Resolution Protocol is a protocol which maps level 3 IP addresses to level 2 hardware addresses (MAC addresses).

B

BBAE

Broadband connection unit. The BBAE is the physical port on the subscriber line for a connection line used for broadband. It splits the supplier network from the connection cable at the subscriber and processes the signals for transmission over the relevant connection segment. In the case of DSL connections, the BBAE usually also features a splitter that splits or combines the broadband and narrowband signals.

B-Channel

An ISDN user data channel ("bearer channel") with a capacity of 64 Kbps.

Bandwidth

The bandwidth of a communication channel is its capacity for transferring data.

Boot

This term refers to the startup procedure. The boot ROM contains the start code; "booting" is another word for "starting".

C

CA

Certification Authority. Trustworthy institution for issuing certificates.

CAPI

Common ISDN Application Interface. Important CAPI interface properties include support for multiple B channels for data and voice, use of the B channel protocol for connection control, selection of different services, support for multiple logical connections over a physical connection, support for multiple connections, use of multiple communication protocols and support for one or more basic accesses or primary rate accesses.

CHAP

Challenge Handshake Authentication Protocol. In the case of CHAP, authentication is controlled by the host. When a client dials in, he or she is prompted by the host to authenticate himself or herself. The username/ password combination used for authentication is transmitted by the client in encrypted form via MD5.

CLI

Command Line Interface. Generic term for command lines and shells, terminal emulations, etc.

CLIR

Calling Line Identification Restriction. ISDN feature.

Codec

Codecs convert analog audio or video data into digital format (encoding) and back into analog format (decoding).

CorNet-NQ

CorNet NQ (from "Corporate Networking") is a proprietary signaling protocol. CorNet-NQ is a superset of CorNet N which supports QSIG.

D

D channel

A D channel is an ISDN signaling channel which transmits call control information.

DES

Data Encryption Standard. Conventional encryption and decryption procedure with symmetrical algorithm; in other words, the same key is used for encryption and decryption. The block size is 64 bits, that is, a 64-bit block of plaintext is transformed into a 64-bit block of ciphertext. The key that controls this transformation is also 64-bit. However, only 56 of these 64 bits are available for the user; the remaining 8 bits (one bit from each byte) are required for the parity check.

DID

Abbreviation of "Direct Inward Dialing". DID is a method of forwarding incoming calls directly to H.323 terminals.

DLS

The DLS (Deployment Service) is a OpenScape management application for administering workpoints (optiPoint telephones and optiClient installations) in OpenScape and non-OpenScape networks.

DLI

DLI is the abbreviation for DLS interface.

DMA

Direct Memory Access. DMA technology allows peripheral devices, such as network cards or sound cards connected to PCs, to communicate directly with each other without a detour over the CPU. The advantage of DMA technology is increased data transmission speeds while at the same time unloading the processor.

DMC

Direct Media Connection. The DMC feature is used in OpenScape for VoIP (Voice over IP)

connections to support the "Payload Switching" feature.

The payload (voice channel) of a OpenScape-internal or network-wide voice connection is transferred via a LAN; here a direct IP connection with no previous TDM data stream conversion may be made.

When the "DMC any-to-any" feature is being used, the payload data in a OpenScape network is transferred directly between the IP endpoints without repeated IP TDM conversion. This direct payload connection is known as Direct Media Connection

DNS

Domain Name System. The DNS is a database distributed over a number of Internet hosts and responsible for correct routing based on the domain name. DNS assigns domain names to IP addresses.

DSA

Digital Signature Algorithm, an encryption algorithm. DSA works with a variable public key length of between 512 bits and (maximum) 1024 bits.

DSL

Digital Subscriber Line. DSL technology speeds up data transmitted over conventional telephone lines significantly and is designed chiefly for fast Internet access. DSL connections are primarily available with the technologies Asymmetric DSL (ADSL) and Single Pair DSL (SDSL). The more common variant, ADSL, transmits Internet data over the existing telephone network above the telephony frequencies between 138 and 1,104 kHz. ADSL is, for example, the basis for the T-DSL offering from Deutsche Telekom AG.

DSP

The HG 3500/3575 comes with DSP modules (DSP - Digital Signal Processor). A DSP provides for two VoIP channels.

DTMF

Abbreviation of "dual-tone multifrequency". DTMF is the multifrequency signaling mode for transmitting telephone numbers.

E

E-DSS1

Abbreviation of "European Digital Subscriber System No. 1". E-DSS1 is the ISDN transport protocol normally used in Europe.

EF

Expedited Forwarded. Procedure for controlling broadband for Quality of Service.

Terminal Device

A terminal device or endpoint is an H.323 component that can initiate or receive calls. Information flows begin or end here. Examples include clients, gateways or MCUs.

F

FTP

File Transfer Protocol. Platform-independent, TCP/IP-based network protocol for transmitting files between a client and a server (download and upload) and for simple file operations on the server.

G

G.711

G.711 is an ITU standard (International Telecommunication Union) standard for voice codecs for a data rate of 64 Kbps.

G.723.1

G.723.1 is an ITU standard (International Telecommunication Union) for voice codecs for transmission rates of 5.3 and 6.3 Kbps.

G.729

G.729 is a group of ITU standards (International Telecommunication Union) for voice codecs for transmission rates of 8 Kbps.

Gatekeeper

A gatekeeper is an H.323 component that provides address conversion and access control services for endpoints in an H.323 network.

Gateway

A gateway is a H.323 component which connects H.323 endpoints in an IP network to telephones in the public telephone network. It translates between H.323 and ISDN protocols.

GSM

Global System for Mobile Communications. Standard for digital mobile communications and the basis for the German D and E cellular network.

GW

Abbreviation of "gateway".

H

H.323

H.323 is a group of standards which describes the transmission of call and fax data in packet-oriented networks such as IP networks. These standards are set down in the H.323 series of ITU-T recommendations (International Telecommunication Union - Telecommunication Standardization Sector).

HFA

HiPath

HiPath (from "Highly Integrated Pathwork") is an innovative strategy which implements an extensive IP migration concept and thereby facilitates the integration of multimedia communication in existing corporate IP networks.

HTML

Hypertext Markup Language. Standard for displaying Web pages, developed by the World Wide Web (or W3) Consortium that is responsible for WWW standardization.

HTTP

Hypertext Transfer Protocol. Platform-independent, TCP/IP-based network protocol for data transmission in the World Wide Web.

HTTPS

Hypertext Transfer Protocol Secure. In contrast to HTTP, all data is transmitted in encrypted form.

I

IKE

Internet Key Exchange Protocol. Procedure for creating secure, authenticated connections. IKE supports various modes for exchanging keys. In the first phase, a secure, authenticated connection is established. In the second phase, the keys needed in the various protocols are exchanged and in general, individual keys (encryption, hashes) are derived from a master key.

ILS

Internet Locator Service. Directory service used primarily by Microsoft NetMeeting.

IP address

An IP address (IP - Internet Protocol) is a group of four numbers that identify a device. Each number can have a value between 0 and 255.

ISDN

Abbreviation of "Integrated Services Digital Network". ISDN is a fully digital public telephone network.

IVR

Abbreviation of "Interactive Voice Response". IVR is a procedure for forwarding calls if an individual line does not have numbers for dialing H.323 endpoints directly. HG 3500/3575 does not support IVR.

L

LAN

Abbreviation of "Local Area Network". A local area network (LAN) connects PCs within a company.

LCP

Link Control Protocol. The LCP is used to set up, configure, test, and clear down a PPP connection. Connection setup is split into a number of phases. First of all, the connection parameters are negotiated, including which type of authentication (PAP, CHAP) should be performed.

LCS

Abbreviation for "Live Communication Server". Live Communication Server is the new Instant Messaging solution for your business and an upgradable realtime communication platform from Microsoft.

M

MAL

Abbreviation for "Magic Adaptation Layer". Is the layer between application and platform.

MCU

Abbreviation of "Multipoint Controller Unit". MCUs are used for audio and video calls with multiple subscribers. They centralize data distribution and combine voice and video.

MD5

Message Digest algorithm that can create a 128-bit digital signature from a text of any length. The digital signature shows if the text was subsequently changed. MD5 is therefore used as an authentication procedure.

MIB

Abbreviation of "Management Information Base". An MIB compiles information and parameters of a network device. It is required for administration via SNMP.

DTMF

Dual-tone multifrequency signaling, also known as tone dialing. Procedure for transmitting station number and other data. Each key on a terminal is assigned two frequencies. When you press a key, a tone is generated from the two frequencies assigned to it. Dialing a station number at a subscriber generates a sequence of tones based on mixture frequencies.

MoH

Music on Hold. A melody or else an announcement text heard by the waiting subscriber when a connection is placed on hold or being forwarded within a telecommunication system.

MPPC

Microsoft Point-to-Point-Compression. Data compression procedure implemented for speeding up data transmissions.

MSC

Abbreviation for "Media Stream Control". The Media Stream Control (MSC) monitors and administers the media streams that are routed via HG 3500/3575. The MSC is used to transmit media data between LAN and ISDN.

Multicast

Multicast is the simultaneous transfer of data from a source to multiple recipients in networks.

N

NAT

Network Address Translation. Procedure for mapping private IP addresses to public IP addresses. NAT is necessary because public IP addresses are becoming scarcer. NAT is also used for data security because it conceals the internal LAN structure.

NTBA

Network terminator adapter. Is responsible for switching the Uk0 interface (national) to the S0 bus (international) for an ISDN basic access.

NTBBA

Network Termination Broadband Access. The NTBBA provides the network terminator for the broadband signal portion at the DSL subscriber line. In ADSL connections, this function is performed by the ADSL controller or the ADSL modem. The ADSL controller transforms the ADSL signal from the network interface into a mostly hardware-specific user interface suitable for the PC.

O

OAM

Operation, Administration, and Maintenance. OAM refers to all equipment that is used to operate, administer, and maintain networks.

OSPF

Open Shortest Path First. A routing protocol developed by the IETF. It is defined in RFC 1247 and based on the "Shortest Path First" algorithm developed by Edsger Dijkstra.

P

PAP

Password Authentication Protocol. Authentication procedure based on the point-to-point protocol, described in RFC 1334. In contrast to CHAP, the PAP protocol transmits the password for authentication in plaintext.

PBX

Abbreviation of "Private Branch Exchange". A PBX is a telecommunications system.

PCM

Physical Connection Management. Belongs to the functional blocks of Connection Management (CMT) in the FDDI ring.

PKI

Public Key Infrastructure Environment in which encryption and digital signature services based on the public key procedures are provided. In the case of this security structure, a certified party's public key is authenticated on the basis of the relevant identification features by a digital signature from the certification authority (CA). Using PKI provides a trustworthy network environment in which communication is protected against unauthorized access by encryption and the authenticity of the communication partner is guaranteed by the digital signature.

PPP

Point to Point Protocol. Protocol for connection setup over dial-up lines (mostly over modem or ISDN). It supports the transport of a wide variety of network protocols, including the Internet's IP protocol.

PPPoE

PPP over Ethernet. Use of the PPP network protocol over an Ethernet connection. PPPoE is currently used in Germany for ADSL connections.

PPTP

Point-to-Point Tunneling Protocol. Microsoft protocol for creating a Virtual Private Network (VPN); it supports PPP tunneling by an IP network.

PSTN

Abbreviation of "Public Switched Telephone Network". PSTN is the worldwide public telephone network.

PRI

Abbreviation of "Primary Rate Interface". A PRI is an ISDN interface comprising 23 (TS1) or 30 (TS2) B channels each with a capacity of 64 Kbps and one D channel with a capacity of 16 Kbps.

Q

Q.931

Q.931 is a call signaling protocol for setting up and clearing down calls.

QCU

Abbreviation for "QoS Monitoring Control Unit".

QDC

Abbreviation for "Quality of Service Data Collection".

The OpenScape IP service QDC is a tool that collects data on OpenScape products. This data is used to analyze the voice and network quality of the products.

QSIG

QSIG is a protocol for networking nodes which has been adapted by the ITU-T (International Telecommunication Union - Telecommunication Standardization Sector). QSIG can be used to network PBXs from different manufacturers.

QoS

Quality of Service. Prioritization of IP data packets on the basis of specific features and ISDN properties. This means that voice over IP (VoIP) transmissions that need a delay-free and continuous date stream, for example, can be given a higher priority than downloads from file servers or Web page callups.

R

RAS

Registration/Admission/State is a protocol that regulates signaling between client and gateway in the area of automatic detection and registration.

RIP

The Route Information Protocol automatically generates and maintains network routes between routers that support this protocol.

Router

A router is a network component which connects subnetworks and transfers packets between them.

RSA

The RSA cryptosystem is an asymmetrical cryptosystem, that is, it uses different keys for encryption and decryption. It is named after its founders, Ronald L. Rivest, Adi Shamir, and Leonard Adleman.

RTP

The Real-Time Transport Protocol governs the transmission of real-time audio and video packets from a terminal to one or more different terminals.

S

SCN

Abbreviation of "Switched Circuit Network". Switched circuit network that includes all digital telephone and cellular networks as well as analog telephone facilities connected over digital telephone switches.

SHA1

Security Hash Algorithm. This generates a unique 160-bit hash from a string. It is a one-way encryption procedure. In other words, the encrypted string can no longer be determined from the hash.

SIP

Abbreviation for "Session Initiation Protocol". The SIP is a network protocol for setting up communication sessions between two or more stations. The protocol is specified in the RFC 3261.

SMTP

Simple Mail Transfer Protocol. Network transmission protocol for sending e-mails.

SNMP

Simple Network Management Protocol. The protocol is used to administer and monitor network elements that mainly originate in the LAN area (for example, routers, servers, etc.). SNMP transfers and changes management information and alarms. In LANs, a special SNMP management server can gather and evaluate this management information so that the network administrator has an overview of the most important events in the LAN.

SNTP

Simple Network Time Protocol. Protocol for transporting an official time in networks and the Internet. The SNTP protocol is characterized by its simplicity and an inaccuracy of several hundred milliseconds. It is defined in RFC 1769. The extended variant is called NTP.

SRTP

Abbreviation for "Secure Real-time Transport Protocol".

SSL

Secure Socket Layer. Transmission protocol that supports encrypted communication. The advantage of the SSL protocol is that it supports the implementation of every higher protocol based on the SSL protocol. This guarantees application- and system-independence. SSL performs encryption using public keys that are confirmed by a third party in accordance with the X.509 standard. The high level of security is guaranteed by the fact that the decryption key must be individually redefined and is only saved at the user's facility.

STAC

Data compression procedure implemented for speeding up data transmissions. The PPP Stac LZS Compression protocol described in RFC 1974 is a competitor procedure for MPPC.

T

T.30

T.30 is an ITU standard for fax transmission. It specifies the functions within the first three layers for the implementation of the group 3 fax service.

T.38

T.38 is an ITU standard for fax transmission. It governs the communication of Group 3 fax devices via IP networks.

TCP

Transmission Control Protocol. TCP sets up a virtual channel between two computers (more precisely: endpoints between two applications on these computers). Data can be transmitted in both directions on this channel. In most cases, TCP is based on the IP protocol. It belongs to Layer 4 of the OSI network layer model.

TFTP

Trivial File Transfer Protocol described in RFC 783. This protocol does not support user authentication, directory switching or directory listings. It is only used for uploading and downloading files directly with get and put commands.

TLS

Abbreviation for "Transport Layer Security" or Secure Sockets Layer (SSL) is an encryption protocol for data transmissions on the Internet. TLS is the standardized further development of SSL 3.0.

U

UDP

User Datagram Protocol. The User Datagram Protocol (UDP) supports wireless data exchange between computers. The UDP was also developed to enable application processes to send datagrams and thereby to satisfy the requirements of transaction-oriented traffic. UDP is based directly on the IP protocol. UDP is a basic protocol mechanism that does not guarantee datagram delivery to a destination partner or provide mechanisms to protect against duplication or ordering errors. The functional scope of the UDP protocol is limited to the transport service, connection multiplexing and error correction.

URL

Uniform Resource Locator. Addressing form for Internet files that are used primarily in the World Wide Web (WWW). The URL format provides a unique designation for all documents on the Internet. It describes the address of a document or object that can be read by a WWW browser.

UTC

Universal Time Coordinated. This is a world time and as such replaces Greenwich Mean Time (GMT). UTC time is a reference time that is used as a global standard. The coordinated world time uses International Atomic Time (TAI) as the reference time. These are both identical apart from the leap seconds that may be added at the end of June and/or December. The reference point for Universal Time Coordinated (UTC) is the 0Â° degree of longitude.

V

VCAPI

Virtual CAPI. VCAPI lets you reach remote computers using ISDN-specific protocols (for example, Euro File Transfer).

VoIP

The Voice over Internet Protocol (VoIP) controls telephone calls via IP networks.

W

WAN

Wide Area Network. A WAN is a network that connects multiple LANs over long distances. For example, a WAN network can connect several branches of a company spread over different locations.

WBM

Web Based Management. This is an option for configuring PCs and telecommunication hardware and software over a Web browser. No specific software needs to installed locally. The software is implemented as a Web application and can be called up over HTTP or HTTPS.

X

XML

Extensible Markup Language. Standard developed by the W3 Consortium for the definition of markup languages. The best-known markup languages defined with XML are XHTML, SVG, and WML.

XSL

Extensible Stylesheet Language. Standard developed by the W3 Consortium for formatting and conversion (in the XSLT component) of XML-based markup languages into other formats.

Index

A

About WBM 17
Address Resolution Protocol 281
Admin Log Language (parameter) 112
Allow SIP Registration for Trunking (parameter) 35
Area Code (parameter) 54
arp 267
ARP 281
ASSERTION_FAILED_EVENT (event code) 181
Associated Trace Profile (parameter) 111, 112
Authentication Required 64, 64
Automatic Deactivation Time 106

B

B channels 281
Bandwidth 281
Basic User Input String for Outband Signaling (parameter) 57, 62
Board Name (parameter) 34
Buttons 19

C

Central Conference DAR (Digit Analysis Result) 64
CGE_GENERAL_ERROR (event code) 253
CGE_PSS_STORE_ERROR (event code) 253
Change sort sequence 20
Check boxes 19
Cipher 64
Circuit Number (circuit) 59, 64
ClearChannel (parameter) 58
Client Registered 64
Clients 63
Codecs 282
Confirm CLIR (parameter) 53
Contact Address (parameter) 34
CorNet NQ 282
Country Code (parameter) 54
Create heap dump 90

D

D channels 282
Destination address (parameter) 52, 53
Destination Codec Parameters 62
DID 282
Digital Signaling Processor 283
Direct Inward Dialing 282
Disable Processing of ANS/CED Tone 67
Disable Processing of CNG Tone 67
Disable Processing of CT Tone 67
Disable Processing of Early ANS/CED Tone 67
Dropdown lists 19
DSP 283
DSS1 283
DTMF 283

E

E-DSS1 283
EPID 64
Error Correction Used for T.38 Fax (UDP) (parameter) 58
ERROR_IN_COMMON_CLIENT (event code) 254
Events 98, 109
EXIT_REBOOT_EVENT (event code) 181

F

Factory default 97
Factory settings 97
Filter 89
Flash Call (FLASH) 63
Flash_Override (FLASHOV) 63
FP_EVT_ INFORMATION (event code) 178
FP_EVT_ TRACE_START (event code) 178
FP_EVT_ TRACE_STOP (event code) 178
FP_EVT_CRITICAL (event code) 183
FP_EVT_INDETERMINATE (event code) 179
FP_EVT_MAJOR (event code) 183
FP_EVT_MINOR (event code) 178
FP_EVT_SNMP_TRAP (event code) 178
FP_EVT_WARNING (event code) 183
Frame Size (parameter) 58, 58, 62

G

G.711 57, 284
G.723.1 284
G.729 57, 62, 284
Gatekeeper 284
Gateway IP Address (parameter) 35
Gateway Location (parameter) 34
Gateway Subnet Mask (parameter) 35
Gateways 284
Group Pickup DAR (Digit Analysis Result) 64

H

H323 (trace component) 125
H323_MISSING_PARAMETER (event code) 196
Headers only 89
hostname 260
HTTP 13

I

Immediate Call (IMMED) 63
Input fields 19
International Prefix (parameter) 54
Internet Explorer 13
IP Address 64
IP Address of Client 64
IP addresses 285
IP addressing 269
IP Networking Mode 59
ipconfig 257
ISDN 285
IVR 285

L

LAN 285
Level 0 code (parameter) 54
Level 0 prefix (parameter) 54
Level 1 code (parameter) 54
Level 1 prefix (parameter) 54
Level 2 code (parameter) 54
Level 2 prefix (parameter) 54
Location Code (parameter) 54
Locked (parameter) 64
LoopBack interface (only) 89

M

Manager 20
Max. UDP Datagram Size for T.38 Fax (parameter) 58
Maximum Trace File Size (byte) (parameter) 100
MCU 285
Memory Usage Threshold for Heapdump 89
MIB 286
MSG_ADMIN_DIDN'T_GET_WRITE_ACCESS (event code) 233
MSG_ADMIN_FORCE_RELEASE_WRITE_ACCESS (event code) 233
MSG_ADMIN_GOT_WRITE_ACCESS (event code) 233
MSG_ADMIN_LOGGED_IN (event code) 232
MSG_ADMIN_LOGGED_OUT (event code) 233, 233
MSG_ADMIN_REBOOT (event code) 180
MSG_ADMIN_RELEASED_WRITE_ACCESS (event code) 233
MSG_ADMIN_SESSION_CREATED (event code) 232
MSG_ADMIN_SESSION_EXPIRED (event code) 233
MSG_ASC_ERROR (event code) 246
MSG_ASP_ERROR (event code) 246
MSG_ASP_INFO (event code) 245, 246
MSG_BSD44_ACCEPT_DGW_ERR (event code) 199
MSG_BSD44_ACCEPT_ERROR (event code) 221
MSG_BSD44_DGW_BIND_FAIL (event code) 199
MSG_BSD44_DGW_CONNECT_FAIL (event code) 199
MSG_BSD44_DGW_NO_LIST (event code) 199
MSG_BSD44_DGW_SOCKET_FAIL (event code) 199
MSG_BSD44_SELECT_ERROR (event code) 220
MSG_BSD44_VCAPI_NO_LIST (event code) 199
MSG_CAR_ALIVE_IP_CONNECTION_LOST (event code) 207, 207
MSG_CAR_ALIVE_IP_CONNECTION_OK_AGAIN (event code) 207
MSG_CAR_CALL_ADDR_REJECTED (event code) 234
MSG_CAR_CAN_NOT_ARRANGE_NODE_TAB (event code) 208
MSG_CAR_CAN_NOT_SORT_MAC_ADDRESS (event code) 208
MSG_CAR_CODEC_ENTRY_DELETED (event code) 210
MSG_CAR_CODECS_INCONSISTENT (event code) 208
MSG_CAR_DB_READ_NODE_TABLE_ERROR (event code) 207
MSG_CAR_DBF_SERVER_INCONSISTENT (event code) 208
MSG_CAR_DBFS_POSS_CONFLICT (event code) 209
MSG_CAR_ERROR_WITH_OAM_INTERFACE (event code) 207
MSG_CAR_FKT_GET_IPADR_FAILED (event code) 206
MSG_CAR_GENERAL_ERROR (event code) 206
MSG_CAR_MALLOC_FAILED (event code) 185
MSG_CAR_NO_FREE_CODEC_TAB_ELE (event code) 208
MSG_CAR_NO_MAC_ADDRESS (event code) 209
MSG_CAR_NO_MEMORY (event code) 206
MSG_CAR_NODE_INFO_ALREADY_AVAILABLE (event code) 208
MSG_CAR_PARAM_NOT_FOUND (event code) 209
MSG_CAR_SENDING_UPDATE_REQUEST_FAILED_SOH_ERROR (event code) 206, 207
MSG_CAR_SOH_MESSAGE_NOT_FROM_VENUS (event code) 207
MSG_CAR_START_TCP_LISTENER_FAILED (event code) 206
MSG_CAR_UNAUTHORIZED_IP_ACCESS (event code) 209
MSG_CAR_UNEXPECTED_DATA_RECV (event code) 209
MSG_CAR_UNEXPECTED_MSG_RECV (event code) 209
MSG_CAR_UPDATE_NUMBER_OF_ENTRIES_CALLADDRTAB_TO (event code) 207
MSG_CAR_WRONG_EVENT (event code) 209
MSG_CAR_WRONG_IP_ADDRESS (event code) 209
MSG_CAR_WRONG_LENGTH (event code) 209
MSG_CAR_WRONG_NODE_ID (event code) 208
MSG_CAR_WRONG_SERVICE (event code) 208
MSG_CAT_H235 (event code) 198
MSG_CAT_HSA_REBOOT (event code) 180
MSG_CAT_NWRS (event code) 186
MSG_CLI_LOGGED_IN_FROM_TELNET (event code) 234
MSG_CLI_LOGGED_IN_FROM_V24 (event code) 234
MSG_CLI_TELNET_ABORTED (event code) 234
MSG_DELIC_ERROR (event code) 248
MSG_DEVM_BINDING_FAILED (event code) 238
MSG_DEVM_NO_PROTOCOL_FOR_DEVICE (event code) 238, 238

MSG_DEVMGR_CAN_NOT_READ_PERSISTENCY (event code) 239
MSG_DEVMGR_CLOSE_LEG_FAILED (event code) 243
MSG_DEVMGR_CONNECT_LEGS_FAILED (event code) 243
MSG_DEVMGR_CONNECT_WRONG_LEGS (event code) 243
MSG_DEVMGR_CONNECT_WRONG_RES_STATE (event code) 243
MSG_DEVMGR_CREATE_FAILED (event code) 239
MSG_DEVMGR_DEVICEID_OUT_OF_RANGE (event code) 238
MSG_DEVMGR_DISCONNECT_LEGS_FAILED (event code) 243
MSG_DEVMGR_INTERROR_CHNID (event code) 242
MSG_DEVMGR_INTERROR_DEVID (event code) 239
MSG_DEVMGR_INTERROR_RESID (event code) 241
MSG_DEVMGR_LAYER2_SERVICE_TRAP (event code) 245
MSG_DEVMGR_LISTEN_WRONG_RES_STATE (event code) 243
MSG_DEVMGR_MSCERROR_RESID (event code) 242
MSG_DEVMGR_NO_DEVICE_ID_FOR_DEVICE (event code) 239
MSG_DEVMGR_NO_DEVICE_TYPE_FOR_DEVICE (event code) 238
MSG_DEVMGR_OPEN_LEG_FAILED (event code) 242
MSG_DEVMGR_OPEN_WRONG_RES_STATE (event code) 243
MSG_DEVMGR_SCN_TASK_FAILED (event code) 239
MSG_DEVMGR_UPDATE_LEG_FAILED (event code) 243
MSG_DGW_ABORT_SOCK_UNKN (event code) 204
MSG_DGW_ACCEPT_FAILED (event code) 206
MSG_DGW_ALLOC_CHN_CONN_FAIL (event code) 202
MSG_DGW_ALLOC_CHN_RUN_OUT (event code) 202
MSG_DGW_ALLOC_DISC_B3 (event code) 200
MSG_DGW_ALLOC_REQ_ERR (event code) 200, 201
MSG_DGW_BUFAVAIL_SOCK_UNKN (event code) 204
MSG_DGW_CONF_ALLOC_ERR (event code) 202
MSG_DGW_CONN_B3_ACT_IND (event code) 200
MSG_DGW_CONN_COMPL_ALLOC (event code) 204
MSG_DGW_CONN_OUT_OF_RANGE (event code) 199
MSG_DGW_CONN_RUN_OUT (event code) 204
MSG_DGW_CONNECT_FAILED (event code) 203
MSG_DGW_DATA_B3_ALLOC_ERR (event code) 200
MSG_DGW_DISC_B3_IND (event code) 200
MSG_DGW_DISC_B3_NOT_SEND (event code) 203
MSG_DGW_FREE_ALLOC_ERR (event code) 201
MSG_DGW_FREE_CHN_ALLOC_FAIL (event code) 203
MSG_DGW_FREE_NOT_SEND (event code) 203
MSG_DGW_FREE_UNKNOWN_ID (event code) 202
MSG_DGW_IND_ALLOC_ERR (event code) 201
MSG_DGW_INV_DATA_LEN (event code) 205
MSG_DGW_INV_MSG_LEN (event code) 205
MSG_DGW_INVALID_LENGTH (event code) 205
MSG_DGW_LISTENING_ERR (event code) 206
MSG_DGW_MGR_NOT_READY (event code) 204
MSG_DGW_MSG_IGNORED (event code) 200
MSG_DGW_MSG_RCV_FAIL (event code) 205
MSG_DGW_NO_PLCI (event code) 201
MSG_DGW_OPEN_CHN_ALLOC_FAIL (event code) 202
MSG_DGW_OPEN_CHN_UNKNOWN_ID (event code) 202
MSG_DGW_OPEN_CHN_WRONG (event code) 202
MSG_DGW_RCV_ALLOC_FAIL (event code) 205
MSG_DGW_RCV_FAILED (event code) 204
MSG_DGW_RCV_SOCK_UNKN (event code) 204
MSG_DGW_RECEIVE_ERR (event code) 201
MSG_DGW_SEC_ALLOC_FAIL (event code) 203, 203
MSG_DGW_SEND_DATA_ERR (event code) 205
MSG_DGW_SEND_FAILED (event code) 205
MSG_DGW_SOCKET_BIND_ERR (event code) 205
MSG_DGW_SOCKET_NOT_OPEN (event code) 205
MSG_DGW_SOCKET_UNKNOWN (event code) 203
MSG_DGW_UNHANDLED_EVENT (event code) 201
MSG_DGW_UNHANDLED_MSG (event code) 200
MSG_DGW_UNKNOWN_ID_CHANNEL (event code) 203
MSG_DGW_UNKNOWN_NOTIFIC (event code) 204
MSG_DGW_UNKNOWN_PRIMITIVE (event code) 201
MSG_DGW_WRONG_EVENT_CAPI (event code) 202
MSG_DGW_WRONG_EVENT_CAPI20 (event code) 201
MSG_DGW_WRONG_STATE (event code) 199
MSG_DISP_SENDER_NOT_SET (event code) 231
MSG_ERH_ADMISSION_ERROR (event code) 252
MSG_ERH_ERROR (event code) 251, 251
MSG_ERH_NO_LICENSE (event code) 252
MSG_ERH_REGISTRATION_ERROR (event code) 252
MSG_ERH_SECURITY_DENIAL (event code) 252
MSG_FAXCONV_ERROR (event code) 249
MSG_FAXCONV_INFO (event code) 249
MSG_GSA_SNMP (event code) 198
MSG_GW_OBJ_ALLOC_FAILED (event code) 181
MSG_GW_OBJ_MEMORY_EXHAUSTED (event code) 181
MSG_GW_OBJ_MEMORY_INCONSISTENT (event code) 181
MSG_GW_SUCCESSFULLY_STARTED (event code) 177
MSG_H323_INFORMATION (event code) 197
MSG_H323_INVALID_CONFIGURATION (event code) 196
MSG_H323_INVALID_PARAMETER_VALUE (event code) 196
MSG_H323_INVALID_POINTER (event code) 197
MSG_H323_LOGIC_ERROR (event code) 197
MSG_H323_OSCAR_NSD_ERROR (event code) 197
MSG_H323_PROTOCOL_ERROR (event code) 197
MSG_H323_SNMP_TRAP (event code) 198
MSG_H323_STACK_ERROR (event code) 197
MSG_H323_UNEXPECTED_MESSAGE (event code) 197
MSG_H323_UNEXPECTED_RETURN_VALUE (event code) 196
MSG_H323CLIENT_INVALID_ADMIN_MSG (event code) 229
MSG_H323CLIENT_INVALID_CLIENTID (event code) 229
MSG_H323CLIENT_INVALID_PARAM (event code) 229
MSG_H323CLIENT_MAPS_DIFFER (event code) 230
MSG_H323CLIENT_NWRS_ENTRY_FAILED (event code) 229

MSG_HACKER_ON_SNMP_PORT_TRAP (event code) 186
MSG_HFAA_INTERNAL_ERROR (event code) 219
MSG_HFAA_INTERNAL_EVENT (event code) 219
MSG_HFAA_MEMORY_ERROR (event code) 219
MSG_HFAA_MESSAGE_ERROR (event code) 219
MSG_HFAA_PARAM_ERROR (event code) 219
MSG_HFAM_HAH_ALLOC_CHAN_ERR (event code) 214
MSG_HFAM_HAH_ALLOC_CONF_ERR (event code) 214
MSG_HFAM_LIH_ACCEPT_CLIENT_CON_ERR (event code) 216
MSG_HFAM_LIH_ACCEPT_INETOA_CON_ERR (event code) 216
MSG_HFAM_LIH_ACCEPT_TCPIP_CON_ERR (event code) 215
MSG_HFAM_LIH_ALGORITM_OBJID_ERR (event code) 217
MSG_HFAM_LIH_BIND_REGISOCK_ERR (event code) 215
MSG_HFAM_LIH_CREATE_REGISOCK_ERR (event code) 215
MSG_HFAM_LIH_IPADR_TOO_LONG_ERR (event code) 216
MSG_HFAM_LIH_LISTEN_REGISOCK_ERR (event code) 215
MSG_HFAM_LIH_MAX_CON_EXCEED_ERR (event code) 216
MSG_HFAM_LIH_PROTOCOL_LIST_ERR (event code) 217
MSG_HFAM_LIH_RETURNED_SOCKET_ERR (event code) 217
MSG_HFAM_LIH_SOCK_REUSE_ADR_ERR (event code) 215
MSG_HFAM_LIH_SOCK_WOULDBLOCK_ERR (event code) 216
MSG_HFAM_LIH_SUBNO_TOO_LONG_ERR (event code) 216
MSG_HFAM_LIH_TCDATAGRAM_RCV_ERR (event code) 216
MSG_HFAM_LIH_UNEXP_CORNET_ERR (event code) 216
MSG_HFAM_MAIN_ILLEG_PORTNO_ERR (event code) 215
MSG_HFAM_MAIN_NO_LOGONTIMER_ERR (event code) 215
MSG_HFAM_MAIN_UNEXP_LWEVENT_ERR (event code) 215
MSG_HFAM_MON_NO_MON_TIMER_ERR (event code) 217
MSG_HFAM_REG_ESTAB_NOTREG_ERR (event code) 218
MSG_HFAM_REG_INVAL_PWD_LEN_ERR (event code) 218
MSG_HFAM_REG_LOGIN_NOTREG_ERR (event code) 217
MSG_HFAM_REG_MISSING_L2INFO_ERR (event code) 218, 218
MSG_HFAM_REG_RELIN_NOTREG_ERR (event code) 218
MSG_HFAM_REG_SUBNO_NOTCONFIG_ERR (event code) 218
MSG_HFAM_REG_SUBNO_TOO_LONG_ERR (event code) 218
MSG_HFAM_SIH_CORNET_LONGER_28_ERR (event code) 217
MSG_HFAM_SIH_INVAL_TSLOT_PARAM_ERR (event code) 217
MSG_HFAM_SIH_NO_LOGIN_TIMER_ERR (event code) 217
MSG_HIP_ALLOC_DEV_OBJ (event code) 234
MSG_HIP_ALLOC_MES_SI (event code) 236
MSG_HIP_NO_CLBLK (event code) 236
MSG_HIP_NO_CLPOOL_ID (event code) 235
MSG_HIP_NO_CLUSTER (event code) 236
MSG_HIP_NO_DEVLOAD (event code) 235
MSG_HIP_NO_DEVSTART (event code) 235
MSG_HIP_NO_MEM_CL (event code) 235
MSG_HIP_NO_MEM_CLBLK (event code) 234
MSG_HIP_NO_MEM_TO_SI (event code) 235
MSG_HIP_NO_NETPOOL_INIT (event code) 235
MSG_HIP_NO_OBJ_INIT (event code) 235
MSG_HIP_NO_PMBLK (event code) 236
MSG_HIP_PKTLEN_ZERO (event code) 236
MSG_HIP_PMBLK_ZERO (event code) 236
MSG_IP_LINK_ FAILURE (Event Code) 183
MSG_IP_RTP_QUALITY_FAILURE (event code) 198
MSG_IP_RTP_QUALITY_WARNING (event code) 198
MSG_IPACCSRV_INTERNAL_ERROR (event code) 250
MSG_IPACCSRV_MARK_REACHED (event code) 251
MSG_IPACCSRV_MEMORY_ERROR (event code) 250
MSG_IPACCSRV_MESSAGE_ERROR (event code) 251
MSG_IPACCSRV_OVERFLOW (event code) 251, 251
MSG_IPACCSRV_SOCKET_ERROR (event code) 250
MSG_IPF_ON_OFF (event code) 247
MSG_IPF_PARAMETER (event code) 247
MSG_IPF_STARTED (event code) 246
MSG_IPF_STOPPED (event code) 247
MSG_IPNC_CP_ASYNCH (event code) 230
MSG_IPNC_INCONSISTENT_STATE (event code) 230
MSG_IPNC_INTERNAL_ERROR (event code) 230
MSG_IPNC_MESSAGE_DUMP (event code) 230
MSG_IPNC_MESSAGE_ERROR (event code) 230
MSG_IPNC_PARAM_ERROR (event code) 230
MSG_IPNCA_ERROR (event code) 231
MSG_IPNCV_INTERNAL_ERROR (event code) 178
MSG_IPNCV_MEMORY_ERROR (event code) 186
MSG_IPNCV_SIGNALING_ERROR (event code) 252
MSG_IPNCV_STARTUP_ERROR (event code) 177
MSG_IPNCV_STARTUP_SHUTDOWN 178
MSG_IPNCV_STARTUP_SHUTDOWN (event code) 178
MSG_IPSTACK_INVALID_PARAM (event code) 248
MSG_IPSTACK_NAT_ERROR (event code) 248
MSG_IPSTACK_SOH_ERROR (event code) 248
MSG_ISDN_CMR_ADD_OBJECT_FAILED (event code) 192
MSG_ISDN_CMR_DEVICE_PTR_BAD (event code) 194

MSG_ISDN_CMR_GEN_CALL_REF_FAILED (event code) 194
MSG_ISDN_CMR_GENERIC_EVENT (event code) 193
MSG_ISDN_CMR_INIT_FAILED (event code) 191
MSG_ISDN_CMR_MAND_FIELDS_MISSING (event code) 192
MSG_ISDN_CMR_MESSAGE_ERROR (event code) 195
MSG_ISDN_CMR_MSG_DECODE_FAILED (event code) 192
MSG_ISDN_CMR_MSG_ENCODE_FAILED (event code) 194
MSG_ISDN_CMR_MSG_SEND_FAILED (event code) 194
MSG_ISDN_CMR_MSG_UNEXPECTED (event code) 194
MSG_ISDN_CMR_NEW_OBJECT_FAILED (event code) 192
MSG_ISDN_CMR_OBJECT_NOT_FOUND (event code) 192
MSG_ISDN_CMR_PROTOCOL_ERROR (event code) 195
MSG_ISDN_CMR_SEG_MSG_ERROR (event code) 194
MSG_ISDN_CMR_SESSION_NOT_FOUND (event code) 193
MSG_ISDN_CMR_STATUS_MSG_RECEIVED (event code) 193
MSG_ISDN_CMR_TIMER_EXPIRED (event code) 192
MSG_ISDN_CMR_UNEXPECTED_ERROR (event code) 194
MSG_ISDN_CMR_UNEXPECTED_EVENT (event code) 193
MSG_ISDN_CMR_UNEXPECTED_VALUE (event code) 194
MSG_ISDN_CMR_UNH_STATE_EVENT (event code) 195
MSG_ISDN_CMR_UNIMPLEMENTED (event code) 192
MSG_ISDN_CMR_WRONG_DEVICE_TYPE (event code) 192
MSG_ISDN_CMR_WRONG_INTERFACE (event code) 195
MSG_ISDN_CMR_WRONG_PROTVAR (event code) 193
MSG_ISDN_DEVICE_PTR_NOT_FOUND (event code) 194
MSG_ISDN_ERROR (event code) 195
MSG_ISDN_NO_ERROR (event code) 195
MSG_ISDN_NULL_PTR (event code) 195
MSG_ISDN_OVERLOAD_CONDITION (event code) 196
MSG_ISDN_RESOURC_IN_USE_BY_O_CALL (event code) 193
MSG_ISDN_RESOURCE_NOT_AVAILABLE (event code) 193
MSG_ISDN_RESOURCE_NOT_IN_SERVICE (event code) 193
MSG_ISDN_START_UP (event code) 196
MSG_ISDN_START_UP_ERROR (event code) 195
MSG_LDAP_ENCODE_DECODE_ERROR (event code) 186
MSG_LDAP_GENERAL_ERROR (event code) 186
MSG_LDAP_IP_LINK_ERROR (event code) 186
MSG_LDAP_MEMORY_ERROR (event code) 186
MSG_LDAP_SOCKET_ERROR (event code) 186
MSG_LDAP_SUCCESSFULLY_STARTED (event code) 178
MSG_LLC_EVENT_INVALID_PARAMETER_VALUE (event code) 254
MSG_LLC_EVENT_MISSING_PARAMETER (event code) 253
MSG_LLC_EVENT_MISSING_RESOURCE (event code) 253
MSG_LLC_EVENT_UNEXPECTED_RETURN_VALUE (event code) 253
MSG_MAF_ETHERNET_HEADER (event code) 248
MSG_MAF_NETBUFFER (event code) 248
MSG_MAF_NO_OF_RULES (event code) 247
MSG_MAF_ON_OFF (event code) 247
MSG_MAF_PARAMETER (event code) 247
MSG_MAF_STARTED (event code) 247
MSG_MAF_STOPPED (event code) 247
MSG_MAND_PARAM_MISSING (event code) 191
MSG_MPH_INFO (event code) 231
MSG_MSP_HDLC_ERROR (event code) 250
MSG_MSP_HDLC_INFO (event code) 250
MSG_NU_CAR_FAILED (event code) 211
MSG_NU_CAR_RESP_INVALID (event code) 211
MSG_NU_DEV_TAB_NOT FOUND (event code) 213
MSG_NU_EVENT_EXCEPTION (event code) 212
MSG_NU_FREE_CHN_CONF_TOO_LATE (event code) 212
MSG_NU_FREE_CHN_UNEXPECTED (event code) 212
MSG_NU_GENERAL_ERROR (event code) 211
MSG_NU_INTERNAL_ERROR (event code) 213
MSG_NU_INVALID_CIDL (event code) 211
MSG_NU_IP_ERROR (event code) 213
MSG_NU_NO_FREE_TRANSACTION (event code) 211
MSG_NU_NO_PORT_DATA (event code) 212
MSG_NU_SOH_RESP_INVALID (event code) 213
MSG_NU_SUPERFLUOS_MSG (event code) 213
MSG_NU_TCP_LISTENER_FAILED (event code) 213
MSG_NU_TOO_MUCH_DIGITS (event code) 213
MSG_NU_TRANSPCONT_MISSING (event code) 211
MSG_NU_UNEXPECTED_MSG (event code) 212
MSG_NU_UNEXPECTED_SETUP (event code) 212
MSG_NU_UNEXPECTED_TIMER (event code) 212
MSG_NU_UNKNOWN_MESSAGE (event code) 213
MSG_NU_WRONG_CALL_REF (event code) 212
MSG_NULC_INTERNAL_ERROR (event code) 214
MSG_NULC_INTERNAL_EVENT (event code) 214
MSG_NULC_MEMORY_ERROR (event code) 214
MSG_NULC_MESSAGE_ERROR (event code) 214
MSG_NULC_PARAM_ERROR (event code) 214
MSG_NWRS_DEVICE_NOT_FOUND (event code) 188
MSG_NWRS_DEVICE_TABLE_NOT_FOUND (event code) 188
MSG_NWRS_DPLN_ENTRY_INVALID (event code) 187
MSG_NWRS_EMPTY_FIELD_ECHOED (event code) 187
MSG_NWRS_NO_DPLN_FOUND_FOR_DEVICE (event code) 187
MSG_NWRS_ODR_COMMAND_UNKNOWN (event code) 187
MSG_NWRS_ODR_NOT_FOUND (event code) 187

MSG_NWRS_ROUTE_NOT_FOUND (event code) 188, 188, 188
MSG_NWRS_UNKNOWN_FIELD_ECHOED (event code) 187
MSG_OAM_DMA_RAM_THRESHOLD_REACHED (event code) 184
MSG_OAM_FAN_OUT_OF_SERVICE (event code) 185
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION (event code) 185
MSG_OAM_INTERNAL_EVENT (event code) 232
MSG_OAM_PRIO_INCREASED (event code) 231
MSG_OAM_PRIO_SWITCHED_BACK (event code) 232
MSG_OAM_PSU_OR_RPS_OUT_OF_SERVICE (event code) 185
MSG_OAM_PUT_TO_QUEUE_FAILED (event code) 232
MSG_OAM_QUEUE_BLOCKED (event code) 232
MSG_OAM_QUEUE_FULL (event code) 232
MSG_OAM_RAM_THRESHOLD_REACHED (event code) 184
MSG_OAM_THRESHOLD_REACHED (event code) 185
MSG_OAM_TIMESYNC (event code) 231
MSG_OAM_TIMESYNC_FAILED (event code) 231
MSG_OSF_PCS_ERROR (event code) 253
MSG_OSF_PCS_EXCEPTION (event code) 180
MSG_PPPM_ERR_CONFIG (event code) 219
MSG_PPPM_ERR_OPERATION (event code) 219, 220
MSG_REG_ERROR_FROM_SOH (event code) 210
MSG_REG_GLOBAL_ERROR (event code) 210
MSG_REG_NIL_PTR_FROM_SOH (event code) 210
MSG_REG_NO_MEMORY (event code) 210
MSG_REG_NO_REGISTRATION_POSSIBLE (event code) 211
MSG_REG_REQUEST_WITHIN_REGISTRATION (event code) 210
MSG_REG_SOH_SEND_DATA_FAILED (event code) 210
MSG_REG_SOH_UNKNOWN_EVENT_FROM_SOH (event code) 211
MSG_RESTORE_CFG_REBOOT (event code) 181
MSG_SCN_ADD_PARAMETER_FAILED (event code) 244
MSG_SCN_BIND_FAILED (event code) 245
MSG_SCN_DEV_NOT_IN_DEVLIST (event code) 244
MSG_SCN_ERROR_12_MSG (event code) 244
MSG_SCN_GET_ADMMSG_FAILED (event code) 244
MSG_SCN_GET_LDAPMSG_FAILED (event code) 244
MSG_SCN_OPEN_STREAM_FAILED (event code) 245
MSG_SCN_OPERATION_ON_STREAM_FAILED (event code) 244
MSG_SCN_POLL_FD (event code) 244
MSG_SCN_UNEXPECTED_L2_MSG (event code) 244
MSG_SCN_UNEXPECTED_POLL_EVENT (event code) 245
MSG_SDR_INIT (event code) 188
MSG_SDR_UNEXPECTED_EVENT (event code) 188
MSG_SI_L2STUB_ERROR_INIT_DRIVER (event code) 237
MSG_SI_L2STUB_NO_ALLOC (event code) 237
MSG_SI_L2STUB_NO_CLONE (event code) 237
MSG_SI_L2STUB_OPEN_OTHER_STREAM_NOT_POSSIBLE (event code) 237
MSG_SI_L2STUB_PORT_NOT_OPEN (event code) 237
MSG_SI_L2STUB_STREAM_ALREADY_OPEN (event code) 236, 237
MSG_SI_L2STUB_UNEXPECTED_DB_TYPE (event code) 237
MSG_SI_L2STUB_UNEXPECTED_EVENT_CODE (event code) 238
MSG_SI_L2STUB_UNKNOWN_SOURCE_PID (event code) 237
MSG_SIP_FM_INTERNAL_ERROR (event code) 179
MSG_SIP_FM_MSG_INTERNAL_ERROR (event code) 179
MSG_SIP_FM_MSG_NOT_PROCESSED (event code) 179
MSG_SIP_FM_STARTUP_FAILURE (event code) 179
MSG_SNCP_ADD_OBJECT_FAILED (event code) 190
MSG_SNCP_CHANNEL_ID_MISSING (event code) 189
MSG_SNCP_COULD_NOT_CREATE_OBJECT (event code) 189
MSG_SNCP_COULD_NOT_DELETE_OBJECT (event code) 189
MSG_SNCP_COULD_NOT_SET_FORW_ENC (event code) 189
MSG_SNCP_COULD_NOT_SET_REV_ENC (event code) 190
MSG_SNCP_DEVICE_ID_MISSING (event code) 189
MSG_SNCP_ERROR (event code) 190
MSG_SNCP_NEITHER_ENC_COULD_BE_SET (event code) 190
MSG_SNCP_NO_RESOURCE_ID (event code) 189
MSG_SNCP_UNANTICIPATED_MESSAGE (event code) 189
MSG_SNMP_TRAP_COLLECTOR_START_ERROR (event code) 182
MSG_SPL_ADD_OBJECT_FAILED (event code) 190
MSG_SPL_ERROR (event code) 191
MSG_SPL_FMSEM_ERROR (event code) 191
MSG_SPL_MISSING_CS_ID (event code) 190
MSG_SPL_SESSION_NOT_FOUND (event code) 190
MSG_SPL_UNANTICIPATED_MESSAGE (event code) 190
MSG_SSM_BAD_NWRS_RESULT (event code) 191
MSG_SSM_INVALID_PARAM (event code) 191
MSG_SSM_NO_CS_ID (event code) 191
MSG_SSM_NUM_OF_CALL_LEGS_2BIG (event code) 182
MSG_SSM_SESSION_CREATION_FAILED (event code) 182
MSG_SSM_UNSPEC_ERROR (event code) 191
MSG_SYSTEM_REBOOT (event code) 180, 181
MSG_T90_ERROR (event code) 249
MSG_T90_INFO (event code) 249
MSG_TESTLW_ERROR (event code) 249
MSG_TESTLW_INFO (event code) 248
MSG_TLS_MUTEX_BLOCKED (event code) 231
MSG_TLS_POOL_SIZE_EXCEEDED (event code) 182
MSG_VCAPI_ACCEPT_ERROR (event code) 222
MSG_VCAPI_ADD_OBJECT_FAILED (event code) 228
MSG_VCAPI_BUF_NOT_CREATED (event code) 223

MSG_VCAPI_CONF_ALLOC_ERR (event code) 224
MSG_VCAPI_CONF_WITHOUT_REQ (event code) 229
MSG_VCAPI_CONV_H2N_ERROR (event code) 221
MSG_VCAPI_CONV_H2N_FAILED (event code) 221
MSG_VCAPI_CONV_N2H_FAILED (event code) 222
MSG_VCAPI_COULD_NOT_CREATE_OBJECT (event code) 228
MSG_VCAPI_COULD_NOT_DELETE_OBJECT (event code) 228
MSG_VCAPI_COULD_NOT_FIND_CSID (event code) 229
MSG_VCAPI_COULD_NOT_FIND_OBJECT (event code) 228
MSG_VCAPI_COULD_NOT_FIND_PLCI (event code) 228
MSG_VCAPI_COULD_NOT_STORE_REQ (event code) 229
MSG_VCAPI_CSID_MISSING (event code) 228
MSG_VCAPI_DATA_B3_ALLOC_ERR (event code) 225
MSG_VCAPI_DATA_NOT_STORED (event code) 223
MSG_VCAPI_DISP_NOT_READY (event code) 222
MSG_VCAPI_ILLEGAL_LINK_NUMBER (event code) 227
MSG_VCAPI_ILLEGAL_PARTNER_NUMBER (event code) 228
MSG_VCAPI_IND_ALLOC_ERR (event code) 224
MSG_VCAPI_LINK_TABLE_FULL (event code) 221, 221
MSG_VCAPI_LISTENING_ERR (event code) 224
MSG_VCAPI_MESSAGE_LENGTH_TOO_SHORT (event code) 227
MSG_VCAPI_MSG_NOT_SEND (event code) 225
MSG_VCAPI_MSGBASE_WITHOUT_CAPIMSG (event code) 227
MSG_VCAPI_MSGBASE_WITHOUT_DATAGWMSG (event code) 227
MSG_VCAPI_MSGBASE_WITHOUT_DISPMSG (event code) 227
MSG_VCAPI_NO_ALLIC_MSG (event code) 224
MSG_VCAPI_NO_ALLOC_EXTENDED (event code) 223
MSG_VCAPI_NO_ALLOC_SINGLE (event code) 223
MSG_VCAPI_NO_CAPI_DATA (event code) 221
MSG_VCAPI_NO_CLIENT (event code) 222
MSG_VCAPI_NO_LIST_SOCKET (event code) 225
MSG_VCAPI_NO_LNK_CONN (event code) 226
MSG_VCAPI_NO_NEW_BUF (event code) 223
MSG_VCAPI_NO_PLCI_AVAILABLE (event code) 228
MSG_VCAPI_NO_PLCI_DATA_B3 (event code) 225
MSG_VCAPI_NO_PLCI_DISCONNECT (event code) 225
MSG_VCAPI_NO_RCV_BUFFER (event code) 223
MSG_VCAPI_PLCI_NOT_FOUND (event code) 224
MSG_VCAPI_RCV_LEN_ERR (event code) 226
MSG_VCAPI_RECEIVE_ERR (event code) 224
MSG_VCAPI_SERVER_ERROR (event code) 226
MSG_VCAPI_SOCK_NOT_AVAIL (event code) 226
MSG_VCAPI_SOCKET_BIND_ERR (event code) 224
MSG_VCAPI_SOCKET_NOT_OPEN (event code) 223
MSG_VCAPI_SOCKET_RCV_ERR (event code) 226
MSG_VCAPI_TOO_MANY_CLIENTS (event code) 222
MSG_VCAPI_UNANTICIPATED_CAPI_MESSAGE (event code) 226
MSG_VCAPI_UNANTICIPATED_DISP_MESSAGE (event code) 227
MSG_VCAPI_UNANTICIPATED_MESSAGE (event code) 226
MSG_VCAPI_UNANTICIPATED_MESSAGE_BASE (event code) 227
MSG_VCAPI_UNKNOWN_MSG_N2H (event code) 222, 222
MSG_VCAPI_UNKNOWN_NTFY (event code) 226
MSG_VCAPI_WRONG_BUF_LEN (event code) 223
MSG_VCAPI_WRONG_CONV_H2N (event code) 221
MSG_VCAPI_WRONG_EVENT_CAPI (event code) 225
MSG_VCAPI_WRONG_EVENT_SRV (event code) 224
MSG_VCAPI_WRONG_LENGTH_MSG (event code) 225
MSG_VCAPI_WRONG_LINKNUM (event code) 221
MSG_VCAPI_WRONG_MSG_LENGTH (event code) 222
MSG_WEBSERVER_INTERNAL_ERROR (event code) 234
MSG_WEBSERVER_MAJOR_ERROR (event code) 180
MSG_X25_ERROR (event code) 250
MSG_X25_INFO (event code) 249
MSG_X75_ERROR (event code) 250
MSG_X75_INFO (event code) 250
MSG_XMLUTILS_ERROR (event code) 252
Multicast 286

N

National Prefix (parameter) 54
nbtstat 263
netstat 260
nslookup 259
Number of Circuits Configured for IP Networking 59
Number of Echo Requests to Send (parameter) 52

O

Only Secure (parameter) 64
OpenScape 4000 Manager 20

P

Password 15, 15
PBX 287
Physical Node Number (4K) 34
ping 256
Port number 64
Prerequisites
    Hardware 13
    Software 13
PRI 287
Priority (parameter) 58, 62
Priority Call (PRTY) 63
Priority Class for Data Payload (parameter) 36
Priority Class for Network Control (parameter) 36
Priority Class for Signaling Data (parameter) 36
Priority Class for Voice Payload (parameter) 36
Product documentation 17

PSTN 287

Q

Q.931 288
QDC_ERROR_IN_CLIENT (event code) 255
QDC_INVALID_CONFIGURATION (event code) 254
QDC_PERSYSTENCY_ERROR (event code) 254
QDC_SIGNALLING_DATA_ERROR (event code) 254
QDC_SYSTEM_ERROR (event code) 254
QDC_VOIPSD_ERROR (event code) 255
QSIG 288
Quality of Service Data Collection (QDC) 29

R

Radio buttons 19
RAS 288
Realm 64
RIP 288
Route 265
Router 288
Routine Call (DSNR) 63
RTP 288

S

Sample rate 89, 89
SCN 288
Secure trace
    basic procedure 79
SecureTrace for these protocols 106
SecureTrace is active 106
Send an E-mail (parameter) 111, 112
Server port 100
Signaling Protocol for IP Networking 35, 59
SIP Trunk Profile Parameter 60
SIP via TCP 57
SIP via TLS 57
SIP via UDP 57
SIP_INFORMATION (event code) 255
SIP_INVALID_PARAMETER_VALUE (event code) 255
SIP_INVALID_POINTER (event code) 255
SIP_REBOOT (event code) 183
SIP_UNEXPECTED_RETURN_VALUE (event code) 255
Sound cards 276
Start 89, 89, 89
Start/Stop Trace Profile (parameter) 111, 112
Starting WBM 15
Station number 64
Status 89, 89, 89
Subnets 269
Subscriber Prefix (parameter) 54
Support for Dispatch Application 35
Switch Event Logging via LAN On (parameter) 110
System Country Code (parameter) 35
System Name (parameter) 34

T

T.38 289
T.38 Fax (Parameter) 58
TCP/IP diagnostics 256
Terminal Devices 283
Thread CPU Load Threshold for Stacktrace 89
Timer Value (sec) (parameter) 100
TIs used 64
TOS Byte (parameter) 53
tracert 267

U

Use DMC 64
User account 15
User name 15
User-Id of Client 64
Utility programs 256

V

Voice Activity Detection (VAD) (parameter) 58, 62
VoIP 290

W

WBM 13
    control area 16
    control icons 17
    function area 16, 16
    icons 17
    menu area 16
    starting 15
WBM icons 17

X

XTracer Connected (parameter) 100