

Documentation

HiPath 3000/5000 V9 Configuration Examples

Administrator Documentation

A31003-H3590-M102-7-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standard certified by an external certification company.

Copyright © Siemens Enterprise Communications GmbH & Co. KG 06/2012
Hofmannstr. 51, D-80200 München

Siemens Enterprise Communications GmbH & Co. KG is a Trademark Licensee of Siemens AG

Reference No.: A31003-H3590-M102-7-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

OpenScape, OpenStage and HiPath are registered trademarks of Siemens Enterprise Communications GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Contents

1 HiPath 3000 Manager E Service Tasks	1-1
1.1 Transferring CDBs (HiPath 5000 RSM/AllServe Server)	1-2
1.2 Transferring CDBs (Single Communication System)	1-4
1.3 Configuring Stations	1-6
1.4 Programming and Labeling Keys	1-9
1.5 Configuring IP Clients	1-12
1.6 Configuring Call Pickup	1-13
1.7 Configuring Call Forwarding	1-14
1.8 Configuring Groups/Hunt Groups	1-16
1.9 Loading IVM Data	1-17
1.10 Configuring IVM - Music On Hold (MOH)	1-18
1.10.1 Changing Music-on-hold Announcements	1-19
1.10.2 Playback Sequence of Entries 1-4 on a Music-on-hold Port	1-20
1.11 Configuring IVM Announcements	1-21
1.12 Configuring Classes of Service	1-22
1.13 Configuring Call Detail Recording	1-27
1.14 Configuring System Parameters	1-30
1.15 APS Transfer	1-34
1.16 Swapping/Replacing Languages	1-35
1.17 Incoming Calls that Display Company Names	1-36
1.18 Announcement Prior to Answer (on an Analog Port)	1-38
1.19 Configuring an Internal S ₀ Bus with Multiple Stations	1-39
1.20 Remote Service via ISDN	1-40
1.21 Universal Call Distribution (UCD)	1-42
1.22 Configuring Attendants	1-44
1.23 Configuring Mobility Entry (not the U.S.)	1-45
1.24 Loading Logos for OpenStage Telephones	1-54
1.24.1 Transfer of the Logo Files to the System	1-54
1.24.2 Download of the Logos in the OpenStage Telephones	1-56
2 Practical Examples for HG 1500	2-1
2.1 License Management	2-2
2.1.1 Target Configuration	2-2
2.1.2 Configuration Steps	2-3
2.2 HiPath Feature Access	2-4
2.2.1 Target Configuration	2-4
2.2.2 Configuration Steps	2-5
2.3 IP Networking (Data)	2-6
2.3.1 Target Configuration	2-6
2.3.2 Configuration Steps	2-8
2.4 Host Routing	2-9
2.4.1 Target Configuration	2-9

Contents

2.4.2 Configuration Steps	2-10
2.5 Host Routing With Alternate Route	2-13
2.5.1 Target Configuration	2-13
2.5.2 Configuration Steps	2-14
2.6 LAN-LAN Routing	2-19
2.6.1 Target Configuration	2-19
2.6.2 Configuration Steps	2-19
2.7 Static Routing	2-21
2.7.1 Target Configuration	2-21
2.7.2 Configuration Steps	2-22
2.8 Configuring an Internet Telephony System Connection	2-26
2.8.1 Target Configuration	2-26
2.8.2 Initial Setup in the HiPath 3000 Manager E	2-28
2.8.3 Router Entry via the HG 1500 WBM	2-33
2.8.4 Configuration via HG 1500 WBM	2-34
2.8.5 Check Setup	2-39
2.9 Adding Internet Telephony User Connections	2-40
2.9.1 Target Configuration	2-40
2.9.2 Configuration in HiPath 3000 Manager E	2-41
2.9.3 Configuration via HG 1500 WBM	2-44
2.9.4 Check Setup	2-46
2.10 HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication	2-47
2.10.1 Target Configuration	2-47
2.10.2 Activate SSL Secure Access	2-49
2.10.3 Create CA Certificates on the Master System	2-50
2.10.4 HiPath 2000/HiPath OpenOffice EE to HiPath 3000 VPN Tunnel Configuration	2-56
2.10.5 Rules, Services, General	2-59
2.10.6 Tracing, Troubleshooting and Checking the Configuration	2-60
2.10.7 Configuring a VPN Remote Client on the HiPath 2000/HiPath OpenOffice EE .	2-61
2.10.8 VPN Remote Client Software	2-63
2.10.9 VPN Client Configuration for Tunnel with HiPath 2000	2-64
2.10.10 Tunnel VPN client configuration with HiPath 2000/HiPath OpenOffice EE . .	2-68
2.10.11 VPN Client Configuration for Tunnel with HiPath 3000	2-70
2.11 ISDN-Based Connection Between LANs	2-71
2.11.1 Target Configuration	2-71
2.11.2 Configuration Steps	2-72
2.12 Firewall Functionality (Authorization Firewall)	2-73
2.12.1 Target Configuration	2-73
2.12.2 Configuration Steps for IP Filter	2-75
2.12.3 Configuration Steps for MAC Filter	2-75
2.13 IP Firewall	2-76
2.13.1 Target Configuration	2-76
2.13.2 Configuration Steps	2-77

2.14	Call-By-Call Internet Connection	2-80
2.14.1	Target Configuration	2-80
2.14.2	Configuration Steps	2-81
2.15	ISP Access over ADSL	2-83
2.15.1	Target Configuration	2-83
2.15.2	Configuration Steps	2-84
2.16	Teleworking via PPP (ISDN, Analog Modem, GSM)	2-85
2.16.1	Target Configuration	2-85
2.16.2	Settings for PPP Connection with Analog Modem or GSM	2-85
2.16.3	Settings for PPP Connection with ISDN	2-86
2.17	Connecting Teleworkers when Using VPN and Firewall	2-87
2.17.1	Basic Requirements	2-87
2.17.2	"Routing HG" Configuration (Board 1)	2-89
2.17.3	"Teleworker HG" Configuration (Board 2)	2-92
2.18	Home Workstation / Remote Service	2-96
2.18.1	Target Configuration	2-96
2.18.2	Configuration Steps	2-97
2.19	Administration via RDT Connection (Remote Access)	2-99
2.19.1	Target Configuration	2-99
2.19.2	Configuration Steps	2-100
2.20	Internet-Based Administration	2-101
2.20.1	Target Configuration	2-101
2.20.2	Configuration Steps	2-102
2.21	IP Accounting at Teleworker PCs	2-103
2.21.1	Target Configuration	2-103
2.21.2	Configuration Steps	2-104
2.22	IP Accounting at the Internet Connection	2-105
2.22.1	Target Configuration	2-105
2.22.2	Configuration Steps	2-106
2.23	IP Accounting Between LAN 1 and LAN 2	2-107
2.23.1	Target Configuration	2-107
2.23.2	Configuration Steps	2-108
2.24	Setting up a VPN Configuration	2-109
2.24.1	Target Configuration	2-109
2.24.2	Setting up SSL via a V.24 Interface and CLI	2-110
2.24.3	Additional Administration Steps over WBM and HTTPS	2-112
2.24.4	Configuring Tunnels with Pre-Shared Keys	2-116
2.24.5	Deleting Tunneling and Rules	2-126
2.24.6	Setting up a Tunnel with Digital Signatures	2-127
2.24.7	Internet Access for the Corporate Network	2-133
2.24.8	Configuring Teleworkers for HiPath 3800 and HiPath 3500	2-134
2.24.9	Connection Setup between Teleworkers	2-146
2.24.10	Teleworker 1 (DSL) Access to the Remote Station LAN	2-147
2.24.11	Internet Access for Teleworker 1 (DSL) via HiPath 3800	2-149

Contents

2.24.12	Creation of Certificates for Multigateway Administration	2-149
2.25	Setting up an E-Mail Connection	2-155
2.25.1	Target Configuration	2-155
2.25.2	WBM Settings	2-156
2.26	SNMP with HG 1500	2-157
2.26.1	Target Configuration	2-157
2.26.2	Configuration Steps	2-157
2.27	Multigateway Administration	2-161
2.27.1	Target Configuration	2-161
2.27.2	Configuration Steps	2-162
3	Signaling & Payload Encryption (SPE) – Encryption	3-1
3.1	Overview	3-1
3.2	SPE Configuration in a HiPath 3000/5000 from V7 R4 Environment	3-2
3.2.1	Prerequisites for Configuration	3-2
3.3	Generating SPE Certificates via the HG 1500 WBM	3-4
3.3.1	Certificate Generation	3-4
3.3.2	Generating the Root CA Certificate	3-5
3.3.3	Saving the Root CA Certificate	3-6
3.3.4	Displaying the Root CA Certificate	3-6
3.3.5	Generating a Server Certificate (Peer Certificate)	3-7
3.3.6	Saving the SSL Server Certificate (Peer Certificate)	3-8
3.3.7	Exporting the Root CA Certificate as "X.509"	3-8
3.3.8	Importing the SSL Server Certificate [PKCS#12]	3-9
3.3.9	Checking the SSL Server Certificate	3-9
3.3.10	Importing an Exported Root CA Certificate	3-10
3.4	Setting Parameters for the SPE Security Configuration	3-11
3.5	Setting System Flags for SPE via HiPath 3000 Manager E	3-12
3.6	Configuring an optiPoint 410/420 Telephone for SPE	3-13
3.6.1	Displaying Connection Information on an IP Phone's Screen	3-13
3.6.2	Configuring a Key for Secure Status Display	3-13
3.7	DLS - SPE Certificate Deployment	3-14
3.7.1	SPE with Certificate Check	3-14
3.7.2	Checking the HG 1500 Deployment and Licensing Client Configuration	3-15
3.7.3	Displaying CA Certificates	3-16
3.7.4	Adding IP Gateways and IP Phones to the DLS	3-16
3.7.5	Adding HG 1500 to the DLS as a Virtual Device	3-17
3.7.6	Displaying 1. CA and 1. DLSC Client Certificates	3-18
3.7.7	Correcting DLS - HG 1500 Errors	3-19
3.7.8	Adding IP Phones to the DLS	3-20
3.7.9	Reading out Parameters and the Software Version of IP Phones	3-20
3.7.10	Updating IP Phones	3-21
3.7.11	Importing and Deploying SPE CA Certificates	3-21
3.7.12	Configuring optiClient 130	3-24
3.7.13	optiClient Attendant V8.0	3-24

3.7.14 "Gateway not found!" Error Message	3-24
3.8 Automatic SPE Configuration via DLS.....	3-25
3.9 SPE Secure Trace.....	3-26
3.9.1 SPE Secure Trace Certificate	3-26
3.9.2 Importing the SPE Secure Trace Certificate	3-26
3.9.3 Displaying the SPE Secure Trace Certificate	3-27
3.9.4 Starting the SPE Secure Trace	3-27
4 Networking Scenarios for HiPath 3000/5000 V8.....	4-1
4.1 Overview	4-1
4.2 Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP.....	4-2
4.2.1 Target Configuration	4-2
4.2.2 Configuring HiPath 3000/5000	4-2
4.2.3 Configuring the HG 1500 in HiPath 3000/5000.....	4-5
4.2.4 Configuring HiPath 2000 / HiPath OpenOffice EE	4-6
4.2.5 Using Signaling & Payload Encryption	4-9
4.3 Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2	4-10
4.3.1 Target Configuration	4-10
4.3.2 Prerequisites	4-10
4.3.3 Configuring HiPath 3000/5000	4-10
4.3.4 Configuring the HG 1500 in HiPath 3000/5000.....	4-13
4.3.5 Configuration of HiPath 2000 / HiPath OpenOffice EE	4-14
4.3.6 Using Signaling & Payload Encryption	4-17
4.4 Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-NQ Trunks	4-18
4.4.1 Target Configuration	4-18
4.4.2 Configuring the HiPath 3000/5000, HiPath 2000 / HiPath OpenOffice EE and HG 1500	4-18
4.4.3 Configuring the HiPath 3000/5000, HiPath 2000 / HiPath OpenOffice EE and HG 1500 for E.164	4-18
4.4.4 Configuring HiPath 3000 Node1	4-19
4.4.5 Configuring the HG 1500 in HiPath 3000 Node1	4-21
4.4.6 Configuring HiPath 2000 / HiPath OpenOffice EE Node3.....	4-22
4.5 Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Breakout to the ITSP	4-25
4.5.1 Target Configuration	4-25
4.5.2 Configuration for "Breakout" from HiPath 2000 / HiPath OpenOffice EE via HiPath 3000 to ITSP	4-25
4.5.3 Configuring the HiPath 2000 / HiPath OpenOffice EE Node3.....	4-26
4.6 Networking HiPath 3000 V9 with HiPath 3000 V9 via IP	4-27
4.6.1 Target Configuration	4-27
4.6.2 Configuring HiPath 3000 Node1	4-27
4.6.3 Configuring the HG 1500 in HiPath 3000 Node1	4-29

Contents

4.6.4	Configuring HiPath 3000 Node2.	4-30
4.7	Networking HiPath 3000 V9 with HiPath 3000 V9 via TDM	4-34
4.7.1	Target Configuration.	4-34
4.7.2	Configuring HiPath 3000 Node1.	4-34
4.7.3	Configuring HiPath 3000 Node2.	4-36
4.8	Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164	4-38
4.8.1	Target Configuration.	4-38
4.8.2	Configuring HiPath 3000 Node1.	4-38
4.8.3	Configuring the HG 1500 in HiPath 3000 Node1	4-40
4.8.4	Configuring HiPath 3000 Node2.	4-41
4.8.5	Configuring the HG 1500 in HiPath 3000 Node2	4-43
4.9	Networking HiPath 3000 V8 with HiPath 4000 V4 via IP	4-44
4.9.1	Target Configuration.	4-44
4.9.2	Configuring HiPath 3000 Node1.	4-44
4.9.3	Configuring the HG 1500 in HiPath 3000 Node1	4-46
4.10	Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2.	4-48
4.10.1	HiPath 3000 V8 Configuration	4-48
4.10.2	HiPath 4000 V5 Configuration	4-56
4.11	Networking HiPath 3000 V9 with HiPath 4000 V4 via TDM	4-57
4.11.1	Target Configuration.	4-57
4.11.2	Configuring HiPath 3000 Node1.	4-57
4.12	Networking HiPath 3000 V8 and HiPath 4000 V4 with E.164.	4-60
4.12.1	Target Configuration.	4-60
4.12.2	Configuring HiPath 3000 Node1.	4-60
4.13	Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2	4-63
4.13.1	Networking Limitations	4-64
4.13.2	Configuration of HiPath 3000	4-65
4.13.3	Configuring OpenScape Voice	4-98
4.13.4	Configuring OpenScape Branch.	4-113
4.14	Networking HiPath 3000 V9 with External Systems via ISO-QSIG or ECMA-QSIG	4-122
4.14.1	Target Configuration.	4-122
4.14.2	Configuring HiPath 3000 Node1.	4-122
4.15	Information on Configuring Networking Routes	4-125
4.15.1	ISDN Numbering Plan	4-125
4.15.2	E.164 Network	4-125
4.15.3	Configuration via Manager E	4-125
4.16	Information on the Rerouting Parameter and Path Optimization Flag	4-127
4.17	Least Cost Routing (LCR) for E.164	4-128
4.17.1	Setting up Least Cost Routing	4-129
4.18	IP Networking with SPE	4-141
4.18.1	IP Networking with SPE Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000/5000.	4-141
4.19	E.164 Connection with OpenScape Office - General Rules	4-142

4.19.1 Gateway Node (Node with direct CO access)	4-142
4.19.2 Sub node (Node without direct CO access)	4-142
4.19.3 Configuration Groups	4-143
5 Sample Configuration for Xpressions Compact	6-1
5.1 Basic Configuration of Xpressions Compact and HiPath 3000/5000	6-2
5.2 Configuring the Conference Server	6-2
5.2.1 Assigning Licenses	6-3
5.2.2 Configuring the Conference Server Number	6-3
5.3 Configuring and Opening Conference Spaces	6-5
5.3.1 Setting up a Conference Space	6-5
5.3.2 Opening a Conference Space via WBM	6-7
6 Setting Up Dual Mode Mobility Entry	7-1
6.1 Assigning a License	7-2
6.2 Setting up the SIP Station	7-2
6.3 Setting up a Basic MULAP	7-2
6.4 Setting up Mobility Entry	7-3
6.5 Configuring DISA	7-3
7 Configuring FMC Parallel Signaling with IVM	8-1
7.1 Required Components	8-2
7.2 Performing Basic Configuration	8-2
7.3 Assigning Licenses	8-2
7.4 Configuring Basic MULAP	8-2
7.5 Configuring a Mobility Mailbox	8-3
7.6 Configuring Mobility Function Numbers in Manager E	8-4
7.7 Configuring Mobility Function Numbers in WBM	8-5
7.8 Configuring a Mobility Mailbox	8-6
7.9 Configuring Call Pickup	8-7
7.9.1 Configuring a DSS Key	8-8
7.9.2 Configuring "Associated Dialing" for the Desktop Telephone	8-8
7.9.3 Configuring Call Forwarding on the Desktop Telephone	8-8
Index	Z-1

Contents

1 HiPath 3000 Manager E Service Tasks

This chapter contains a detailed description of selected service tasks required for configuring a HiPath 3000/5000 system using HiPath 3000 Manager E.

HiPath 3000 Manager E Service Tasks

Transferring CDBs (HiPath 5000 RSM/AllServe Server)

1.1 Transferring CDBs (HiPath 5000 RSM/AllServe Server)

Select **HiPath 5000 RSM/AllServe Server | Transfer... | HiPath 5000 RSM/AllServe Server** from the menu to transfer a CDB.

Reading/writing CDB data

You must have the necessary password to transfer data between the communication system and your PC.

First, as explained under Server below, determine the application server with which you want to exchange data (if this has not been done yet).

Prerequisite: When accessing from an external PC, the DCOM setting must permit this access.

1. Enter the name of the server in the combo box.
or
Select a name from the combo box if you have already used this function before.
or
Press the **Find** button.
All servers that are available in the network are listed in the **Find computer** window. Mark the server that you want and select the **OK** button. The name is added to the combo box.
2. Click the **Server > Manager** button if you want to transfer a CDB from the application server to your PC.
3. Select the **Delta mode** check box only if you have transferred a current CDB to the communication system before administering the customer data. This option ensures that only the actual changes are transferred, and by doing so, shortens transmission time.
or
Click the **Manager > Server** button if you want to transfer a CDB from your PC to the application server.
4. The **Data transmission server** window is displayed. The transfer starts now and can take several minutes, depending on the amount of data to be transferred.
5. Once the transfer is complete, confirm the procedure by selecting **Close**.

The data has been successfully transferred.

Changing the password

The password can only be changed when the PC is connected to the application server.

To change the password, proceed as follows:

1. Click the **Change password** button.
The **Change password in system** window opens.
2. Enter the old password (e.g., the default password "633423") in the **Old password** field.
3. Then enter the new password in the **New password** field and repeat it in the **Confirm new password** field.
4. Confirm the entries with the **OK** button.

The password has been changed.

A password may contain all common characters. Upper and lower case are evaluated (case-sensitive). If you use a character that is not allowed, you will receive an error message that shows the character that is not allowed.

Updating the server from the communication system

In order to access the application server's current CDB, the CDB must first be transferred from the communication system to the application server.

1. Click the **System > Server** button to transfer the CDB from the communication system to the application server.

Merging the speed dialing destinations

Select **Settings | System parameters... | Speed dialing system** to merge speed dialing destinations.

HiPath 3000 Manager E Service Tasks

Transferring CDBs (Single Communication System)

1.2 Transferring CDBs (Single Communication System)

Select **File | Transfer... | Communication** from the menu to transfer the data.

Transferring a customer database (CDB)

You must have the necessary password to transfer data between the communication system and your PC.

1. First define how the data is to be transferred between the communication system and your PC.
 - Select the **IP** option button to exchange data between your PC and the communication system in an IP-based network.
 - Select the **Direct** option if your PC is directly connected to your communication system via a serial connection cable.
 - Select the **Modem** option if you have access to your communication system via a modem. Before you can transfer a CDB, you must first set up a connection.
 - Select the **ISDN** option to exchange data between your PC and the communication system via an ISDN connection. Before you can transfer a CDB, you must first set up a connection.
2. Enter the parameters for the selected communication method.
 - If you select **IP**, enter the IP address of the communications system in the **IP address** field.
 - If you select **Modem** or **ISDN**, enter a call number to be used for setting up the connection in the **Tel. No.** field.
Then enter the code needed to enable the connection (the default is "000000") in the **PIN code** field. After you have enabled the connection, you have 30 minutes to set up the connection to the communication system.
3. Select the **Read/write database** option.
4. If you select the **Call charges** option, the call charge data at the transfer destination is overwritten with the call charge data of the CDB to be transferred.
 - The following selection determines the direction of the data transfer:
If you are starting to edit the CDB:
Click **System > PC** to transfer a CDB from the communication system to your PC.
Enable **IVM Download** to load the IVM data simultaneously.
 - If you have finished editing the CDB:
Select the **Delta mode** option only if you have transferred a current CDB from the communication system before administering the customer data. This option ensures that only the actual changes are transferred, and by doing so, shortens transmission time.
Click the **PC > System** button if you want to transfer a CDB from your PC to the communication system. After the data has been successfully transferred, the new CDB is automatically activated in the communication system.
5. Confirm logon with the **OK** button.

6. The **Transfer** window is displayed.
The transfer starts now and can take several minutes, depending on the amount of data to be transferred.
7. Once the transfer is complete, confirm the procedure by selecting **Close**.

The data has been successfully transferred.

Change password

Please change the password after the initial startup to prevent unauthorized access to the configuration of your communication system.

The password can only be changed when the PC is connected to the communication system.

To change the password, proceed as follows:

1. Select the option **Security**.
2. Click the **Change password** button.
The **Change password in system** window opens.
3. Enter the old password (e.g., the default password "633423") in the **Old password** field.
4. Then enter the new password in the **New password** field and repeat it in the **Confirm new password** field.
5. Confirm the entries with the **OK** button.

The password has been changed.

A password may contain all common characters. Upper and lower case are evaluated (case-sensitive). However, if you use a character that is not allowed, you will receive an error message that displays the invalid character.

1.3 Configuring Stations

To configure a station, go to **Stationview** and select **Settings | Set up station... | Station** from the menu.

Changing call numbers of stations

1. In the **Stationview**, go to **Station selection** and select the station with the call number you want to change.
2. Click the arrow icon after the **Call number** field to switch to the **Set up station... | Station** dialog.
3. Overwrite the existing call number with the call number that you want to use. The call number can have a maximum of 6 digits. Every call number in the communication system must be unique and can only be used once. Overlaps in the call number range cannot be implemented either, i.e., if the internal call number 20 is already being used, for example, then the call number 200 cannot be created, and vice versa "Eliminating conflicts that showed up during the check").
4. Click the **Check** button.
 - If no conflicts arise, you will see the message "No collisions found" in the status line (bottom left).
 - The Conflicts window opens if conflicts were recorded during the check. First eliminate the conflicts.
5. Confirm your changes by selecting **Apply**.

Changing an MSN for a multi-device connection (standard ISDN port) - Not for the USA

The following procedure applies only if you have a **multi-device connection** (standard ISDN port).

Your provider has assigned you MSNs. In this case, the MSNs are the CO numbers that are entered in the direct inward dialing (**DID**) column to define call allocation. The MSN is entered without the "prefix".



An MSN (**DID** column) can only be assigned to a single internal call number. If an MSN is to be signaled at multiple internal stations, a group or hunt group call number must be entered. The stations are then assigned to the **Groups/Hunt groups**.

1. In the **Stationview**, go to **Station selection** and select the station on which you want edit direct inward dialing.
2. Click the arrow icon after the **Direct inward** field to switch to the **Set up station... | Station** dialog.

3. Overwrite any existing MSN (CO numbers) with the MSN that you want to use. Make sure that you only use an MSN (CO numbers) that was assigned to you by your telecommunications provider. You will find your MSN (CO numbers) in the registration form of the telecommunications provider.
If you want to unassign the MSN, you can also delete it from the **DID** column. Please note, however, that a call to an unassigned MSN (CO numbers) will not be signaled!
4. Confirm your changes by selecting **Apply**.

Changing the DID phone number at a PCPBX system connection

The entry in the **DID** column depends on which connection type you have ordered from your telecommunications provider and on which connection type was selected (see also "Changing an MSN for a multi-device connection (standard ISDN port) - Not for the USA" above).

The following procedure applies only if you have a **PCPBX system connection** (with direct inward dialing to the internal station).

Your telecommunications provider will have assigned you a call number range that you can allocate to your stations. In this case, it would be best to use the same call numbers in the **Call no.** (call number) and **DID** (direct inward dialing) columns. This would allow the station to be reached under the same call number both internally and externally.

1. In the **Stationview**, go to **Station selection** and select the station on which you want edit direct inward dialing.
2. Click the arrow icon after the **Direct inward** field to switch to the **Set up station... | Station** dialog.
3. Overwrite any existing direct inward dialing phone number with the one that you want to use. Make sure that you only use DID phone numbers that were assigned to you by your telecommunications provider. You will find the appropriate call number range in the registration form of the telecommunications provider.
4. Click the **Check** button.
 - If no conflicts arise, you will see the message "No collisions found" in the status line (bottom left).
 - The Conflicts window opens if conflicts were recorded during the check. First eliminate the conflicts.
5. Confirm your changes by selecting **Apply**.

Eliminating conflicts that showed up during the check

The "Conflicts" window opens when you use the **Check** button to check for collisions and a collision is detected. You must eliminate all conflicts before transferring the CDB to the communication system.

Each conflict is displayed in a separate line. This is followed by the station that you edited or that created the conflict (indented).

1. If you double-click a line in the Conflicts window, the corresponding conflict (e.g., **Call no.** or **DID**) is automatically selected in the **Station** tab.
2. Edit the conflict.
For example, you may not use a station with the call number 10 if other stations already exist with the call numbers 100, 101, 102, etc.
3. Click the **Check** button.
Repeat these steps until you receive the message **No collisions found** in the status line (bottom left).
4. Confirm your changes by selecting **Apply**.

Changing names

Station names are used to improve station identification during further processing in this program; the text is also displayed on the display of the connected system telephones.

1. In the **Stationview**, go to **Station selection** and select the station with name you want to change.
2. Enter the station name in the **Name** field (on the right). Use a maximum of 16 alphanumeric characters, including special characters.
3. Confirm your changes by selecting **Apply**.

Changing parameters/flags

In the **Stationview**, you can use the tabs (Flag status, Activated features, etc.) to display and modify additional parameters. In the **Flag status** tab, you can apply tabs that you defined for one station to other stations.


1.4 Programming and Labeling Keys

To program keys, go to **Stationview** and select **Settings | Set up station... | Key programming**.

Perform the following two steps to label and program keys:

1. In the **Stationview**, go to **Station selection** and select the station with the key programming you want to modify.
2. Switch to **Systemview** and select **Set up station... | Key programming**. The user's telephone is displayed. Stations that have not yet logged on at the time of the transfer are identified with an asterisk "*".


Key programming

1. Select the option **Key programming**.
2. Click one of the telephone's label fields to the left of the keys (in the pictorial display of the telephone) to select a key.
The current key code is displayed in the **Current assignment** field.
3. Select the new function from the **Key code** drop-down list. The additional information needed for the chosen function is queried in the other fields.
4. Click the button with the red check mark  to enter the new function and to move on to the next key.
5. Confirm your changes by selecting **Apply**.



If you have programmed a key with the **Level switchover** function, you can double-program each additional key by selecting the **Level 2** option. To do this, repeat the steps for key programming.

Changing key labeling

1. Select the **Label** option.
2. Click one of the telephone's label fields to the left of the keys (in the pictorial display of the telephone or key module) to select a key. The current key text is displayed in the **Current assignment** field.
3. Enter the new text for the label in **Key text**.
4. Click the button with the red check mark  to enter the new key text and to move on to the next key.
5. Confirm your changes by selecting **Apply**.

Printing a label sheet


1. Select the **Label** option.
2. You also have the option of using a customized font:
Click the **Font...** button.
The font window is opened.
 - The **Font** lists contains all the fonts that are installed on your operating system. Select one of them.
 - You can also define the **Font style**, **Size** and **Script**. A sample text is displayed in the **Sample** field.
 - Your settings are accepted after you press the **OK** button.
3. Click the **Print...** button. This opens a dialog in which you can select the ports (stations) to be printed.
4. In the **Print** column, select the ports for which the key label should be printed.
5. In the **BLF / EKL** column, select the ports for which an additional key label should be printed for the key modules you have added.
6. Select the **All stations** option if you want the key label to be printed for all ports.
7. Select the option **Print on printed form?** if you want a key label to be printed on standard paper without frames.
8. Start the printing process by selecting **OK**.



You will find additional information on ordering and using label sheets in the documentation for your telephone.

Adding a key extension unit

You can add key extension units (for example, key extension units with 16 keys).

1. Add a key extension unit with the symbol button .
2. The following query appears: **Do you want to add a key extension unit?**
If you want to add a key extension unit, confirm this question by selecting **Yes**.


You can now use the  button to switch between the added key extension units and the system telephone.



To program and label the keys on your key extension unit, proceed as described for your system telephone.


Deleting a key extension unit


The key extension unit added last is always deleted first.

1. Delete the last key extension added with the icon button .
2. The following query appears: **Do you want to remove a key extension unit?**
If you want to delete the key extension unit, confirm this question by selecting Yes.

Adding a busy lamp field


You can add busy lamp fields.

1. Add a key extension unit with the symbol button .
2. The following query appears: **Do you want to add a key extension unit?**
Answer this question by selecting **No**.
3. The following query appears: **Do you want to add a busy lamp field?**
If you want to add a busy lamp field, confirm this question by selecting Yes.

You can now use this icon button  to switch between the additional busy lamp fields and the system telephone.

Deleting a busy lamp field

The busy lamp field added last is always deleted first.

1. Use the icon button  to delete the most recently added busy lamp field.
2. The following query appears: **Do you want to remove a busy lamp field?**
If you want to delete the busy lamp field, confirm this question by selecting Yes.

1.5 Configuring IP Clients

This section provides information on the configuration of IP-based terminals. Every IP client is assigned a corresponding station number (while also indicating the HG 1500 card at which the client should be logged on). Before configuring the IP clients, ensure that the client licenses are correctly enabled.

To configure IP clients, go to **Stationview** and select **Settings | Set up station...** followed by the **Gatekeeper** tab.

1. In the **Stationview**, go to **Station selection** and select the station (IP client).
2. Click the arrow icon after the **Call number** field to switch to the **Set up station... | Station** dialog.
3. Enter the call number (Call no.), the direct inward dialing phone number (DID) and the name, and apply the settings.
4. Select **Settings | Set up station...** from the menu followed by the **Gatekeeper** tab.
5. Select the IP station from the **Stations** list.
6. Under **Selected station...**, select whether a **System Client** (optiPoint, optiClient) or an **SIP Client** should be configured, and click the **setup** button. Apply the settings.
7. Switch to **Stationview**.
8. Switch to the **WorkPoint Client** tab and specify the parameters. **SIP stations** do not need a unique **IP address**. Apply the settings. The **Analog adapter connected** parameter ensures that H.323 calls are routed via a DSP (digital signal processor) and that features are activated in the system.

H.323 clients are not supported in HiPath 3000 from V9.

1.6 Configuring Call Pickup

The members of a call pickup group can easily answer calls for other members. Calls to one telephone in the call pickup group are signaled optically and, after a timeout, acoustically at all other telephones in the group. Any telephone can then pick up the call. The call pickup can be executed via a programmed key or a code at the telephone.

Select **Settings | Incoming calls... | Call pickup** to configure call pickup.

Allocating stations to a call pickup group

1. Select a group from the **Call pickup group**.
2. In the **Selection** list, click the station that you want to allocate.
3. Click the > button to transfer the station to the **Members** list and simultaneously allocate it to the call pickup group.
4. Confirm your changes by selecting **Apply**.

Cancelling allocation to a call pickup group

1. In the **Call pickup group** list, select the group whose allocation to a station you want to cancel.
2. In the **Members** list, click the station with the allocation you want to cancel.
3. Click the <- button to remove the station from the **Members** list and the call pickup group.
4. Confirm your changes by selecting **Apply**.

1.7 Configuring Call Forwarding

Call forwarding (CFW) can be used if the station does not respond to a call within a given time (this time can be set). The call is then automatically forwarded to the call forwarding destination that has been entered. Calls can be forwarded to stations, hunt groups or via a system search.

Select **Settings | Incoming calls... | Call forwarding** to configure call forwarding.

Configuring / modifying a call destination list

Call forwarding allows you to set up different **call destination lists**. **Call destination lists** determine how incoming calls are processed.

1. The current configuration of call destination lists is displayed in the **Call dest. list - Definition** table. You can use the drop-down lists in each column to change the current definition. Click the **arrow icon** to open a drop-down list.
2. The **Target 1** column is always the currently selected station. A star * is therefore displayed in this column. Target 1 cannot be changed in Manager C.
3. In the **Target 2** list, select the first station to which calls are forwarded. Enter only stations that actually exist. # stands for a system search through all stations.
4. Where necessary, you can also select additional stations in the **Target 3** and **Target 4** columns, in the same way as described for the **Target 2** column.
5. The **Cycles** column defines the time of the call forwarding. (Default setting 3 x 5 seconds = 15 seconds.)
6. Confirm your changes by selecting **Apply**.

External call forwarding destinations

Proceed as follows to forward calls to a satellite PABX system or the public network:

1. In the **Target 2**, **Target 3** or **Target 4** columns, select the "External destination" entry. An **External destinations** window is opened. Here, you can enter an external number in the **Call no.** field.
2. Confirm the changes in the **External destinations** window by selecting **OK**.
3. Confirm your changes by selecting **Apply**.

Searching for unassigned call destination lists

Proceed as follows to search for an unassigned call destination list:

1. Select the option "Show members of call dest. list <n>". The members and stations allocated to the list you selected are displayed in the **Call dest. list - Station assignment** table.
2. In the **Call dest. list - Definition** table, consecutively select the call destination lists.
3. If no members or stations are displayed in the **Call dest. list - Station assignment** table, the call destination list is not assigned.

Assigning a call destination list to a station

Every station can be assigned a call destination list. Different entries can be made for internal (day or night) and external calls. Day, night and external service is set via a programmable key at the telephone or via a code.

1. Select the **Show all stations** option. Current call destination assignments are displayed in the **Call dest. list - Station assignment** table (default setting for all stations is: call destination list 14 for Day, 15 for Night, 16 for Internal).
2. You can use the drop-down lists **Day**, **Night** and **Internal** to assign different call destination lists to the stations.
3. Open the drop-down list by clicking the **arrow symbol**.
4. Select the number for the call destination list. More than one station can use the same call destination list.
5. Confirm your changes by selecting **Apply**.

1.8 Configuring Groups/Hunt Groups

A group/hunt group is a set of several stations that can be reached at one call number. This call number can be a code or the call number of the first station in the hunt group (master hunt group). A group hunt group is typically used when a call is to be signaled simultaneously at multiple stations. The stations can activate or deactivate the hunt group via a program key or a code for the hunt group.

Select **Settings | Incoming calls... | Groups/Hunt groups** to configure hunt groups.

Allocating a station to a hunt group

1. In the **Group** table, select the group you want assign the station to.
2. In the **Call no.** column, enter the group call number to be used for contacting the group.
3. In the **Selection** list, click the station you want to allocate to the group you selected.
4. Click the > button to add this station to the **Members** list.
5. Confirm your changes by selecting **Apply**.

The station is now entered as a member in the hunt group.

Cancelling allocation to a hunt group

1. In the **Group** table, select the group whose allocation to a station you want to cancel.
2. In the **Members** list, click the station with the allocation you want to cancel.
3. Click the <- button. The allocation for this station is canceled.
4. Confirm your changes by selecting **Apply**.

Setting up external destinations

1. Select the **External dest...** button.
2. Use the **Previous group** or **Next group** button to select the group/hunt group that you want.
3. Select the external route in the **Route** drop-down list. If available, you can also select a route in a satellite PABX system.
4. Enter the required call number in the **Call no.** entry field. Use a maximum of 6 digits for seizure and 25 digits of dialing information.
5. Confirm your changes with the **Setup** button.
6. The call number is added to the **Members** list.
7. The window closes when you press the **Close** button.

1.9 Loading IVM Data

Select **File | Transfer... | Communication** from the menu to transfer the data.

Loading IVM data

IVM data can be loaded from the communication system to the PC (**System > PC**) or from the PC to the communication system (**PC > system**).

- To load IVM data from the communication system to the PC:
 1. Select the **Read/write database** option.
 2. Enable the **IVM Download** option and click the **System > PC** button.
- To load IVM data from the PC to the communication system:
 1. Select the **Read/write database** option.
 2. Enable the **IVM Upload** option and click the **PC > system** button.

1.10 Configuring IVM - Music On Hold (MOH)

The configuration steps must be performed in sequence.

1. Ensure that the ports you want to use for music on hold are not entered in the IVM hunt group (**Incoming calls... | Groups/Hunt groups**).
Recommendation: Use the first or last six IVM ports for music on hold. The first six IVM ports are used in this example.
2. Select **Settings | Auxiliary Equipment... | Ext. connection | External MOH**. Enter the IVM ports that you want to configure as music on hold (one to six ports) in the respective field for ITR groups 1 - 6 (drag and drop).
The IVM port you entered is now responsible for a specific ITR group (for instance, port 140 for ITR 1, port 141 for ITR 2, etc.).
The MOH assigned to the first ITR group is enabled for calls that cannot be assigned to an ITR group (UCD, for instance).
3. Check that the IVM ports are also identified as music-on-hold ports (**Stationview | Activated features | Extension Type**).
4. If the ports are identified correctly (in this example 140 - 145), select **Auxiliary Equipment... | IVM** and set them up as mailboxes with COS (class of service) 17.
5. Transfer the customer database to the communication system (**File | Transfer...**). The data is transferred to the IVM. During this process, the green LED goes out, the orange LED flashes for approximately five seconds and green LED goes back on again. The data transfer is now complete.
Note: All connections currently established with IVM ports are cleared down during data transfer.

If a call is made to a station in ITR group 1, for instance, and the station puts the calling party on hold, the calling party hears the music-on-hold announcement assigned to ITR group 1. If a call is made to a station in ITR group 2, for instance, and the station puts the calling party on hold, the calling party hears the music-on-hold announcement assigned to ITR group 2, and so on.

Note: "Lets get together" is set as the default announcement in the IVM.

1.10.1 Changing Music-on-hold Announcements

There are two ways of changing music-on-hold announcements assigned to a port.

- Via the TUI
- Via **HiPath 3000 Manager**

Changing via TUI:

1. Call the IVM hunt group from an extension that does not have a mailbox.
2. Enter the code (default code: 1234).
3. Enter the mailbox number for the music-on-hold port (music-on-hold port 140, ITR 1, for instance).
4. Use the menu to change music-on-hold announcements 1 to 4.

Changing via HiPath 3000 Manager:

1. Select **File | Transfer... | Maintenance | IVM**. Since the volume of data to be transferred is very large, select access via **IP - IVM** (access in the IVM must be released for this).
2. Select the **Execute file operations** button.
3. Select the **Greetings** option.
4. Once the drop-down list with the mailboxes is released, select the music-on-hold port with the announcement you want to change.
Note: Once you have selected the port, data transfer may take a long time, although the status display may not change.
5. Select the greetings files. The files must be available in a valid WAV format (refer to the IVM manual, where necessary).
6. Select the **PC > IMV Delta** button to transfer the files you have selected to the IVM.

1.10.2 Playback Sequence of Entries 1-4 on a Music-on-hold Port

"Lets get together" is played as the default setting for the IVM. Changing the announcements (greetings) on an music-on-hold port, modifies the playback sequence for the announcements. Note: An announcement is immediately activated once you change it.

1. No announcement is changed
 - a) "Lets get together" is played
2. Announcement 1 is changed
 - b) Announcement 1 is played continuously
3. Announcements 1 and 2 are changed
 - c) Alternation between announcement 1 and 2
4. Announcements 1, 2 and 3 are changed
 - d) Alternation between announcements 1, 2 and 3

Sequence when announcement 4 is changed or activated

The fourth announcement on an IVM music-on-hold port is a special announcement. Once the fourth announcement is changed (and therefore activated), announcement 4 is always prior to announcements 1, 2 and 3 when the system switches between these three announcements.

Announcement 4 can be used, for instance, to advertise a customer's weekly offers between the individual announcements. This ensures that the calling party hears the offers between the music.

1. Announcements 1 and 4 are changed
 - a) Alternation between announcement 1 and 4
2. Announcements 1, 2 and 4 are changed
 - b) Alternation between announcements 1, 4, 2 and 4
3. Announcements 1, 2, 3 and 4 are changed
 - c) Alternation between announcements 1, 4, 2, 4, 3 and 4

1.11 Configuring IVM Announcements

The configuration steps must be performed in sequence.

1. Ensure that the ports you want to use for music on hold are not entered in the IVM hunt group (**Incoming calls... | Groups/Hunt groups**).
Recommendation: Use the first or last six IVM ports for music on hold. The first two IVM ports are used in this example.
2. Select **Auxiliary Equipment... | Announcement | Announcement equipment** to allocate the IVM ports you want to configure as announcements to the announcement device. The type of announcement can be defined as an individual announcement (**Announcement**) or a continuous announcement (**Music On Hold**).
The IVM port you entered is now responsible for a specific announcement device (port 140 for announcement device 1 and port 141 for announcement device 2, for instance).
3. Once the IVM ports (in this example 140 and 141) are assigned to the announcement devices, select **Auxiliary Equipment... | IVM** and set up the configured ports as mailboxes with COS 17.
4. Transfer the customer database to the communication system (**File | Transfer...**). The data is transferred to the IVM. During this process, the green LED goes out, the orange LED flashes for approximately five seconds and green LED goes back on again. The data transfer is now complete.
Note: All connections currently established with IVM ports are cleared down during data transfer.
5. Change the announcements as described in Section 1.10.1, "Changing Music-on-hold Announcements", on page 1-19.
6. Configure, for example, **Announcement prior to answer** for the lines (**Auxiliary Equipment... | Announcement | Announcement prior to answer**).

Alternatively, assign an announcement device to the UCD groups, for example (**Incoming calls... | UCD groups | Group parameters**).



The internal MoH (MoH = Music on Hold) cannot be configured as the first UCD announcement (index 1). This setting can result in problems in scenarios involving IP network connections.

1.12 Configuring Classes of Service

The class of service feature comprises three steps:

- **Stations** is used to assign stations for day and for night to the service groups 1 to 15.
- Assign class of service for **Day** and class of service for **Night** to the individual class of service groups, each with a class of service range from 1 to 14. The class of service codes cover the entire range from heavily restricted to absolutely unrestricted access. Each group is assigned an individual class of service for day and night service.
- Generate lists with the allowed and denied call numbers (**Allowed/Denied numbers**). These lists are referred to by Class of service groups 1 through 15.



The steps mentioned above do not have to be executed in the order listed. You may prefer to compile your lists or define your groups before you assign your stations to groups. These functions are highly interactive. You should draw up an appropriate plan before doing the programming.

Select **Settings | Classes of service...** to configure classes of service.

Assigning/changing class of service groups

Class of service groups are assigned to stations on the **COS: Station** tab. The assignment is achieved by selecting a **COS group** (1 to 15) in the table.

A **COS group** can be assigned to a single, multiple, or even all stations (**Call No.**).

The selection that you make in the **Day** column will refer to the **Day** tab, where the COS Group is linked to the actual Class of service. The selection that you make in the **Night** column will refer to the **Night** tab, where the COS Group is linked to the actual Class of service.

The call number of the station is displayed in the **Call Number** column.

The name of the station is displayed in the **Name** column.

1. In the **Day** column, select the cell for the relevant **Call no.**
2. A drop-down list is now displayed in the **Class of service** cell. Click the arrow symbol.
3. The **Class of service** drop-down list is opened. Use the left mouse button to select a class of service group.
You can choose among **COS group 1** to **COS group 15**. At the same time, even more groups can be set up because each of the class of service groups 1 to 15 can also be defined differently for day and night operation.
4. Confirm your changes by selecting **Apply**.
5. Repeat this process in the **Night** column.

Changing the COS group for day/night

1. Switch to the **Day** or **Night** tab.
2. In the **Selection** list, select a class of service group (**COS group 1** to **COS group 15**).
3. The current settings of the selected class of service group are now displayed.
4. In the table, click the row "Trk Grp 1" in the "Class of service" column.
5. A drop-down list is now displayed in the **Class of service** cell. Click the arrow symbol. You may need to change the column width or use the horizontal scroll bar to make the arrow symbol visible.
6. The drop-down list is opened. Use the left mouse button to select a class of service.
7. Confirm your changes by selecting **Apply**.



Class of service group 1 to Class of service group 15 can each have different **classes of service** for the **Route** in the **Day** and **Night** tab.

Editing the allowed list

1. Switch to the **Allowed/Denied numbers** tab. On the left-hand side, you can create tables with call numbers that may be dialed by the station.
2. Select a list from the **List no.** drop-down list.
You can create a maximum of six such lists. Your first list can have up to one hundred entries, and the remaining five lists can have a maximum of ten numbers.
3. Select the **Input** entry field and enter the digit sequence that the station should be allowed to call.
The separate numbers can be entered with digits (0 to 9) and the * and # characters. The complete telephone number does not need to be listed. To permit users to dial 0800 numbers, for example, just enter 0800. See "Notes and examples for the allowed list" below.
4. The allowed call number is added to the list when you select the **New** button.
5. Confirm your changes by selecting **Apply**.

HiPath 3000 Manager E Service Tasks

Configuring Classes of Service

Notes and examples for the allowed list

Stations with this class of service are generally never allowed to dial external call numbers. A station with this class of service may only call the numbers and other digit sequences contained in the Allowed list. The allowed call numbers are entered without the trunk seizure code (0).

Examples for the Allowed list:

- To create a class of service for a local area where only the emergency services may be dialed, the list must contain the following digits:
110 / 112 (and possibly other call numbers for the medical service, etc.)
- To create a class of service for a local area where only the all call numbers in the local area may be dialed, the list must contain the following digits:
1 / 2 / 3 / 4 / 5 / 6 / 7 / 8 / 9
- To create a class of service for the regional area, the list must contain all local area codes from the regional area:
089 / 08141 / 08151 / etc.
- To create a class of service that only permits national dialing, you will need to create a list with all possible national prefixes:
02 / 03 / 04 / 05 / 06 / 07 / 08 / 09
- To create a class of service that allows dialing to a specific country, enter the country code for that country:
0039

The options indicated above can, of course, also be combined in a list. Furthermore, it would not make sense to authorize a station for national dialing without allowing that station to make calls in the local area.

Digit sequences that specify a call number in detailed format also do not need to be entered. If the entry 08 exists in the list, for example, further area codes such as 089, 08141, etc., do not need to be entered.

Depending on the effort involved, it may be more practical to assign a Denied list to the stations instead, especially if the dialing of only a few call numbers is to be prohibited.

Editing the denied list

1. Switch to the **Allowed/Denied numbers** tab. A maximum of six tables with call numbers that the station cannot dial can be created in the right half of the screen.
2. Select a list from the **List no.** drop-down list.
You can create a maximum of six such lists. Your first list can have up to fifty entries, while the remaining five lists can have a maximum of ten each.

3. Select the **Input** entry field and enter the digit sequence that is denied to the station.
A # sign at the start of the denied list ensures that the terminal toll restriction is not applied where an analog CO line is to be seized using DTMF signaling, or switched to DTMF during dialing.
Numbers can contain up to seven digits, which can include the numbers 0 through 9 and the symbols * and #. The complete telephone number does not need to be listed. For example, to prohibit stations from dialing charge-per-minute 0190 numbers, you would enter 0190 here.
See "Notes and examples for the denied list" below.
4. The denied call number is added to the list when you select the **New** button.
5. Confirm your changes by selecting **Apply**.

Notes and examples for the denied list

Stations with this class of service can basically dial all external numbers except for the call numbers and other digit sequences specified in the list. The prohibited call numbers are entered without the trunk seizure code (0). Examples for the Denied list:

- If you want to create a Denied list with a certain call number, the call number should be entered as in the example below if the station is located in the own local area:
72233427 / 08972233427 / 00498972233427
The digit sequences above all refer to the same call number. If the entry is created with all (possible) prefixes and area codes, it will not be possible to bypass the toll restriction for system telephones by adding an additional prefix.
- The following entries are needed to create a Denied list for 0190 numbers:
0190 / 0049190
- If the station is to be restricted to calling only within the local area, only the following digits need to be entered in the list:
0
Stations with this class of service are rejected immediately as soon as they try to dial a prefix starting with 0 after the trunk seizure. A further entry with 00 is therefore redundant. Entering 0 in the Denied list will also prevent access to the mobile radio network (even if the station or mobile phone happens to be in the local area).
- If the station is to be restricted to the local area, but should also be allowed access to the mobile radio network with the prefixes 0171, 0172, 0173 and 0174, you can use the following entries:
02 / 03 / 04 / 05 / 06 / 07 / 08 / 09 / 011 / 012 / 013 / 014 / 015 / 016 / 018 / 019 / 0175 /
0176 / 0177 / 0178 / 0179 / 0170
00492 / 00493 / 00494 / 00495 / 00496 / 00497 / 00498 / 00499 / 004911 / 004912 / 004913
/ 004914 / 004915 / 004916 / 004918 / 004919 / 0049175 / 0049176 / 0049177 / 0049178
/ 0049179 / 0049170

HiPath 3000 Manager E Service Tasks

Configuring Classes of Service

Digit sequences that specify a call number in detailed format also do not need to be entered. If the entry 01 exists in the list, for example, further prefixes such as 0172, 0174, 0190, etc., do not need to be entered.

Depending on the effort involved, it may be more practical to assign an Allowed list to the stations instead, especially if the dialing of only a few call numbers is to be allowed.

Deleting table entries in Allowed/Denied lists

1. Click the number in the list. The selected number is then displayed in the **Input** entry field.
2. Then click the **Delete** button.
3. As a result, the number is deleted from the list.
4. Confirm your changes by selecting **Apply**.

Changing table entries in Allowed/Denied lists

1. Click the number in the list. The selected number is then displayed in the **Input** entry field.
2. In the **Input** entry field, overwrite the old number with the new number.
3. Click the **Change** button.
4. Confirm your changes by selecting **Apply**.

1.13 Configuring Call Detail Recording

Select **System status | Call charges...** from the menu to configure call detail recording.

Deleting call charges

The call charges per station and per line can be recorded. To delete the call charges:

1. Switch to the **Output format** tab.
2. In the **CDR at station** or **CDR per line** list, select the **Call no.** of the station or the line code (**Code**) for which the call charges are to be deleted. You can select multiple codes by marking several rows or also select all stations/codes by clicking the table header.
3. Click the **Delete** button.

Exporting call charges

The call charges can also be exported for further processing. The tables differ in the way the call charges are totaled.

1. Switch to the **Output format** tab.
2. Click the **Export** button.
3. Select a folder in the dialog window and enter a designation in the **File name** input field. The **File type** (*.CSV) is assigned automatically.
4. Press the **Save** button.

The CSV file is saved in the selected folder.

The data is now available as a list with separators (CSV) and can be further processed, e.g. with Microsoft® Excel.

Example of a CSV file:

```
11;Sabine;0.00
12;Birgit;2.04
13;Wilhelm;0.00
14;Stefan;0.00
```

Defining call charge factors per route

Here you can define and change factors that display call charges as monetary amounts for analysis purposes (in the **Output format** tab) and on system telephones with displays. The accrued counting pulses are multiplied by the factors (price per counting pulse).

1. Switch to the **Factors** tab.
2. Select a cell in the **Multiplier** column. An entry field is then displayed for this cell.

HiPath 3000 Manager E Service Tasks

Configuring Call Detail Recording

3. In the **Multiplier** column, enter the factor to be multiplied with the accrued counting pulses.
4. Confirm your changes by selecting **Apply**.

Depending on the configuration, it may be necessary to adjust the ISDN unit in the communication system to the ISDN unit of the ISDN trunk of the network.

Do this by entering a factor that should be multiplied with the accrued counting pulses of the IDN trunk in the **Multi-ISDN** column for every route Trk Grp. 1

The ISDN unit supplied by the network depends on the network provider.

To define the currency, enter a currency text with up three characters (EUR, for instance) in the **Currency** field.

To define the computing accuracy, select the accuracy to be used when calculating the displayed call charges in the **Computing accuracy** field.

Defining account codes

On the telephone, you can assign the call charges to particular processes or projects. This is done by entering an account code before or even during a chargeable call.

1. Switch to the **Account codes** tab.

Using the account code that appears when printing out the CDB, you can then appropriately assign the chargeable calls.

2. Defining the checking procedure
 - Select the **No check** option if you want the user to be able to enter account codes even if they are not defined in the **Account code lists**. If an account code that is not present in the list is entered, it is added to the list. This is not possible for mandatory input.
 - Select the **List check** option. In this case, the entered account code is compared with the entries in the **Account code lists**. If the entered account code is not present, the connection cannot be set up.
 - Select the **Check number of characters** option if you want an entered account code to match the specification only with respect to the number of characters.
To do this, select a number of characters between 1 and a maximum of 11 characters from the **Characters to be checked** drop-down list.

3. Defining entry procedure

- In the "Entry procedure" table, click the **Procedure** cell for Trk Grp 1.
A drop-down list appears in the cell. Click the arrow symbol to open the drop-down list.
- Select an entry procedure:

Optional (default)

Telephone users can enter an account code at any telephone before the call starts (in other words before a trunk is seized). During a call, an account code may only be entered at system telephones.

Mandatory

Telephone users must enter an account code before the call starts (before a route is seized). The account code is then checked in accordance with the checking procedure you programmed.

The entry of an account code is optional for incoming calls.

4. Defining account code lists/account codes

You can define up to 1000 different account codes. In addition, an **Account code** can be assigned to each **List** (0 to 999).

Click a cell from the **Account code** column in the **Account code lists** table.

You can now enter an account code (max. 11 characters) in the cell.

5. Confirm your changes by selecting **Apply**.

The "Check" button can be used to check if the entries have been accepted by the communication system.

1.14 Configuring System Parameters

Select **Settings | System parameters...** from the menu to configure system parameters.

Defining the key click volume

You can enable the "Key click" function if you want every keystroke on the dialing keypad to be acoustically signaled on your system telephones.

1. Switch to the **System settings** tab.
2. Select one of the four volumes (**1**=quiet, **4**=loud) in the **Volume** drop-down list. The key-stroke is not signaled if you select **Off**.
3. Confirm your changes by selecting **Apply**.

Defining port assignment for the call detail recording



Go to **Call charges...** and "Output format" to assign ports for call detail recording.

You have the option of supplementing a system telephone with a UPN adapter (data or control adapter with RS 232 interface). This adapter makes it possible to output call detail data, for example, to a printer or PC with call charge evaluation.

1. Open the Output format drop-down list.
Select **UPN**.
2. Open the **UPN port** drop-down list.
Select the station that has a system telephone with a UPN adapter.
3. Open the **CDR at station** drop-down list.
Select the station for which the call detail output for call detail recording per station (CDR at station) should be done.
Select **none** if no output should be made.
4. Open the **CDR per line** drop-down list.
Select the station for which the call detail output for call detail recording per line (CDR per line) should be done.
Select **none** if no output should be made.
5. Confirm your changes by selecting **Apply**.



Only experienced users should carry out the port assignment for call detail recording. If you have any questions, please contact your authorized service personnel.

Defining speed dialing system destinations



The entry of **speed dialing** numbers that are already in the table is detected and not accepted.
Speed dialing destinations (**call numbers** and **names**) that are entered without speed dialing numbers are ignored.

1. Switch to the **Speed dialing system** tab.
2. Click a free cell in the **Speed dialing** column.
3. Enter any three-digit speed dialing number from the available range in the input field. You can determine how many speed dialing numbers are available from the numbering of the rows in the table. Since the first speed dialing number begins with 000, the last speed dialing number that can be entered would be 299 if the rows are numbered till 300.
4. Change to the **Call no.** column in this same line.
5. Enter the required destination's call number in the entry field. Use a maximum of 6 digits for seizure and 25 digits of dialing information. For external destinations, enter the external code (trunk group code) in front of the call number for the assignment. This external code was defined by the authorized service personnel.
 - The external code may be "0", for example, or a line code:
81 for route 1
82 for route 2, etc.
 - Entering # causes the following digits to be transmitted as DTMF tones (tone dialing).
 - Entering **P** produces a dial pause when transmitting the call number. This may be required after the external code, for example. If the length of the pause is too short, the pause can also be entered more than once (**PP**). The default setting is P=2 seconds.
6. Change to the **Name** column in this same line.
7. Assign any name in the **Name** column. This name is then displayed in the system telephone's display depending on the situation, for example, when dialing via the speed-dialing number. Use a maximum of 16 alphanumeric characters, including special characters.
8. Confirm your changes by selecting **Apply**.



If the call number is transferred by a caller and this is identical to the call number in the speed-dialing memory, the name assigned to the number is displayed when a call is made to the system telephone.

Changing info and answer texts

1. Switch to the **Texts** tab.
2. Select an entry field for the info or answer texts.
3. Overwrite or add to the existing text. A maximum of 24 characters are allowed in each entry field.
For answer texts:
If the user on a system telephone wants to add to the predefined text, enter a colon followed by an empty space. The user can then add text, e.g. a room number.
4. Confirm your changes by selecting **Apply**.

Resetting to standard texts



All text that you have customized is overwritten and reset to the default values.

1. Switch to the **Texts** tab.
2. Select the language that you want, e.g., **English**, in the **Reset** drop-down list.
3. Confirm your changes by selecting **Apply**.

Setting the start and end of daylight saving time

You can use the **Daylight saving time** tab to define the day and month that daylight saving time begins and ends. The time is valid throughout the system and is shown on system telephone displays, for example.

The switchover is made twice a year, at either 2:00 am or 3:00 am on the defined date. You can save each of the switchover times for a period of 10 years. The total possible time period begins in 1990 and ends in 2088.

1. Switch to the **Daylight saving time** tab.
2. If the year to be edited is not listed in the table, then first enter the first year in a ten year range in the **Starting Year** input field; this range must include the year to be edited (from 1990 to 2079).
Enter the four-digit year.
3. Click the **Apply** button.
The year you wanted is now listed in the table.
4. In the Begins column, click the cell that you want to change.
5. An entry field opens in the cell. Enter a new day and month (in the format **DD.MM.**) when the switchover should occur (e.g. **03.03.**).
6. In the End column, click the cell that you want to change.
7. An entry field opens in the cell. Enter a new day and month when the switchover should occur (e.g. **03.03.**).
8. Confirm your changes by selecting **Apply**.

1.15 APS Transfer

To perform the transfer, proceed as follows:

1. Select **File | Open customer database**
2. Select the file extension ***.fst** from the File type field.
3. Select the folder that contains fst file.
4. Selecting and opening the FST file
5. Select **File | Transfer**
6. Select Modem or ISDN
7. Enter the station number
8. Select **APS transfer** An additional window appears at the top right of the screen. Use this window to specify the time to activate the new APS.



If the **APS transfer** field has a gray background, the fst file was not opened correctly.

9. APS transfer can now begin.
The transfer time may vary depending on the communication system. Generally speaking, it will take from 30 to 40 minutes using a B-channel modem. When an analog modem is used, the transfer times are over an hour. With an V.24 connection at 9600 baud for example, transmission takes about 2.5 hours. With an ISDN modem via IMOD, transfer takes about an hour.
10. Once APS transfer is complete, the message **APS transfer successfully completed** is displayed. A system reset is now performed, and the communication system reboots with the new APS either immediately or after the time entered. The communication system deletes the old APS after rebooting. The delete operation takes approximately seven minutes. You can check whether the new APS is activated via **HiPath 3000 Manager**.
11. During an upgrade from V6 ((V6.0 -> V7, V7 -> V8)) with HiPath 3000/5000, the APS can be transferred with the attached, converted CDB.



When the APS is transferred to a system in a different time zone, the APS is switched at the time specified in the remote communication system.

1.16 Swapping/Replacing Languages

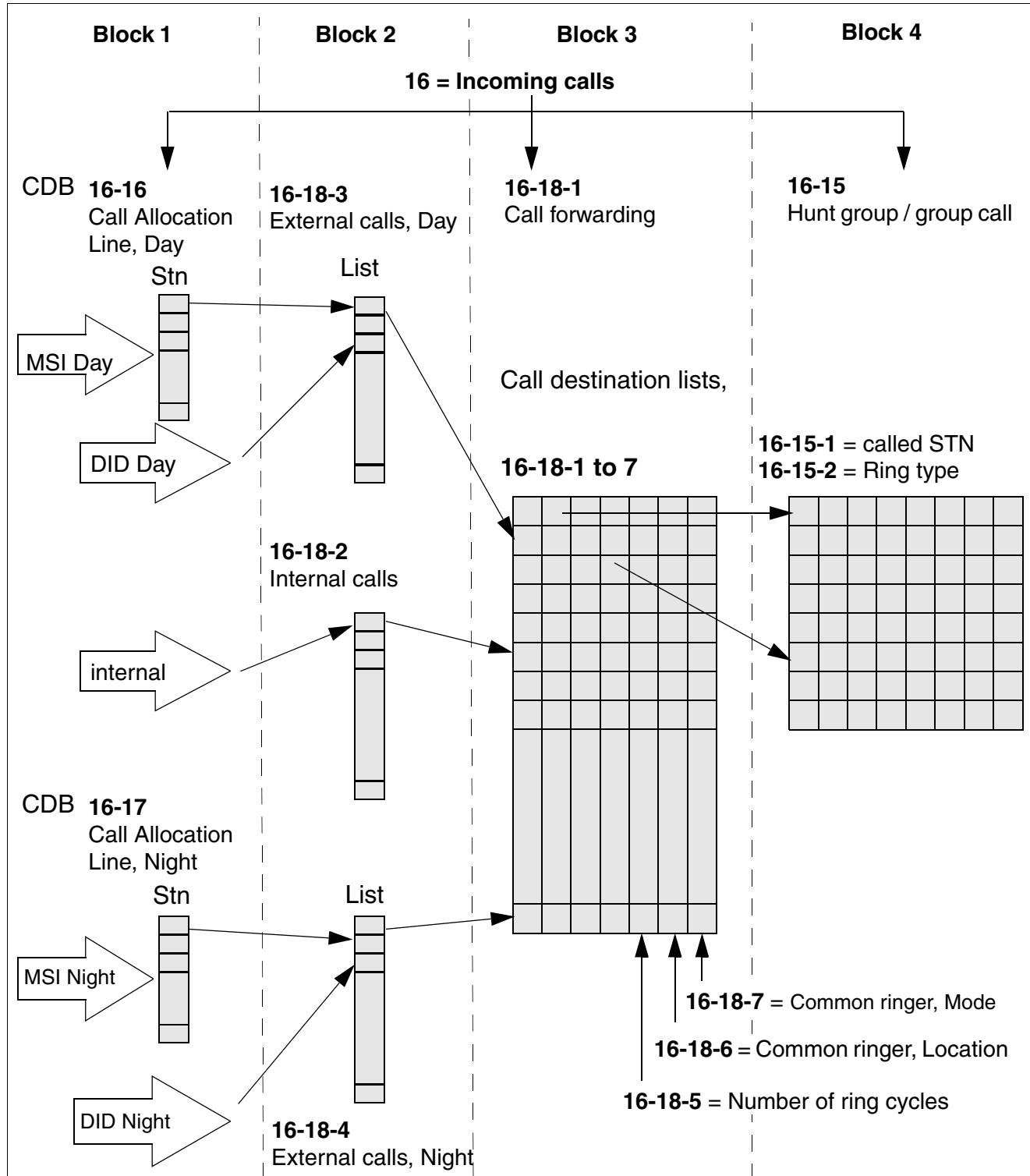
The default languages loaded can be replaced by other languages (overwritten). The languages can be combined as appropriate.

To change the language, proceed as follows:

1. **Select** File | Open customer database.
2. Select the file extension *.lng from the File type field
3. Select the **Lng** folder (below the **HiPath 3000 Manager** installation folder).
4. Select and open the relevant language file ("`<version>_<smr>.lng`").
5. **Select** File | Transfer **and switch to the** Loadable texts tab.
6. In the **variable** selection list boxes, select the four languages that you want (four (or two) variable languages must always be selected).
7. **Apply** the settings.
8. Switch to the **Communication** tab.
9. Select the desired transfer path (**Access**).
10. Activate the **Transfer texts** option and start the transfer with the **Transfer texts** button.
11. The communication system is automatically reset after the completion of the transfer, after which the new languages are available.

1.17 Incoming Calls that Display Company Names

Overview of Call Management



Prerequisites

- An unassigned station must be available if you want to assign a station name (where possible, choose a station that is not available as hardware).
- This station must be configured as an "Answer Machine" extension type.
- To be able to forward the station name, the station must be assigned a free index with "*" as its first entry in Call Management. The second entry contains the call number of the station to be called for the station name specified (this entry may also be a group).

Example

- Direct inward dialing phone number 250 is assigned, for example, to the company "Siemens".
- However, optically and acoustically, the station with call number 200 is called.

Programming via HiPath 3000 Manager

Step	Action
1.	Configure the extension type: Stationview > Activated features
2.	Enter name: Stationview - Station parameters
3.	Enter call destination: Settings > Incoming calls... > Call dest. list Settings > Incoming calls... > Allocation int./ext. calls

HiPath 3000 Manager E Service Tasks

Announcement Prior to Answer (on an Analog Port)

1.18 Announcement Prior to Answer (on an Analog Port)

The announcement prior to answer function is often configured to relieve an intercept position. An answer machine that can accept incoming calls and forward them to a specific station is connected for this purpose.

This function is configured via Call Management.



The station ports to which an answer machine is connected must be configured as answer machines.

Example

- An answer machine must be connected to a hunt group with the call number 450 (stations 224 and 225).
- All incoming external calls should first be answered by the answer machine.

Programming via HiPath 3000 Manager

Step	Action
1.	Settings > Incoming calls... > Groups/Hunt group
2.	Settings > System parameters... > Intercept / Attendant
3.	Stationview > Activated features

1.19 Configuring an Internal S₀ Bus with Multiple Stations

Introduction

Every S₀ bus can support up to eight terminals or devices. To do this, one or more system ports must be configured for a Euro bus.

Example

Port 4 is configured for a Euro bus.

Programming via HiPath 3000 Manager

Step	Action
1.	Settings > Lines / networking... > Trunks
2.	Dial port 4 by double-clicking the corresponding table row in the "Param" table column.
3.	Click the "ISDN flags" tab.
4.	Select and apply "S0:Euro bus" from the drop-down list.

Note

Observe the following when initiating an internal S₀ bus:

- Up to 64 MSNs can be logged on to every bus. The MSNs must be entered in the CDB's internal call number plan and must not be assigned to other terminals. 63 MSNs can be entered at any point in the CDB. When enabling 64 MSNs, one of these must correspond to the default MSN of this S₀ port.

S ₀ port	Default MSN
1	Internal call number of the last port equipment number
2	Internal call number of the last-but-one port equipment number
...	...

- Configure an additional S₀ bus if more than 64 MSNs are required. This bus should be set up in the same way as the first S₀ bus.
- MSN numbers must be assigned for each device or terminal on the Euro bus. If no MSNs are assigned for the devices, the port default is used as the MSN for all devices. In other words, if you dial this default MSN, the call is signaled on all devices connected to the bus.
- MSN configuration on the device is dependent on the device.

1.20 Remote Service via ISDN

Introduction

Remote service via ISDN can be used to read out CDB content, make any necessary modifications and import it back into the communication system.

There are three options available for performing remote service via ISDN:

1. Release procedure
2. Logon without code
3. Logon with code

Example

Release procedure: The release procedure is the default option entered in the system for remote service. The customer simply has to change the release code. (Default code: 000000).

Example

Logon without code: Data can be loaded to and from the system at any time without entering a code.

Programming via HiPath 3000 Manager

Step	Action
1.	File > Transfer... > Callback connection
The tool cannot be used to configure the remote service code.	

Example

Logon with code: Data can be loaded to and from the system at any time, once the six-digit code has been entered in the tool (code can be changed by the customer).

Programming via HiPath 3000 Manager

Step	Action
1.	File > Transfer... > Callback connection
The tool cannot be used to configure the remote service code.	

Example

Changing the code

Example

- Changing the direct inward dialing phone number for remote service.
- Configuring the external direct inward dialing phone number.

1.21 Universal Call Distribution (UCD)

Introduction

Universal call distribution can be released throughout the system using **HiPath 3000 Manager**.

Note

We recommend that you only release universal call distribution once all other UCD parameters are programmed.

Call distribution examples

Group assignment (31 1)

- UCD groups are configured.
- UCD group 1 is assigned to the Purchasing department and has the IDs 100 and 101. UCD group 2 is assigned to the Sales department and has the IDs 110 and 111.

Announcement equipment (25)

- If announcement equipment is required for the UCD groups, the announcement devices and types are specified here.
- A "greeting announcement" can be deployed via the "Announcement prior to answer" feature and is not a typical element of universal call distribution.

Group parameters - Wait dest. (31 2 1)

Wait destinations are assigned to the announcement devices that were previously configured.

Group parameters - Wait time (31 2 2)

- Every wait destination comprises wait times (a total of seven per UCD group) (1-20).
- Default wait time entry: 1 = 30s, Maximum entry: 20 = 6 min.
- Note: Times should not be programmed for announcements.

Group parameters - Call cycles (31 2 3)

- Call cycles are specified in the group parameters.
- This parameter is split into primary and secondary call cycles as well as the call cycle in Call Management.
- The call cycles in Call Management are modified accordingly.

Group parameters - Automatic call acceptance (31 2 4)

- This parameter specifies whether or not "Automatic call acceptance" is permitted per UCD group.
- If "Automatic call acceptance" is configured, the communication system automatically identifies whether a headset is connected to the system telephone and reacts accordingly.



If a headset is connected to the system telephone, the "Disconnect" function should be programmed on a key.

Group parameters - Queued calls (31 2 5)

- This parameter specifies how many incoming calls may be placed in a queue when a UCD group is busy.
- Once the maximum value is reached, Call Management overflow is initiated.

Wrap-up time (31 3)

- Wrap-up time can be specified for the entire system. This parameter specifies that an agent still requires time to process the last call.
- Automatic wrap-up time is not configured by default on a system-wide basis.
- This value can be set to: 0 = no wrap-up time or 1 = 5s to 45 = 45s.

External call priority (31 4)

- A request priority can be assigned for each trunk.
- 1 represents high priority whereas value 10 represents low priority.

Internal call priority (31 5)

- Internal calls can be assigned a system-wide priority. If this priority is higher than one of the trunks, internal calls have precedence.

Call distribution is now fully configured. However, to ensure that this feature functions correctly, trunk assignment and call allocation must be configured in Call Management. (Rufzuordnung = Ringing assignment in Manager tool)

1.22 Configuring Attendants

Introduction

One station or group must be configured as an attendant (intercept position) in the communication system.

Example

- Station 12 is going to be configured as an attendant. Station 13 is the attendant for fixed night service.
- Intercept for direct inward dialing should be deployed if calls are not answered, if the called station is busy and if an invalid or incomplete number has been dialed.
- 0 (default value) should be entered as the call number for contacting the intercept position externally. 91 should be used internally.
- If more than two calls are queued at the attendant, the system should switch to station 13.
- "Speed extending" and "Extend undialed lines" should be activated for the attendant.

Programming via HiPath 3000 Manager

Step	Action
1.	Settings > System parameters... > Intercept / Attendant
2.	Settings > Incoming calls... > Call forwarding > Call dest. list
3.	Settings > Incoming calls... > Ringing assignment per line

Note

The "Disconnect key" (Release call), "Call key" or "Trunk group key" should still be programmed on the attendant.

1.23 Configuring Mobility Entry (not the U.S.)



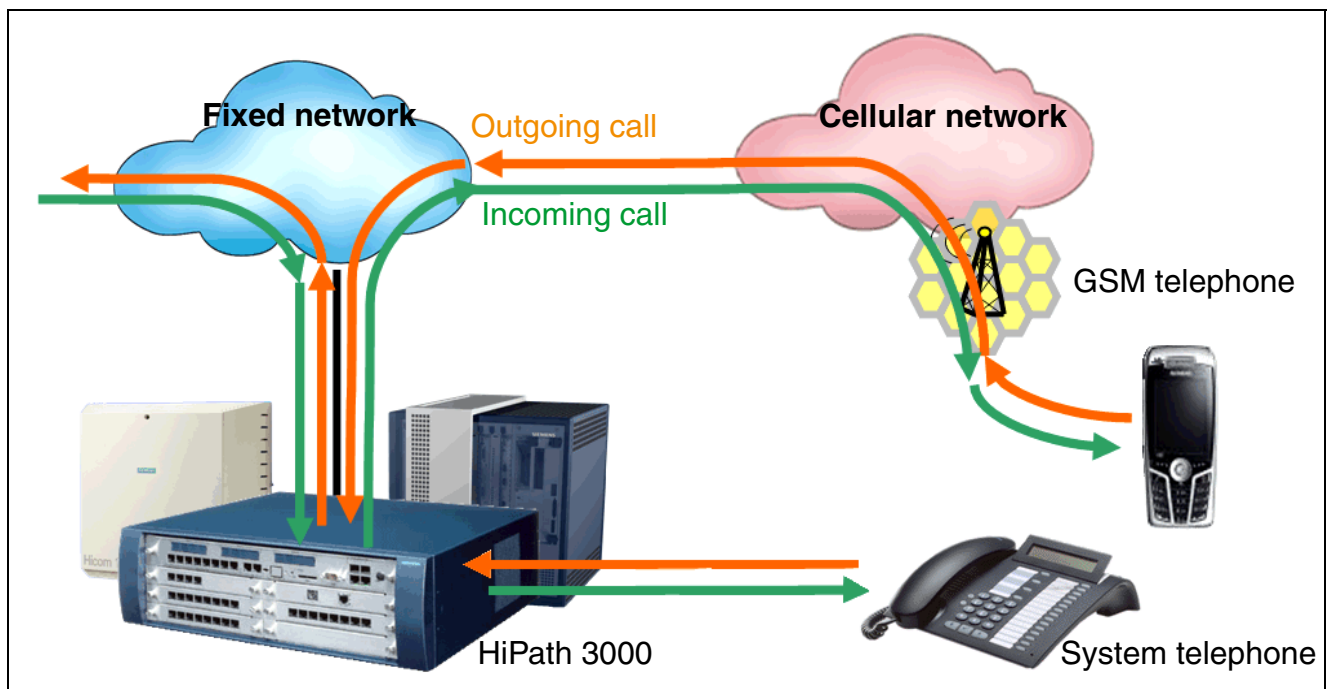
Important: Mobility Entry is not supported behind SIP provider interfaces or in IP networks. Therefore, the "Callback" function is not supported either. Mobility Entry is only enabled for the node to which the CO is connected.

Example

The example configured in this section should operate as follows:

- One Number Service: A subscriber is identified externally and internally by extension number 31. The subscriber uses a stationary system telephone with the extension number 17 in addition to a GSM telephone with a separate mobile station number. Incoming calls should be signaled concurrently at the system telephone and the GSM telephone (twinning).
- Outgoing calls from the stationary system telephone and the GSM telephone should be signaled internally and externally with extension number 31. The CLIP feature is needed for external signaling.
- System features should be accessible via the GSM telephone. DISA should be used for dial-in and the DISA DID number should be 55.
- Busy status should be visible on the GSM telephone.
- Call detail recording should occur in the system for the GSM telephone.

Graphic overview



HiPath 3000 Manager E Service Tasks

Configuring Mobility Entry (not the U.S.)

Call number allocation

A virtual phone number (e.g. extension 27) must be additionally assigned to each stationary phone number (e.g. extension 17). This virtual phone number is internally linked with the mobile phone number. The mobile phone number is generally the phone number of a GSM telephone. A land line phone number is also possible, such as when a home office is being set up. There must be a flatrate plan for the fixed network to avoid charges to the employee. A CMI mobile unit is not permitted.

Procedure

Proceed as follows to configure this example:

1. Configure a virtual station: Open HiPath 3000 Manager E and select **Stationview | Flag status**. Configure a virtual station for call number 27. The stationary station with call number 17 already exists:

The DISA class of service is not required by Mobile Connection stations.

The station with call number 27 is a virtual station.

Click "Apply".

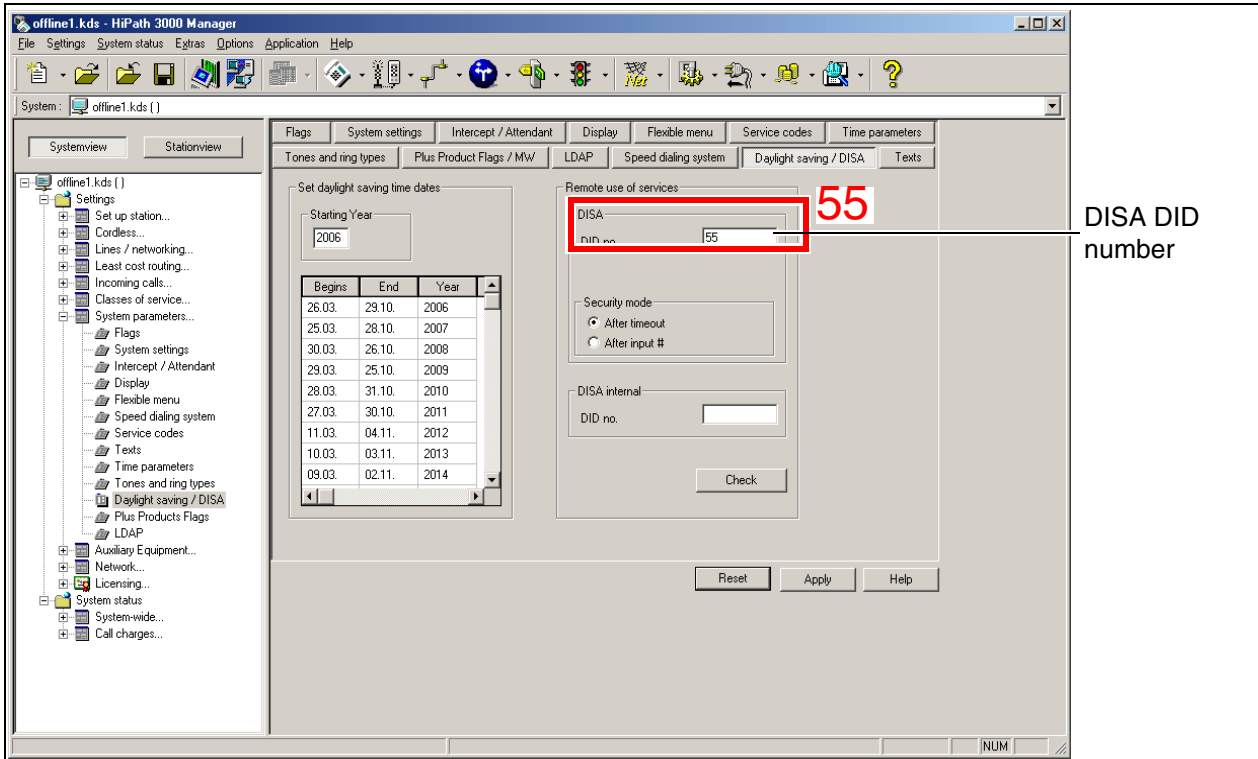
Setting information:

The "DISA class of service" flag must be disabled for the virtual station and the "Virtual station" flag enabled.

HiPath 3000 Manager E Service Tasks

Configuring Mobility Entry (not the U.S.)

3. DISA administration for dialing into the system: Select **Settings | System parameters | Daylight saving / DISA**. Enter 55 as the DID number under "Remote use of services" > "DISA" > "DID no."



DISA DID number

Click "Apply".

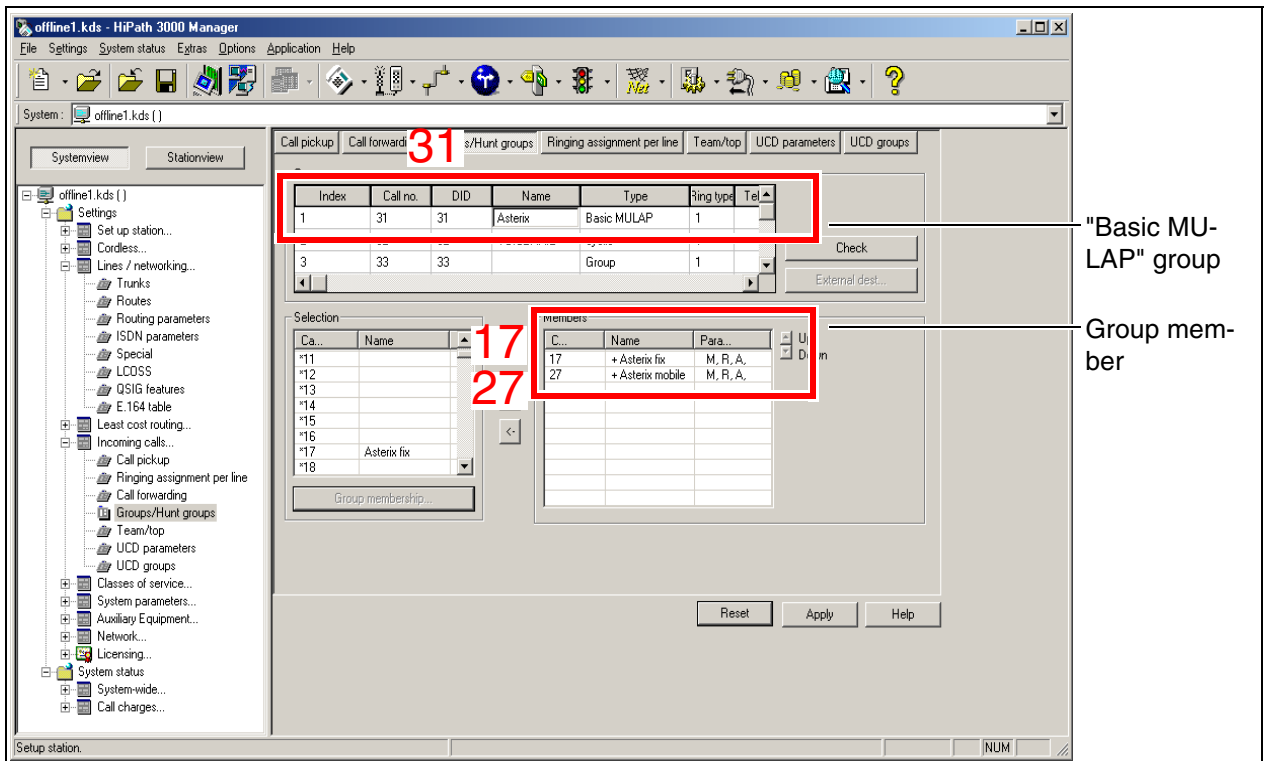
Setting information:

Security mode settings are not relevant for Mobile Connection because the mobile station is authenticated via CLIP.

4. Perform group configuration for the basic MULAP: Select **Settings | Incoming calls | Groups/Hunt groups**.

You must configure a basic MULAP group if you want incoming calls to be signaled at the stationary system telephone and the GSM telephone at the same time. This group should be assigned call number 31 and contain stations 17 and 27.

1. Enter the call number (31), DID number (31), and the group name in the "Group" table and specify the type as "Basic MULAP".
2. Select station 27 in the "Selection" table and transfer it to the "Members" table. This makes this station the "master" (identified by "+"). This ensures the MULAP's CLIP is used.
3. Select station 17 in the "Selection" table and transfer it to the "Members" table.



Click "Apply".

Setting information:

To add a second mobile station (home workstation, for instance), add a third entry to the "Members" table.

HiPath 3000 Manager E Service Tasks

Configuring Mobility Entry (not the U.S.)

5. Transfer the GSM telephone's dialing information to the system and evaluate it:

The GSM telephone operates like a system telephone when transferring dialed digits to the system. That is, it uses DTMF to transfer the digits one by one to the system for evaluation. The following types of numbers can be dialed:

- Internal system call numbers (extension 100, for instance)
- External call numbers with leading **CO code** (for example, 0089722xxx)
- External call numbers with leading **CO code** and `country code` (for example, 00043xxx)

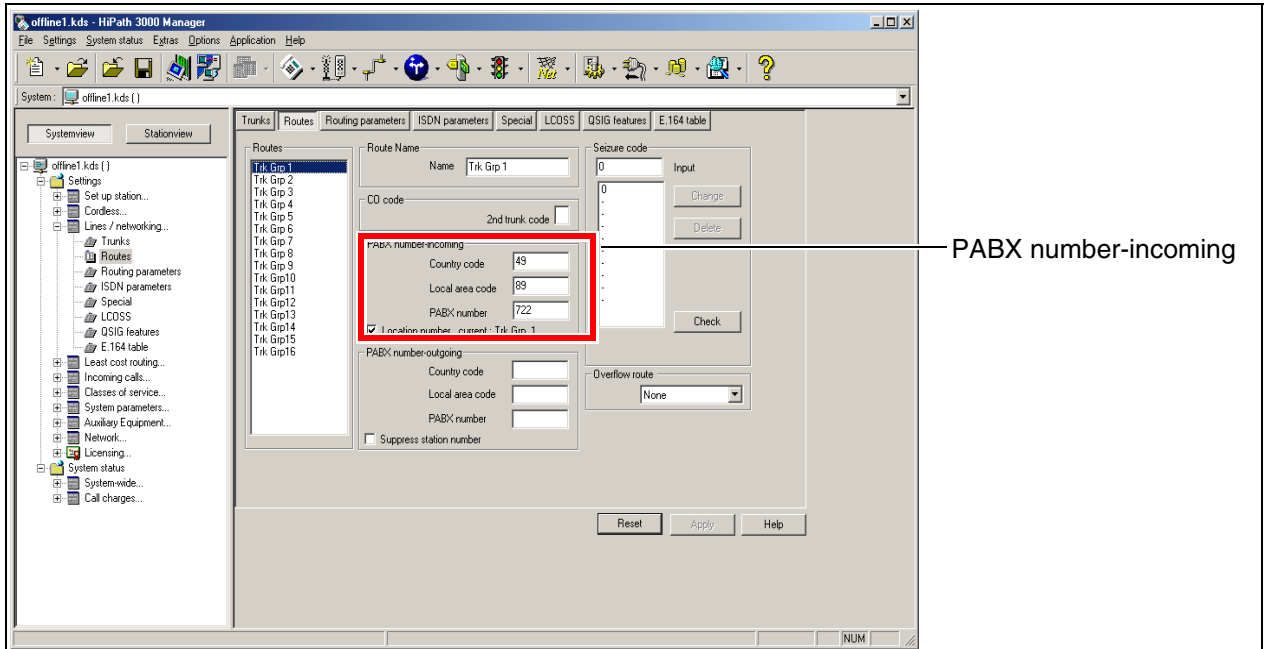
Call numbers can be stored in canonical and non-canonical format in the GSM telephone's phonebook. The formats are handled as follows when dialing:

- Canonical format (+49 89 722xxx): The mobility client transforms the call number to the format specified above by removing the "+" and adding the administratable CO code (0) as well as the country code (00), producing the number 00049 89 722xxx. We therefore recommend storing all phonebook entries in canonical format when using the mobility client.

If the destination is an internal call number, the call stays in the system. This is determined by checking if the first part of the call number matches the "PABX number-incoming" and can therefore be replaced (see below). This only works if the E.164 numbering scheme flag is enabled (see below).

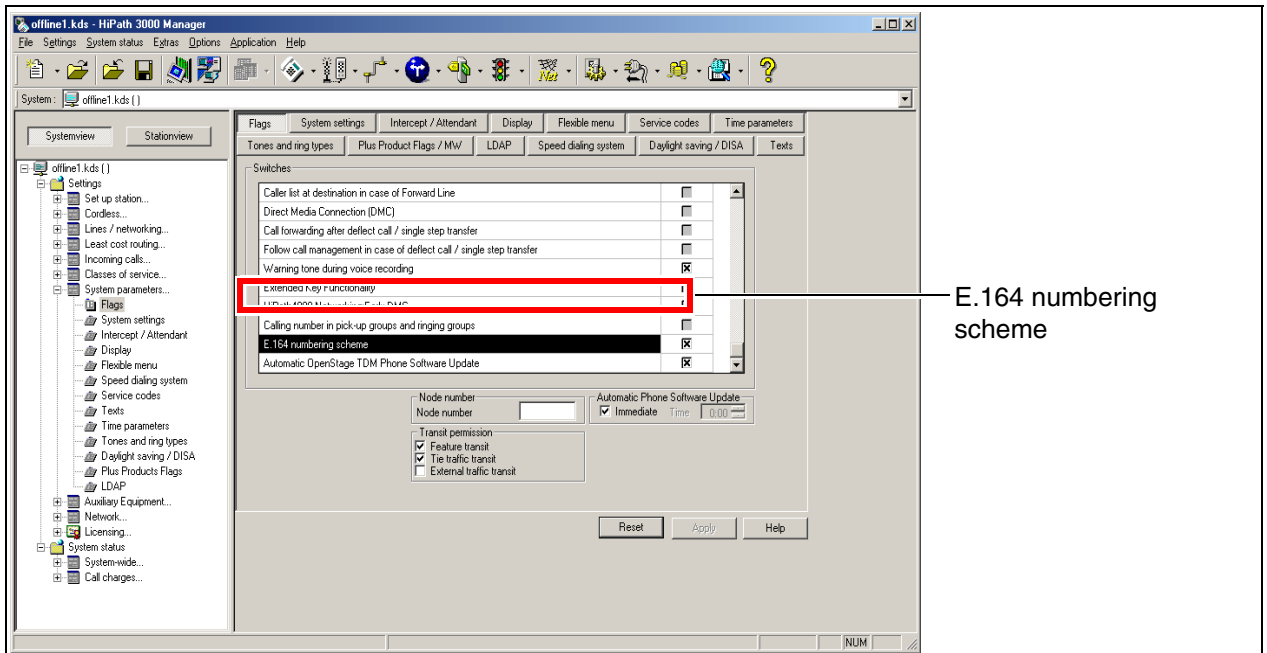
- Non-canonical format (if the mobility client is not used): All call numbers are entered in the GSM phonebook as shown above.
The disadvantage of this format is that duplicate entries may be needed for the same destination station because:
 - If you want to reach the destination station directly from the cellular radio network, you must omit the leading CO code when dialing (089722xxx, for instance).
 - If you want to reach the destination station from the system, you must include the leading CO code when dialing (0089722xxx, for instance).

1. Administer "PABX number-incoming": Select **Settings | Lines/networking | Routes**. Enter the country code, the local area code, and the PABX number of your system under "PABX number-incoming".



Click "Apply".

2. Enable E.164 numbering: Select **Settings | System parameters | Flags**. Enable the "E.164 numbering scheme" flag.



Click "Apply".

HiPath 3000 Manager E Service Tasks

Configuring Mobility Entry (not the U.S.)

Caller number display on GSM phones

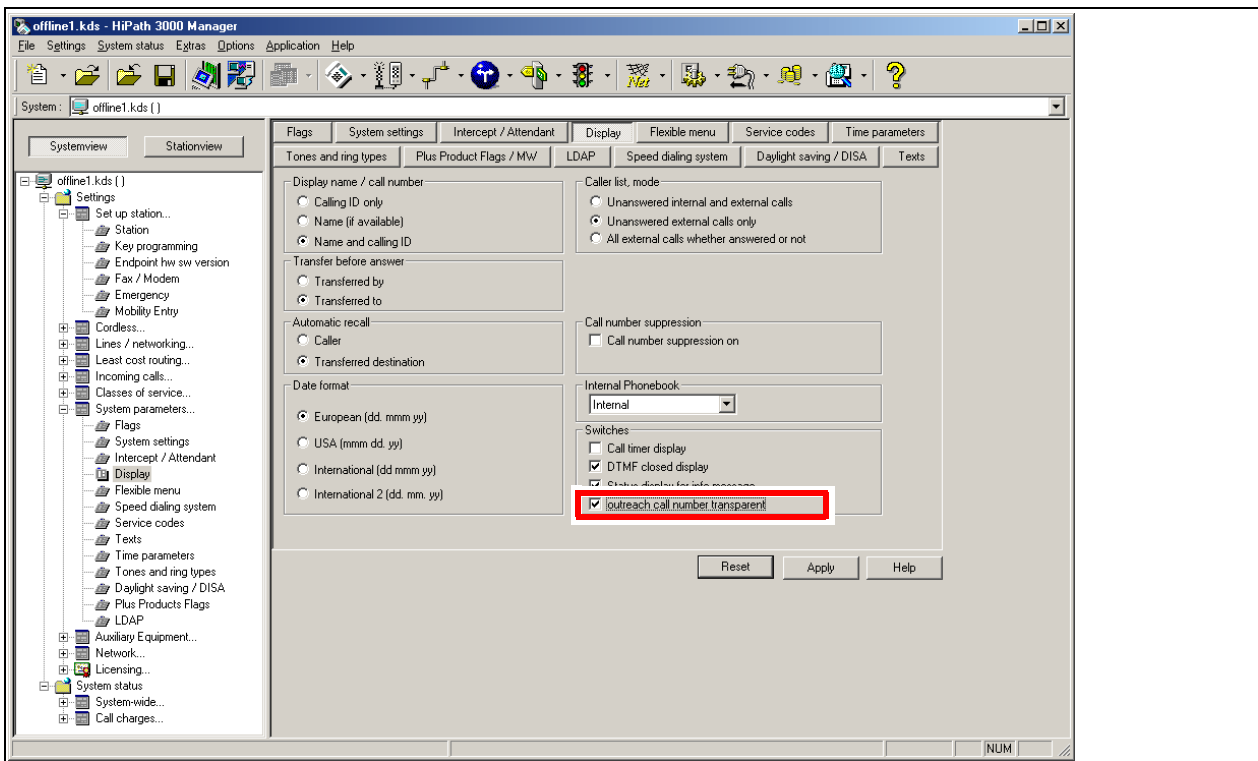
To display the caller number on a mobile subscriber's GSM telephone

- the "outreach call number transparent" flag must be set in the system,
- the "CLIP no screening" parameter must be configured for the provider,
- the ISP must put a caller's number through without verification.

Procedure

Proceed as follows to configure this example:

1. To activate station number display: Select **Settings | System parameters | Display**. Activate the flag "outreach call number transparent".



Click "Apply".

Least Cost Routing configuration and activation

For Mobility Entry, the Least Cost Routing has to be set completely and then activated to reach an external GSM telephone (mobile call number), which is mapped to a virtual station, if an incoming call appears.

The procedure to configure the Least Cost Routing is exemplified in Section 4.17, "Least Cost Routing (LCR) for E.164" .

Additional information

For detailed information about the "Mobile Connection" feature, refer to the [HiPath 3000/5000 feature description](#) .

1.24 Loading Logos for OpenStage Telephones

From V7 R3, HiPath 3000 supports the download of logos in the OpenStage 40, OpenStage 60, and OpenStage 80 telephones of the TDM connection variant.

The prerequisite is that the logo(s) to be loaded is/are available in the system.

The download of logos in the OpenStage telephones of the Cornet-IP connection variant is possible via the local administration menu of a telephone, via the WBM of a telephone, or via the central deployment and licensing service (if available).

1.24.1 Transfer of the Logo Files to the System

Before the download of logos in the OpenStage telephones (TDM connection variant), the corresponding logo files must be provided in the system. The following logo files can be transferred:

- OpenStage 40 T logo

Here, the logo file of a customer specific logo can be selected for the OpenStage 40 telephone and then transferred to the system. The following file specifications must be taken into consideration:

- Size of image: 144 x 32 pixels
- Color: Monochrome
- Format: BMP (Windows bitmap file)
- Maximum size: 702 bytes

- OpenStage 60/80 T logo

Here, the logo file of a customer specific logo can be selected for the OpenStage 60 and OpenStage 80 telephones and then transferred to the system. The following file specifications must be taken into consideration:

- Size of image: 240 x 70 pixels
- Color: Color
- Format: PNG (Portable Network Graphics) or JPG
- Maximum size: 5 - 30 KB

- **Default logo**

Here, the logo file with the 15 default logos for the OpenStage 40, OpenStage 60, and OpenStage 80 telephones can be selected and then transferred to the system. At present, the following default logos are available: Siemens, Deutsche Telekom. Additional company logos are in preparation.

The currently available logo default file can be downloaded via the software download server through which the system software is also provided. The file is labeled with **logoX.X.X.X.bin** (example: **logo1.2.3.4.bin** = logo default file of Version V1R2.3.4).

Note: The version of the logo default file currently present in the system is listed in the last line of the log file for the OpenStage software distribution. The query is possible via **Maintenance | OpenStage Phones: Software Distribution > Log File**.

To transfer the logo files proceed as follows:

1. Select **File | Transfer: Software Transfer**.
2. Go to **OpenStage 40 T Logo** and/or **OpenStage 60/80 T Logo** and/or **Default Logo** and select the desire log files.
3. Confirm your selection by selecting **Apply**.
4. Perform an APS transfer (see Section 1.15, "APS Transfer") to transfer the logo files to the system.

1.24.2 Download of the Logos in the OpenStage Telephones

To download the logos in the OpenStage telephones, proceed as follows:

1. Transfer the CDB to the service-PC (System -> PC) (see Section 1.2, "Transferring CDBs (Single Communication System)").
2. Select **Settings | System parameters | System settings**.
3. Go to **OpenStage Logo** and select the logo you want. The following options are available:

OpenStage logo	Description	Note
No logo download	No logo download to the OpenStage telephones takes place. All telephones keep the existing logo.	Through this system status, the operation of OpenStage telephones with various logos in one system is possible. Example: One part of the OpenStage telephones of a system should be loaded with Logo A, the other with Logo B. First, the customer-specific Logo A is transferred to the system and loaded in all OpenStage telephones. After that, all telephones for which Logo A is planned are disconnected from the system. Next, Logo B is transferred to the system and loaded into the remaining connected telephones. To prevent a future overwriting of the logos, the "No logo download" setting must then be selected. The telephones with Logo A are reconnected with the system again.
Empty logo	An empty logo is loaded into the OpenStage telephones.	Through this setting, for example, an incorrect logo can be overwritten.
Customer logo	The customer-specific logo in the system is loaded in the OpenStage telephones.	If no customer logo is available in the system, an empty logo is transferred.
Siemens	The Siemens logo is loaded in the OpenStage telephones (part of the logo default file).	If no Siemens logo is available in the system, an empty logo is transferred.

OpenStage logo	Description	Note
Deutsche Telekom	The Deutsche Telekom logo is loaded in the OpenStage telephones (part of the logo default file).	If no Deutsche Telekom logo is available in the system, an empty logo is transferred.
Logo 3	The third logo is loaded in the OpenStage telephones (part of the logo default file).	This deals with preliminary services for future default logos. At present, these logos are empty.
Logo 4	The fourth logo is loaded in the OpenStage telephones (part of the logo default file).	
...		
Logo 15	The fifteenth logo is loaded in the OpenStage telephones (part of the logo default file).	

4. Confirm your selection by selecting **Apply**.
5. Transfer the CDB to the system (PC -> system) (system -> PC) (see Section 1.2, "Transferring CDBs (Single Communication System)").

HiPath 3000 Manager E Service Tasks
Loading Logos for OpenStage Telephones

2 Practical Examples for HG 1500

This chapter describes scenarios with typical, practical configurations. The application scenarios are displayed and the configuration steps are described. In the practical examples, WBM is used for configuration.

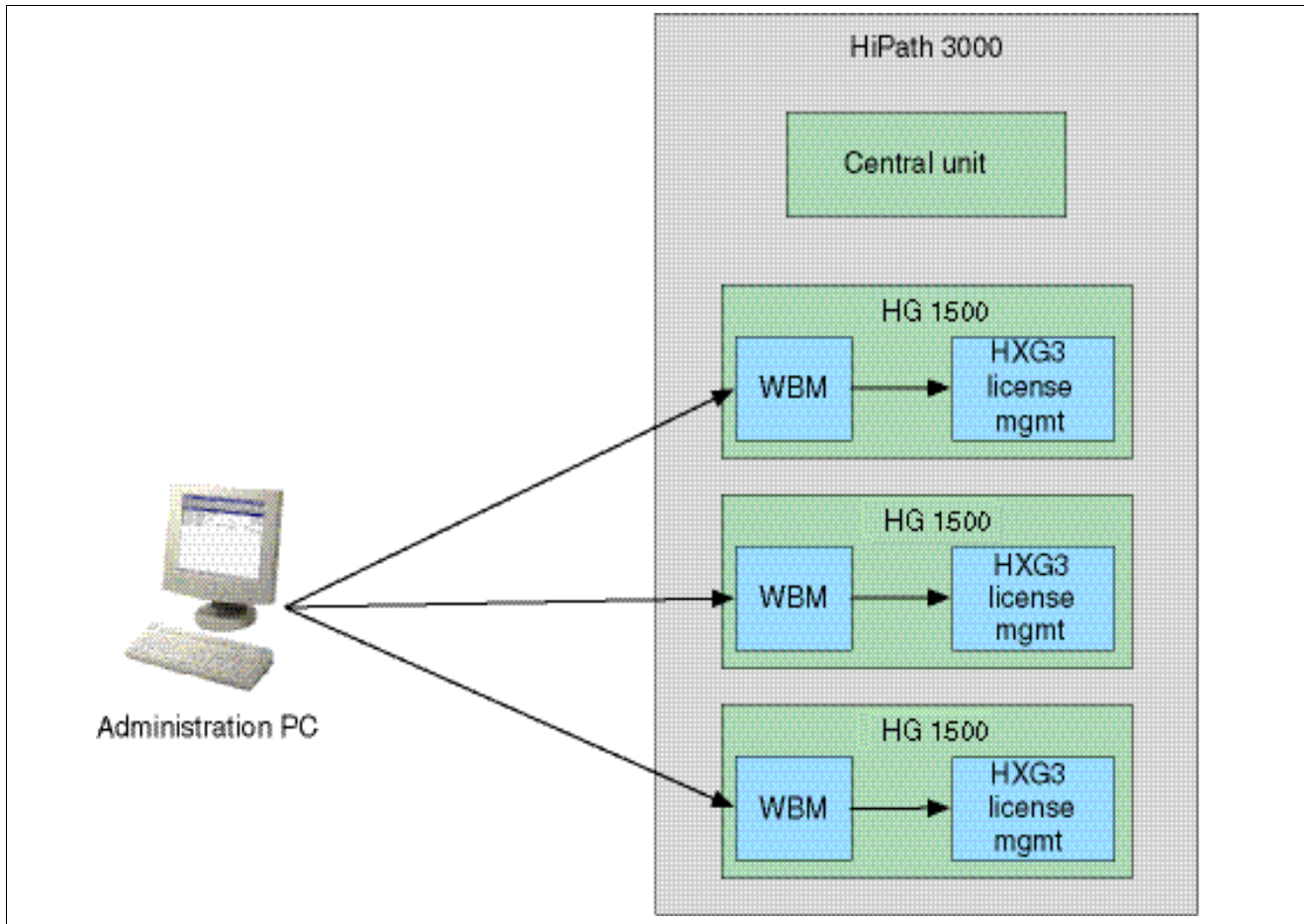


HG 1500 must have already been configured under Basic Settings. Please note that write access must be enabled before you can add, edit or delete configuration data in WBM. This is not explicitly indicated in the individual examples.

2.1 License Management

2.1.1 Target Configuration

With this configuration, you can administer licenses for HG 1500 boards. The license options are dependent on the relevant HiPath version.



Prerequisites

- The license keys must be obtained via the license server (Licensing... is performed on the basis of the MAC address of the HiPath 3000 CB board):
<https://www.central-license-server.com/>.
- Two licence keys are created.

2.1.2 Configuration Steps

HiPath 3000 Manager E

1. Configure the other possible HFA clients.
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.
3. Enter the number of B channels and the number of HFA clients.
4. Activate the purchased security licenses.
5. Enter the license keys. License keys can be obtained via the license server.



The additional B channels are available as soon as the licenses are activated.

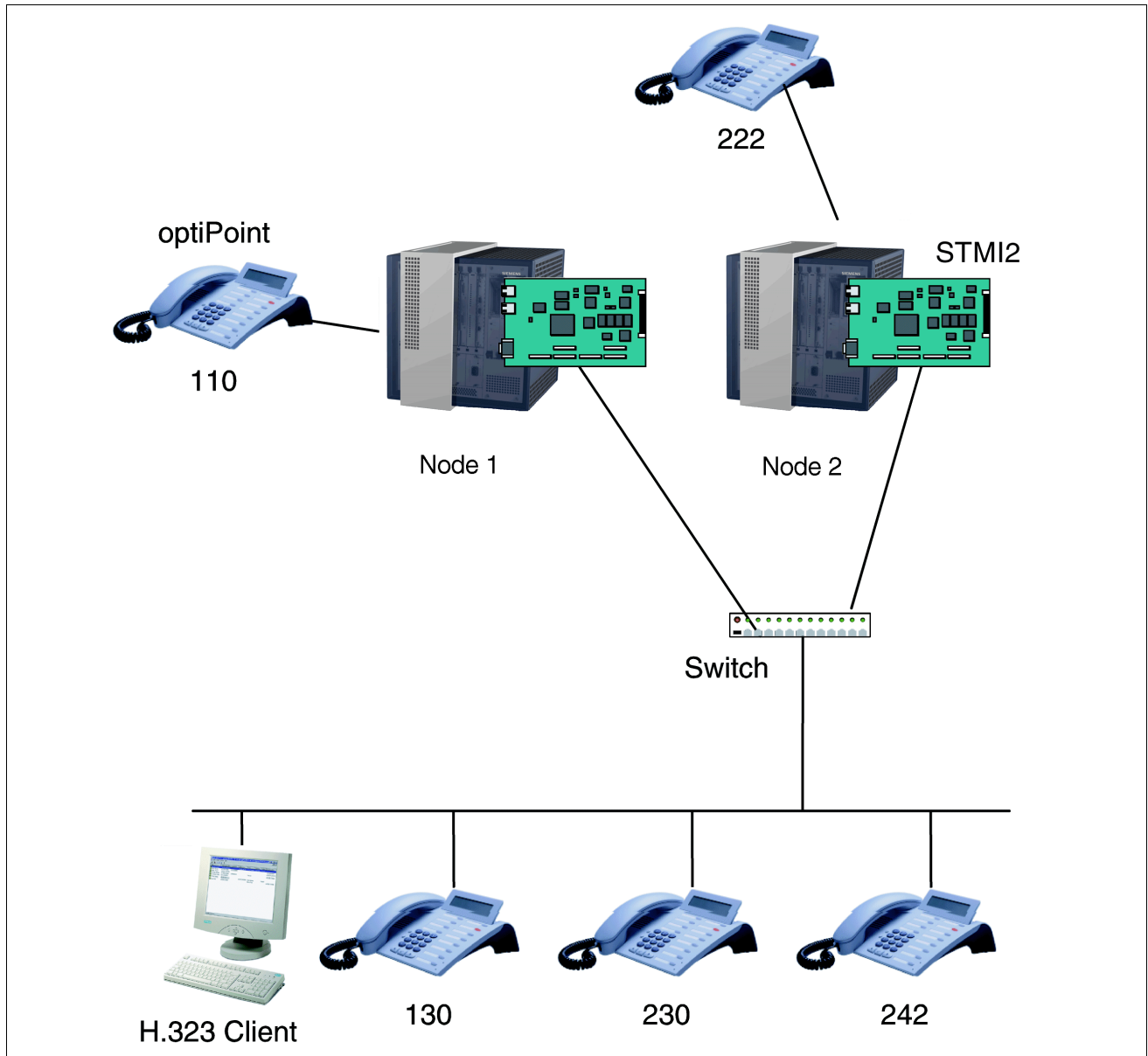
WBM Settings

1. If the IPsec function is licensed: Activate the IPsec function: "Explorers > Security > (right-click) VPN > IPsec on".

2.2 HiPath Feature Access

2.2.1 Target Configuration

HiPath IP telephone (for example optiPoint 420) functions can be used with this configuration. The Cornet-TS protocol is used for this.



Prerequisites

- All HG 1500 boards must be statically set for unique IP addresses.
- The administration PC with HiPath 3000 Manager E must have IP access to all nodes.
- OptiClients and IP telephones with HFA functionality that are connected to the PC must be able to access the IP network.

The following functions are possible in this scenario:

Connection	Normal calls	Call-backs	Call forwarding	Call pick-up	Conferencing	Recalls
SCN <-> HFA	yes	yes	yes	yes	yes	yes
HFA <-> HFA	yes	yes	yes	yes	yes	yes
HFA -> H.323	yes	no	yes	yes	yes	no
HFA <- H.323	yes	no	no	no	no	no

2.2.2 Configuration Steps

HiPath 3000 Manager E

1. System clients (HFA clients) can only be configured at the HG 1500 board that operates as a gatekeeper. Insert as many clients as necessary.
2. Assign a new station number, a DID, and a subscriber name to each new client.
3. Use HiPath 3000 Manager E to transfer the modified database back to the system.

HFA clients

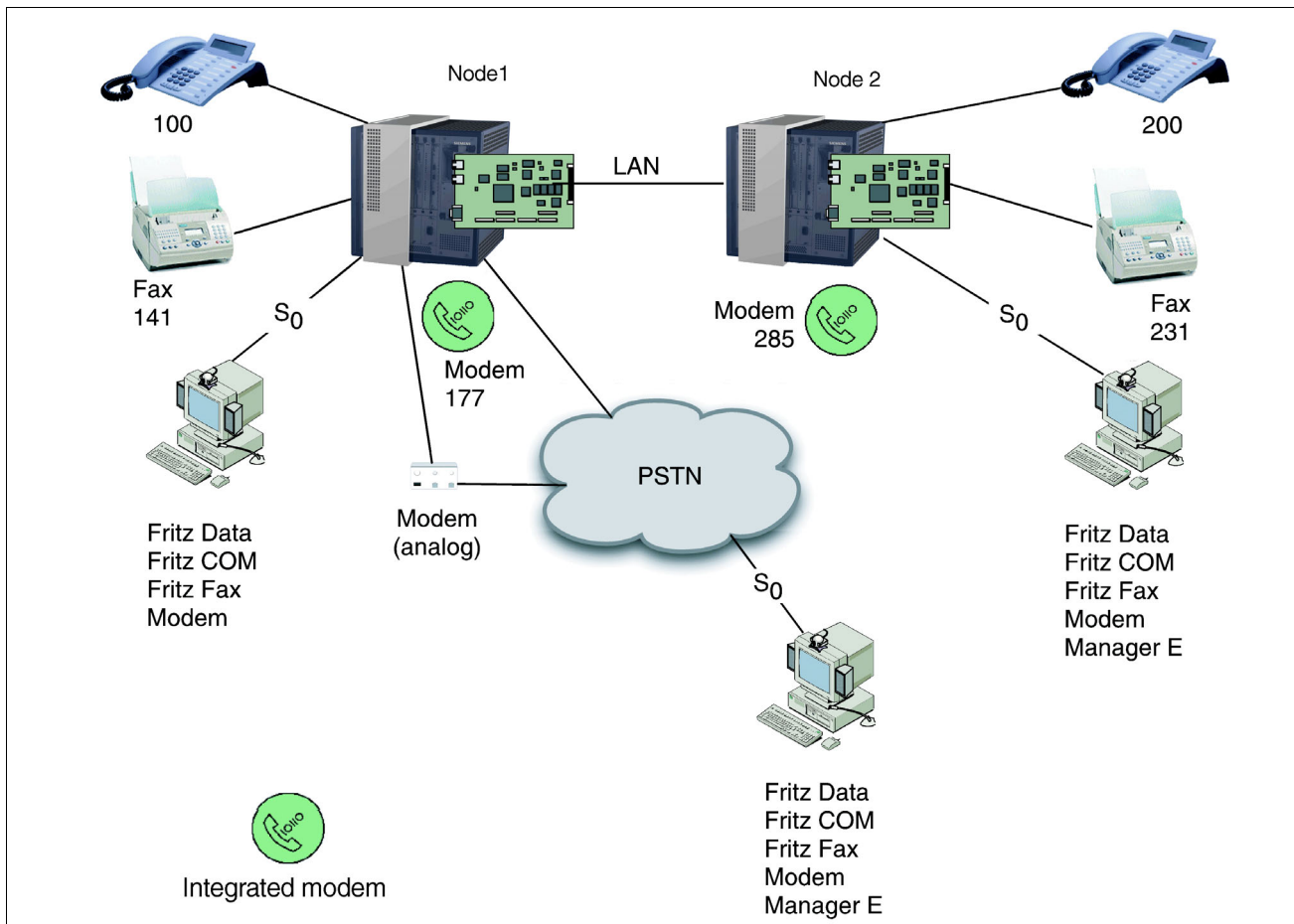
First of all, set the required station numbers in the *Stations* mask in HiPath 3000 Manager E. Select free ports for this. In the next step, these ports will be assigned to the HG 1500.

Configure the clients in accordance with the above settings (for example IP address, call numbers, password). Proceed as outlined in the description for the relevant HFA client.

2.3 IP Networking (Data)

2.3.1 Target Configuration

A number of HiPath systems are connected to each other via the corporate IP network structure using IP networking. The data is packeted and transmitted via the LAN and WAN networks.



The following functions are possible in this scenario:

- System connection and configuration via a remote access using dial-in modem
- Data transfer via ISDN with Fritz Data
- HyperTerminal with Fritz COM

The transmission options are shown in the following table:

	Fritz Fax	Fritz Data	Fritz Com	Analog fax	Analog modem	Integrated modem
Fritz Fax	yes	no	no	yes	no	no
Fritz Data	no	yes	no	no	no	no
Fritz Com	no	no	yes	no	no	no
Analog modem	no	no	no	no	no	yes
Integrated modem	no	no	no	no	yes	no
Analog fax	yes	no	no	yes	no	no

Prerequisites

- All HG 1500 boards must be statically set for unique IP addresses.
- The administration PC with HiPath 3000 Manager E must have IP access to all nodes.
- All nodes must have access to all peer nodes in the IP network.
- The subscriber numbers of all nodes must be known to each other.
- Different nodes must have a separate, unique subscriber number.
- Every HiPath system must have a separate unique node ID.
- Up to 64 nodes can be administered.
- The PC can dial into the telephone network via a modem.
- The analog fax is connected to the system via analog interfaces.

Practical Examples for HG 1500

IP Networking (Data)

2.3.2 Configuration Steps

HiPath 3000 Manager E

1. Enter the number of trunks for every HG 1500 board to be configured for IP networking.
2. Create an IP route for all of these HG 1500 boards.
3. Select the protocol to be used for the trunk port used if this was not automatically set correctly:
 - CorNet-IP
4. Activate the following functions for the routing parameters:

Route type	PABX
No. and type, outgoing	Internal
Callnumber typ	Internal / DID
5. Activate the function "Activate LCR".
6. Specify a name for the outdialing rules table and assign Format A to it. Set "Corporate Network" as the procedure.
7. Define the station number format and then select a routing table.
8. Select a route and a dial plan.
9. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

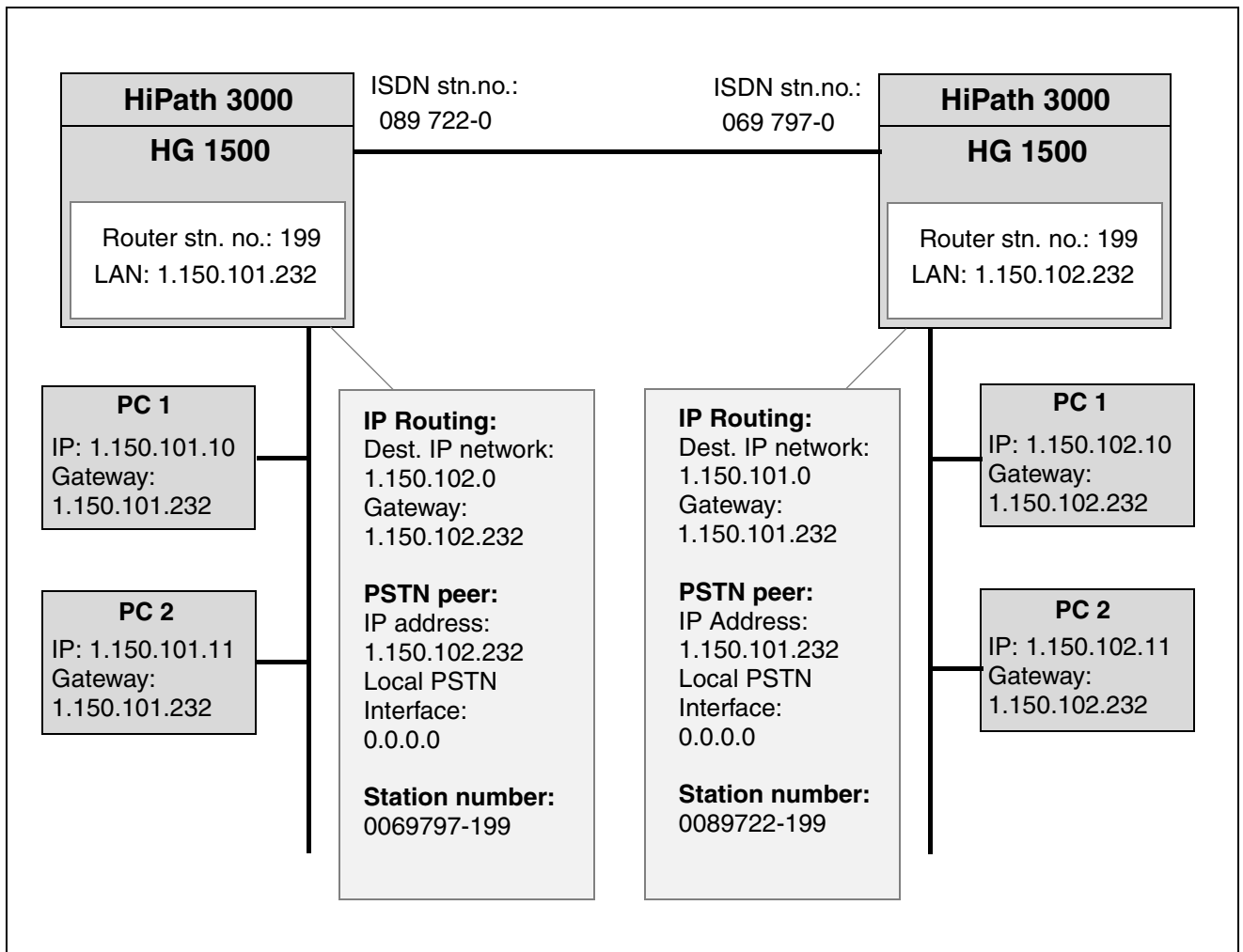
1. Add a PBX node. Enter a new node number.
2. Enter an IP address for each of the HG 1500 boards used in this node.
3. Add a station number to the node just configured and select the service "Fax" or "Modem".
4. Repeat these steps for all the call numbers required.
5. Save the entries.

2.4 Host Routing

2.4.1 Target Configuration

A host IP routing is to be set up between two remote locations in Munich and Frankfurt.

There is no transport network used with a host routing. The connection is set up directly to the router call number of the remote system. In the WAN, IP addressing takes place directly to the IP address of router of the remote station.



2.4.2 Configuration Steps

HiPath 3000 Manager E

1. Generate a host IP routing for your group. Use the data from the figure for the practical example in Section 2.4, "Host Routing".
2. Load the customer data from the HiPath 3000 with "File > Transfer > Read/write database > System > PC".
3. Select "No Port" under "Set up station... – Station". Enter the station number 199 in "Call No." and "DID". Assign a name, e.g. "IP Routing".
4. Select the HG 1500 board under "System-wide... > SW expansion > Card selection".
5. Select the HG 1500 board as Gatekeeper HG 1500 under "Settings > Set up station... > Gatekeeper > Selection".
6. Enable the gateway resources for this HG 1500 board.
7. Assign the station number 199 to the HG 1500 under "Settings > Set up station... > Gateway". Select station 199 and configure it as an S₀ extension.
8. Load the customer data in the HiPath 3000.

WBM settings for HG 1500 – Munich

1. Configure a static IP route.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 3
- Name: Frankfurt
- Destination IP Network/Host: 1.150.102.0
- Destination Netmask: 255.255.255.0
- Gateway: 1.150.102.232

2. Insert a PSTN peer:
"Explorers > Routing > PSTN > (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Name: Frankfurt
- IP Address of PSTN Peer: 1.150.102.232
- IP Address of Local PSTN Interface: 0.0.0.0

- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Frankfurt' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0069797199
- Direction: Incoming and Outgoing

WBM settings for the Frankfurt location

1. Configure a static IP route.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 3
- Name: Munich
- Destination IP Network/Host: 1.150.101.0
- Destination Netmask: 255.255.255.0
- Gateway: 1.150.101.232

2. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Name: Munich
- IP Address of PSTN Peer: 1.150.101.232
- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated

Practical Examples for HG 1500

Host Routing

- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Munich' > (right-click) Add Station Number".

Enter the following data:

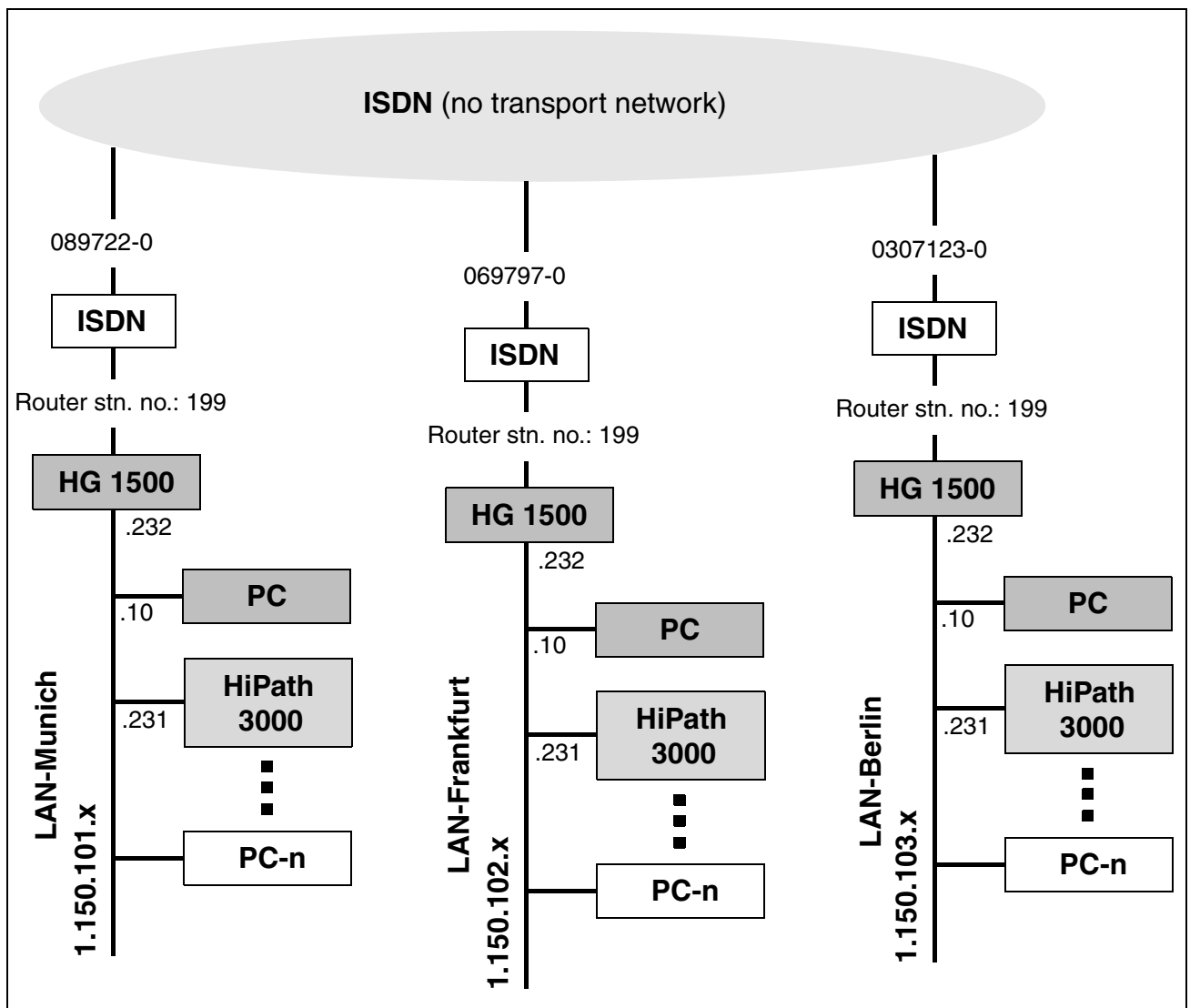
- Station Number: 0089722199
- Direction: Incoming and Outgoing

2.5 Host Routing With Alternate Route

2.5.1 Target Configuration

A host IP routing is to be set up between two remote locations in Munich and Berlin. However, there must be no direct access from Munich to the system in Berlin. It should be possible to have a route via the system in Frankfurt.

The system in Munich sets up the connection to the system in Berlin via the system in Frankfurt.



2.5.2 Configuration Steps

HiPath 3000 Manager E

1. Load the customer data from the HiPath 3000 with "File > Transfer > Read/write database > System > PC".
2. Select "No Port" under "Set up station... – Station". Enter the station number 199 in "Call No." and "DID". Assign a name, e.g. "IP Routing".
3. Select the HG 1500 board under "System-wide... > SW expansion > Card selection".
4. Select the HG 1500 board as Gatekeeper HG 1500 under "Settings > Set up station... > Gatekeeper > Selection".
5. Enable the gateway resources for this HG 1500 board.
6. Assign the station number 199 to the HG 1500 under "Settings > Set up station... > Gateway". Select station 199 and configure it as an S₀ extension.
7. Load the customer data in the HiPath 3000.

WBM settings for the Munich location

1. Configure a static IP route for the route to Frankfurt.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Frankfurt
- Destination IP Network/Host: 1.150.102.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 1.150.102.232

2. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Frankfurt
- IP Address of PSTN Peer: 1.150.102.232
- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated

- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Frankfurt' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0069797199
- Direction: Incoming and Outgoing

4. Configure another static IP route for the route to Berlin via Frankfurt.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 2
- Route Name: Berlin via Frankfurt
- Destination IP Network/Host: 1.150.103.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 1.150.102.232

The required PSTN peer already exists for the Munich-Frankfurt connection.

WBM settings for the Frankfurt location

1. Configure a static IP route for the route to Munich.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Munich
- Destination IP Network/Host: 1.150.101.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 1.150.101.232

Practical Examples for HG 1500

Host Routing With Alternate Route

2. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Munich
- IP Address of PSTN Peer: 1.150.101.232
- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Munich' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0089722199
- Direction: Incoming and Outgoing

4. Configure another static IP route for the route to Berlin.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 2
- Route Name: Berlin
- Destination IP Network/Host: 1.150.103.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 1.150.103.232

5. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Munich
- IP Address of PSTN Peer: 1.150.103.232

- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

6. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Munich' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 003071234199
- Direction: Incoming and Outgoing

WBM settings for the Berlin location

1. Configure a static IP route for the route to Frankfurt.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Frankfurt
- Destination IP Network/Host: 1.150.102.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 1.150.102.232

2. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Frankfurt
- IP Address of PSTN Peer: 1.150.102.232
- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated

Practical Examples for HG 1500

Host Routing With Alternate Route

- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Frankfurt' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0069797199
- Direction: Incoming and Outgoing

4. Configure another static IP route for the route to Munich via Frankfurt.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

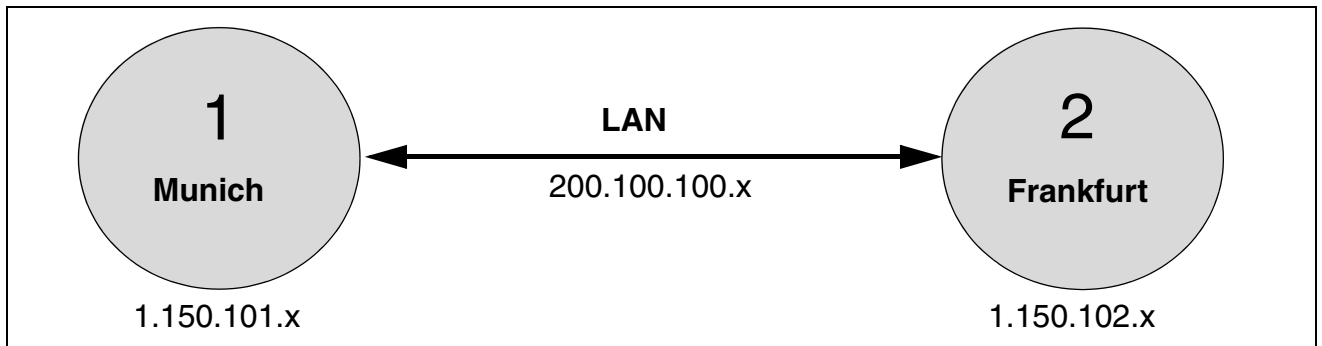
- Route Index: 2
- Route Name: Munich via Frankfurt
- Destination IP Network/Host: 1.150.101.0
- Destination Netmask: 255.255.255.0
- Gateway: 1.150.102.232

The required PSTN peer already exists for the Munich-Frankfurt connection.

2.6 LAN-LAN Routing

2.6.1 Target Configuration

A LAN-LAN routing is to be set up between two remote locations in Munich and Frankfurt. The routing is to be implemented via the LAN2 interface of the HG 1500.



2.6.2 Configuration Steps

WBM settings for the Munich location

1. Configure a static IP route.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Frankfurt
- Destination IP Network/Host: 1.150.102.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 200.100.100.2

2. Configure the LAN2 interface:
"Explorers > Network Interfaces > LAN2 > (right-click) Edit LAN2 Interface".

Select the option "LAN2" under "Use the Second LAN as".

Then enter the following data:

- IP Address: 200.100.100.1
- Subnet Mask: 255.255.255.0

The default values are used for all other parameters.

Practical Examples for HG 1500

LAN-LAN Routing

WBM settings for the Frankfurt location

1. Configure a static IP route.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Munich
- Destination IP Network/Host: 1.150.101.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 200.100.100.1

2. Configure the LAN2 interface:
"Explorers > Network Interfaces > LAN2 > (right-click) Edit LAN2 Interface".

Select the option "LAN2" under "Use the Second LAN as".

Then enter the following data:

- IP Address: 200.100.100.2
- Subnet Mask: 255.255.255.0

The default values are used for all other parameters.



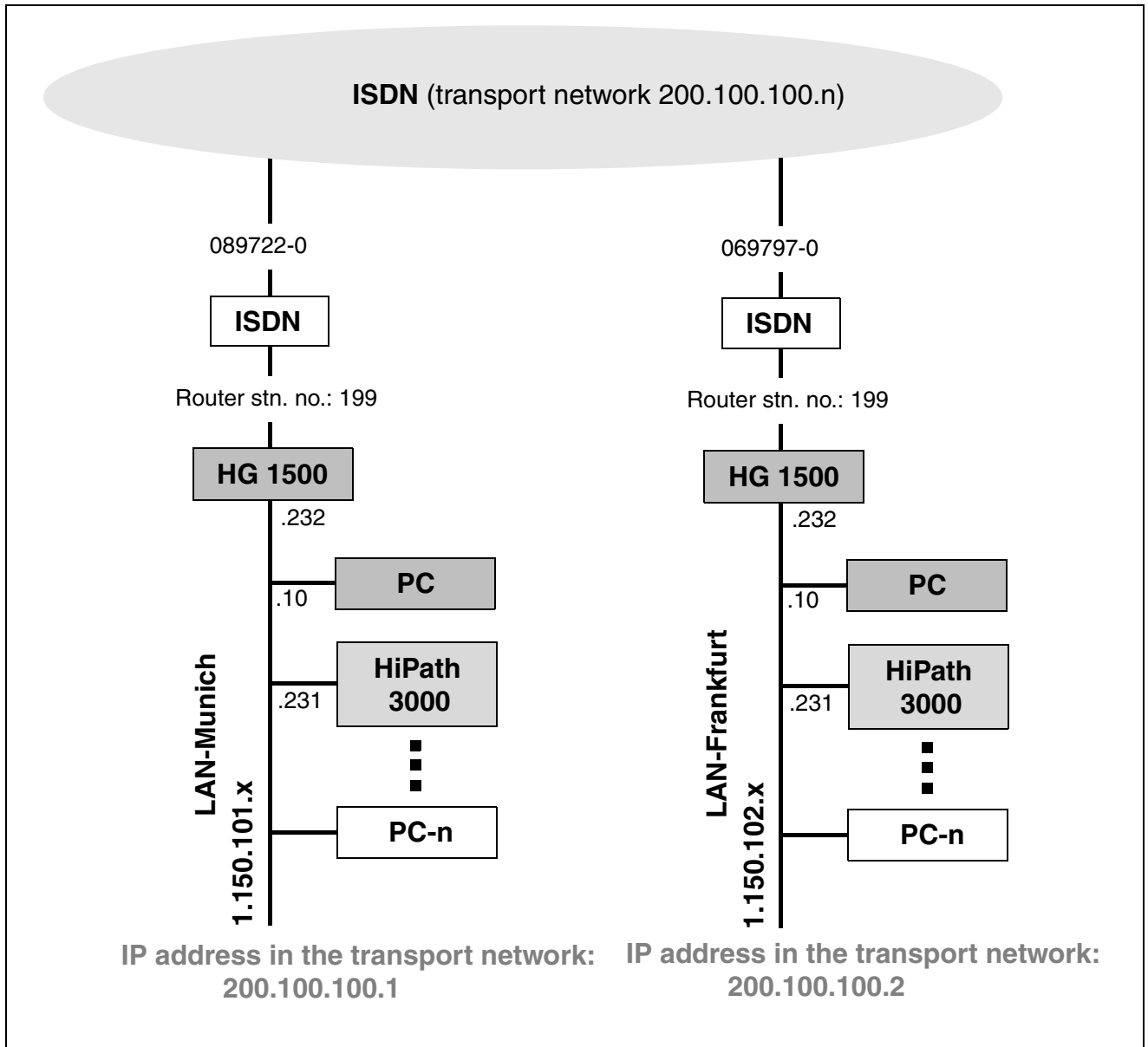
For testing purposes, the outputs of the LAN2 interface can be connected with the partner systems via a crossover cable.

2.7 Static Routing

2.7.1 Target Configuration

A static IP routing is to be set up between two remote locations in Munich and Frankfurt. The PSTN is used in this case.

The routing function should be tested using the "ping" and "tracert" programs.



2.7.2 Configuration Steps

HiPath 3000 Manager E

1. Generate a static IP routing for your group. Use the data from the figure for the practical example in Section 2.7, "Static Routing".
2. Load the customer data from the HiPath 3000 with "File > Transfer > Read/write database > System > PC".
3. Select "No Port" under "Set up station... – Station". Enter the station number 199 in "Call No." and "DID". Assign a name, e.g. "IP Routing".
4. Select the HG 1500 board under "System-wide... > SW expansion > Card selection".
5. Select the HG 1500 board as Gatekeeper HG 1500 under "Settings > Set up station... > Gatekeeper > Selection".
6. Enable the gateway resources for this HG 1500 board.
7. Assign the station number 199 to the HG 1500 under "Settings > Set up station... > Gateway". Select station 199 and configure it as an S₀ extension.
8. Load the customer data in the HiPath 3000.

WBM settings for the Munich location

1. Configure the general settings for PSTN.
"Explorers > Routing > PSTN > (right-click) Edit Global PSTN Data".
Enter the following data:
 - Router Call Number: 199
 - Number of Redial Attempts: 5
 - Pause between Redial Attempts (sec): 5
 - The fields for scripting remain blank.
2. Configure a static IP route for the route to Frankfurt.
"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".
Configure the following data for the static route:
 - Route Index: 1
 - Route Name: Frankfurt
 - Destination IP Network/Host: 1.150.102.0
 - Destination Netmask: 255.255.255.0
 - Route Gateway: 200.100.100.2

3. Insert a PSTN peer:
"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Frankfurt
- IP Address of PSTN Peer: 200.100.100.2
- IP Address of Local PSTN Interface: 200.100.100.1
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

4. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > 'Frankfurt' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0069797199
- Direction: Incoming and Outgoing

WBM settings for HG 1500 – Frankfurt

1. Configure the general settings for PSTN.
"Explorers > Routing > PSTN > (right-click) Edit Global PSTN Data".

Enter the following data:

- Router Call Number: 199
- Number of Redial Attempts: 5
- Pause between Redial Attempts (sec): 5
- The fields for scripting remain blank.

Practical Examples for HG 1500

Static Routing

2. Configure a static IP route.

"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Munich
- Destination IP Network/Host: 1.150.101.0
- Destination Netmask: 255.255.255.0
- Route Gateway: 200.100.100.1

3. Insert a PSTN peer:

"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Munich
- IP Address of PSTN Peer: 200.100.100.1
- IP Address of Local PSTN Interface: 200.100.100.2
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60

The default values are used for all other parameters.

4. Configure a PSTN station number for the PSTN peer:

"Explorers > Routing > PSTN > PSTN Peers > 'Munich' > (right-click) Add Station Number".

Enter the following data:

- Station Number: 0089722199
- Direction: Incoming and Outgoing

PC and extension settings

1. Change the default gateway to the IP address of the HG 1500: 1.150.102.232:
"Network Neighborhood > LAN Connection Properties > Internet Protocol (TCP/IP) > Properties".
2. For diagnostic purposes, configure one key for the router station number and another key for the ISDN trunk groups on extension 100.

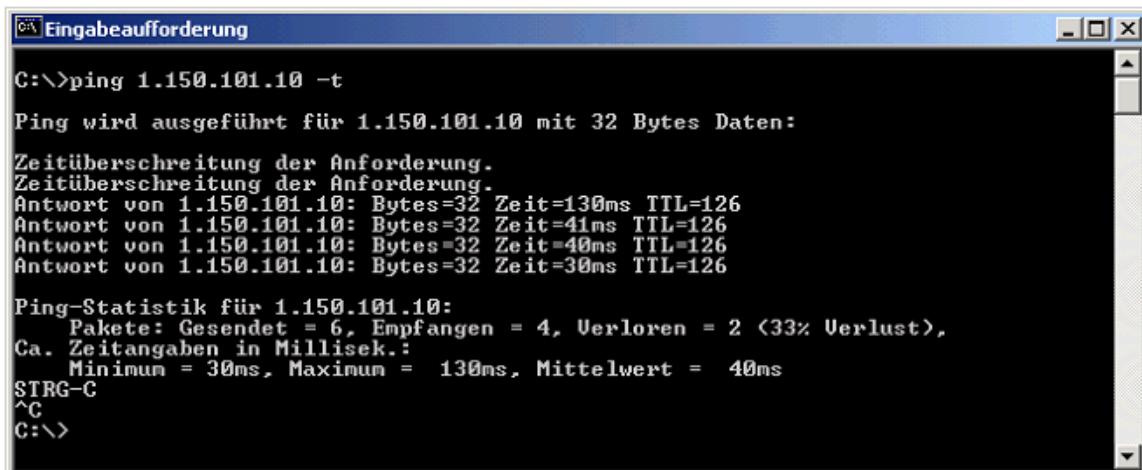
Configure the keys on the first station in the HiPath 3000:

Service code "*91" > Select key 1 > "Edit Key" > Station Number > Enter 199.

Select key 2 > "Edit Key" > Scroll backwards to trunk key > Enter trunk number 7801 for line 1.

Select key 3 > "Edit Key" > Scroll backwards to trunk key > Enter trunk number 7802 for line 2.

3. Check the routing function on the PC using the "ping" and "tracert" programs. Open the DOS prompt and enter the commands as shown in the screenshots below.

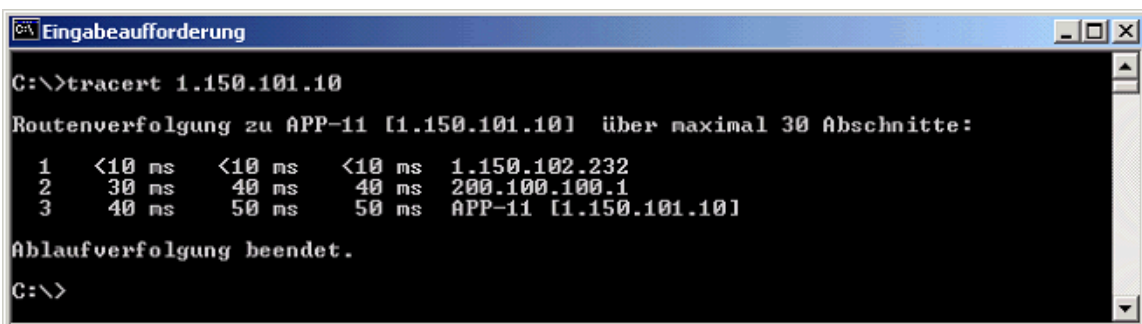


```
C:\>ping 1.150.101.10 -t

Ping wird ausgeführt für 1.150.101.10 mit 32 Bytes Daten:

Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Antwort von 1.150.101.10: Bytes=32 Zeit=130ms TTL=126
Antwort von 1.150.101.10: Bytes=32 Zeit=41ms TTL=126
Antwort von 1.150.101.10: Bytes=32 Zeit=40ms TTL=126
Antwort von 1.150.101.10: Bytes=32 Zeit=30ms TTL=126

Ping-Statistik für 1.150.101.10:
    Pakete: Gesendet = 6, Empfangen = 4, Verloren = 2 (33% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 30ms, Maximum = 130ms, Mittelwert = 40ms
STRG-C
^C
C:\>
```



```
C:\>tracert 1.150.101.10

Routenverfolgung zu APP-11 [1.150.101.10] über maximal 30 Abschnitte:

 1  <10 ms  <10 ms  <10 ms  1.150.102.232
 2   30 ms   40 ms   40 ms  200.100.100.1
 3   40 ms   50 ms   50 ms  APP-11 [1.150.101.10]

Ablaufverfolgung beendet.

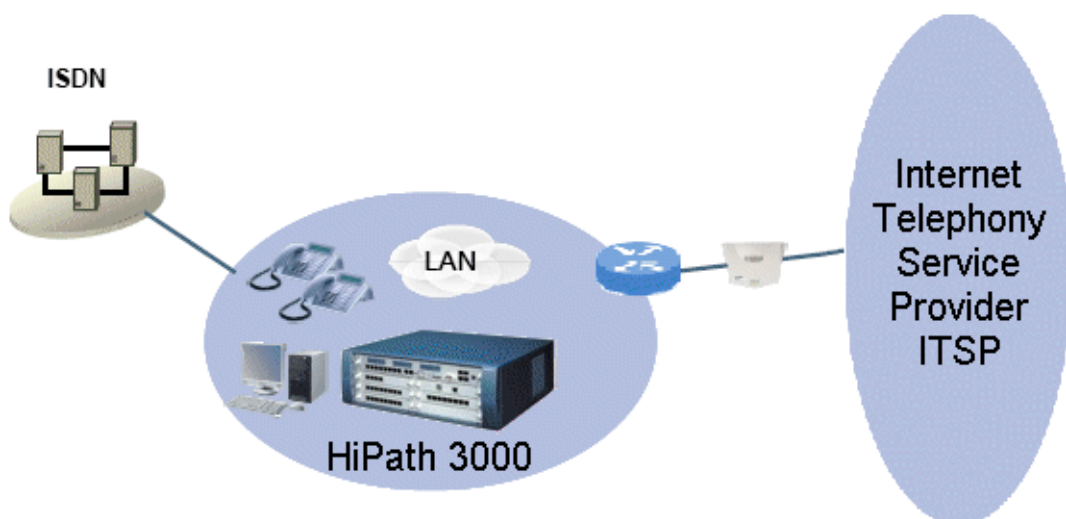
C:\>
```

It is possible to ping the transfer network (200.100.100.x). The transfer network also shows route tracing with tracert (see figure above).

2.8 Configuring an Internet Telephony System Connection

2.8.1 Target Configuration

An Internet telephony system connection should be configured for the HiPath 3000 communications system.



Starting basis

- Initial startup has been performed for the HiPath 3000. The following U_{P0/E} subscribers are configured:
 - "Richard" with the station number 200
 - "Stefan" with the station number 220
 - "Hannelore" with the station number 222
- Richard is to be assigned the Internet telephony DID phone number 0. Stefan is assigned the DID number 1 and Hannelore should be assigned the DID number 2.
- The customer router (such as Netgear Prosafe FVS114) enables the customer to access the Internet. The ADSL at the customer site has a speed of 6 Mbps downstream and 384 Kbps upstream (Provider: T-Online, for instance).



It is only possible to connect an ITSP via a customer router via the LAN1 LAN port of an HG 1500 board. Connection using the LAN2 LAN port is not supported.

- Additionally Internet telephony should be enabled for the HiPath 3000 communications system, via the customer router. The NAT implementation of the upstream customer router is not relevant here.

- The Internet telephony CO connection as well as DID for the ITSP "QSC" is configured with the following features:
 - 1 account (registration and authentication)
 - 2 voice channels
 - 10 local telephone numbers in international format:
 - 49 (Germany) 89 (Munich) 22630488 (local) 0 to 9 (DID)



Interoperability between providers is crucial for the successful establishment and usage of Internet telephony features. Refer to the ITSP's general terms and conditions.

The current list of approved ITSPs can be found here:

http://wiki.siemens-enterprise.com/index.php/Collaboration_with_VoIP_Providers

Configuration

Use 3000 Manager E and the HG 1500 WBM for this purpose.

The following configuration is recommended:

- Manager E > DSL route and parameter configuration
- Manager E > LCR configuration
- WBM of the HG 1500 > SIP provider configuration including Internet telephone subscriber and station number

2.8.2 Initial Setup in the HiPath 3000 Manager E

Add trunks

1. Go to "Settings > Lines / networking..." and select the "IP Trunks" tab.
2. Specify the board that will be used for IP trunking under "Selection > Gatekeeper HG 1500 > Slot X".
3. In the "Number" field, define the number of trunks (e.g. 2, SIP Provider 1) that should be configured. When you click the "Add" button, the trunks appear in the corresponding display field.
4. Enable the gateway resources.
5. Apply the settings.

Configure routes

1. Go to "Settings > Lines / networking ..." and select the "Routes" tab.
2. In the "Routes" display field, select Trk Grp. 12 (Trk Grp. xyz) for the first ITSP and seizure code "855" (default) for establishing calls from the "Missed Calls List" and dialing Trk Grp. 12 (QSC) directly.

If LCR is enabled, a call number already being used for a different trunk group can be assigned here (such as "0").
3. PABX number-incoming/PABX number outgoing > Do not make any entries in these fields.



Trk Grp 13 must be used for the second ITSP, Trk Grp 14 for the third and Trk Grp 15 for the fourth ITSP. You can configure up to four ITSPs.

4. Apply the settings.

Configure routing parameters

1. Go to "Settings > Lines / networking ..." and select the "Routing parameters" tab.
2. Activate the routing type "CO" under "Route type".
3. Activate "Unknown" under "No. and type, outgoing".
4. Activate the type "Internal" under "Callnumber type".
5. Apply the settings.

Configure special networking

1. Go to "Settings > Lines / networking ..." and select the "Special" tab.
2. Deactivate the "Always use DSP" switch under "Switches".
3. Apply the settings.

Configure trunks

1. Go to "Settings > Lines / networking ..." and select the "Trunks" tab.
2. In the "Code" column, configure a trunk code if, for example, the trunks are to be monitored and switched via the TAPI/CSTA.
3. Apply the settings.

Configure LCR

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area " LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Configure LCR classes of service

1. Go to "Settings > Least cost routing..." and select the "Classes of service" tab.
2. Set the LCR class of service for fax/modem to "1". Fax/modem stations can only break out to "ISDN" with class of service "1".

Exception: Internet telephony system connection if the ITSP supports fax connections in accordance with their general terms and conditions.

The current list of approved ITSPs and details on fax connections can be found here:

http://wiki.siemens-enterprise.com/index.php/Collaboration_with_VoIP_Providers

3. Apply the settings.



Ensure that the LCR class of service for fax/modem and the router call number for remote access are set correctly.
Internet telephony requires LCR class of service 15.

Practical Examples for HG 1500

Configuring an Internet Telephony System Connection

Configure dial plan

1. Go to "Settings > Least cost routing" and select the "Dial plan" tab.
2. Configure the dial plan/dial rule.
 - Special/emergency fax and modem numbers via ISDN routes. Refer to the latest sales and service release for more information.

Codes and flags | Classes of service | **Dial plan** | LCR - schedule

Digit analysis wizard

Name	Dialed digits	Route table	Acc. code	COS	Emergency
1 special number	C112	1	No	yes	No
2 special number	C114	1	No		
3 special number		1	No		
4 special number		1	No		
5 special number		1	No		

Route table: 1 | Dial rule wizard

Route	Dial rule	min. COS
1 ISDN	1 ISDN	1
2 .	.	15
3 .	.	15
4 .	.	15
5 .	.	15
6 .	.	15

Dial rule wizard

Edited dial rule: ISDN

Network provider's method of: Main network supplier

Access code:

Pause (max. 12 secs.):

Authorization code:

Dial rule format: A

min. COS: 1

Schedule: .

Warning: None

Type of Number (TON): Unknown

Help OK Cancel

- The first route "QSC" > Overflow to "ISDN" if the ITSP is not available.

Codes and flags | Classes of service | **Dial plan** | LCR - schedule

Digit analysis wizard

Name	Dialed digits	Route table	Acc. code	COS	Emergency
1 Standard	0C01Z	2	No	yes	No
2 Standard	0CONZ	3	No		
3 Standard	0C01Z	3	No		
4 Standard	0CONZ	3	No		
5 Standard		3	No		

Route table: 1 | Dial rule wizard

Route	Dial rule	min. COS
1 QSC	2 SIP-ISDN	1
2 .	.	15
3 .	.	15
4 .	.	15
5 .	.	15
6 .	.	15

Dial rule wizard

Edited dial rule: SIP-ISDN

Network provider's method of: Main network supplier

Access code:

Pause (max. 12 secs.):

Authorization code:

Dial rule format: A

min. COS: 1

Schedule: .

Warning: None

Type of Number (TON): Unknown

Help OK Cancel

- Outgoing local calls via QSC.

Codes and flags | Classes of service | Dial plan | LCR - schedule

Digit analysis wizard

	Name	Dialed digits	Route table	Acc. code	COS	Emergency
1	Standard	0C01Z	2	No	yes	No
2	Standard	0CONZ	3	No		
3	Standard	0C01Z	3	No		
4	Standard	0CONZ	3	No		
5	Standard		3	No		

Route table: 3

	Route	Dial rule	min. COS
1	QSC	3 SIP-City	15
2	.	.	15
3	.	.	15
4	.	.	15
5	.	.	15
6	.	.	15

Dial rule wizard

Edited dial rule: SIP-City

Network provider's method of: Unknown

Access code:

Pause (max. 12 secs.):

Authorization code:

Dial rule format: D089E2A

min. COS: 15

Schedule: .

Warning: None

Type of Number (TON): Unknown

Help OK Cancel

- Outgoing calls with seizure code "855" (default) via QSC.

Codes and flags | Classes of service | Dial plan | LCR - schedule

Digit analysis wizard

	Name	Dialed digits	Route table	Acc. code	COS	Emergency
2	Standard	0CONZ	3	No	yes	No
3	Standard	0C01Z	3	No		
4	Standard	81CZ	4	No		
5	Standard		5	No		
6	Standard		4	No		

Route table: 4

	Route	Dial rule	min. COS
1	QSC	2 SIP-ISDN	15
2	ISDN	4 ISDN	15
3	.	.	15
4	.	.	15
5	.	.	15
6	.	.	15

Dial rule wizard

Edited dial rule: SIP-ISDN

Network provider's method of: Main network supplier

Access code:

Pause (max. 12 secs.):

Authorization code:

Dial rule format: A

min. COS: 15

Schedule: .

Warning: None

Type of Number (TON): Unknown

Help OK Cancel

Practical Examples for HG 1500

Configuring an Internet Telephony System Connection

- Outgoing local calls with seizure code "855" (default) via QSC.

The screenshot shows the 'Dial rule wizard' configuration window. The main window has tabs for 'Codes and flags', 'Classes of service', 'Dial plan', and 'LCR - schedule'. The 'Dial plan' tab is active, showing a table of dial rules. The 'Dial rule wizard' dialog is open, showing the following settings:

Name	Dialed digits	Route table	Acc. code	COS	Emergency
2 Standard	0CONZ	3	No	yes	No
3 Standard	0C01Z	3	No		
4 Standard	81CZ	4	No		
5 Standard	81C1Z	5	No		
6 Standard		4	No		

The 'Dial rule wizard' dialog shows the following settings:

- Edited dial rule: SIP-City
- Network provider's method of: Main network supplier
- Access code:
- Pause (max. 12 secs.):
- Authorization code:
- Dial rule format: D089E2A (highlighted with a red box)
- min. COS: 15
- Schedule: .
- Warning: None
- Type of Number (TON): Unknown

- Apply the settings and load the data into the system.

Activate transit trunk connections if necessary

- Go to "Settings -> System parameters" and select the "Flags" tab.
- Activate the "SIP prov. to SIP prov. transit" flag to enable transit trunk connections with ITSP connections.
- Apply the settings and load the data into the system.



Transit trunk connections should only be activated in consultation with the customer. A transit trunk connection is established if a call seizes two lines of the same system. Example An external call is routed to a HiPath 3000 station via an ITSP. The HiPath 3000 station then hands the call over again to an external destination via an ITSP. This produces a transit trunk connection within the HiPath 3000 system. Two lines are seized for the duration of the call. If the flag is not set (default setting), transit trunk connections are not possible with ITSP connections.

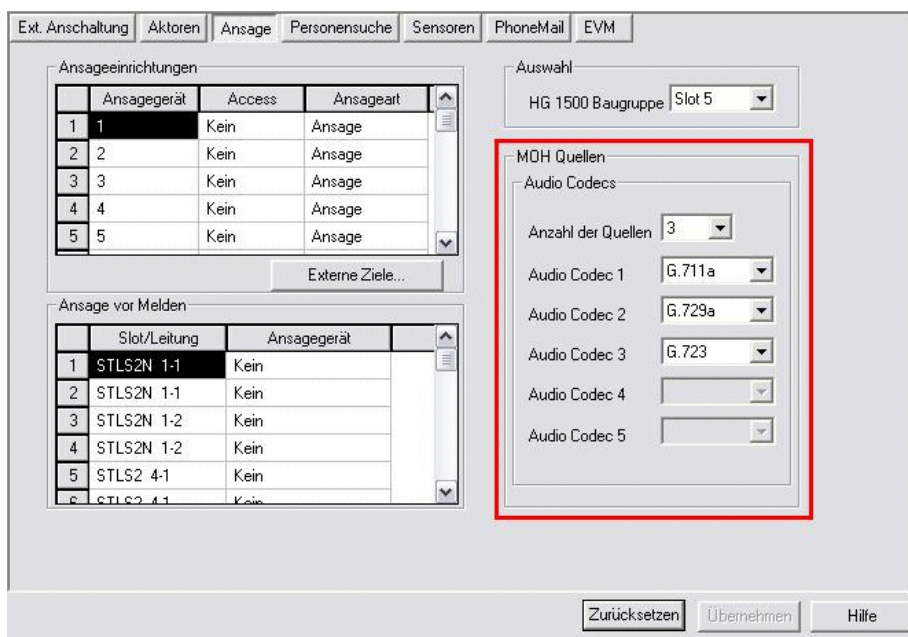
Configure MoH sources if required

Callers will be played music (Music On Hold MOH) if they cannot be connected immediately to the required HiPath 3000 station.

1. In "Settings > Auxiliary Equipment" select the "Announcement" tab.
2. Under "MoH Sources" select the "Number of sources" and the audio codes supported by the ITSP.

The current list of approved ITSPs and details on which codecs the different ITSPs support can be found here:

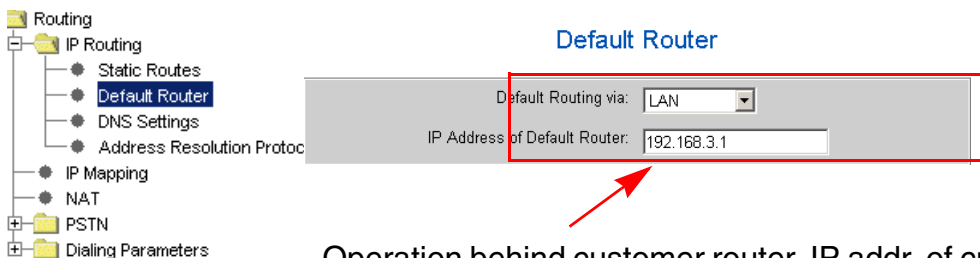
http://wiki.siemens-enterprise.com/index.php/Collaboration_with_VoIP_Providers



3. Apply the settings and load the data into the system.

2.8.3 Router Entry via the HG 1500 WBM

The following example illustrates a router entry if the HiPath 3000 system was connected behind a customer router (customer router: 192.168.3.1). The customer router routes all IP packets via the DSL interface to the Internet.



Operation behind customer router, IP addr. of customer router

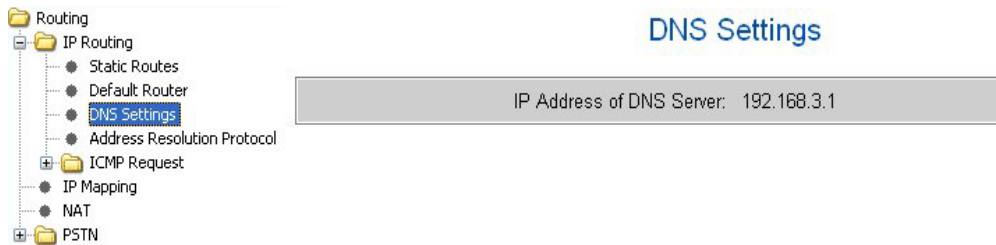
Practical Examples for HG 1500

Configuring an Internet Telephony System Connection

2.8.4 Configuration via HG 1500 WBM

DNS entry

The following example illustrates a DNS entry if the HiPath 3000 system is connected behind a customer router (customer router: 192.168.3.1) and the customer router is a DNS forwarder or DNS proxy for calls in the direction of the Internet Service Provider.



Check gateway settings

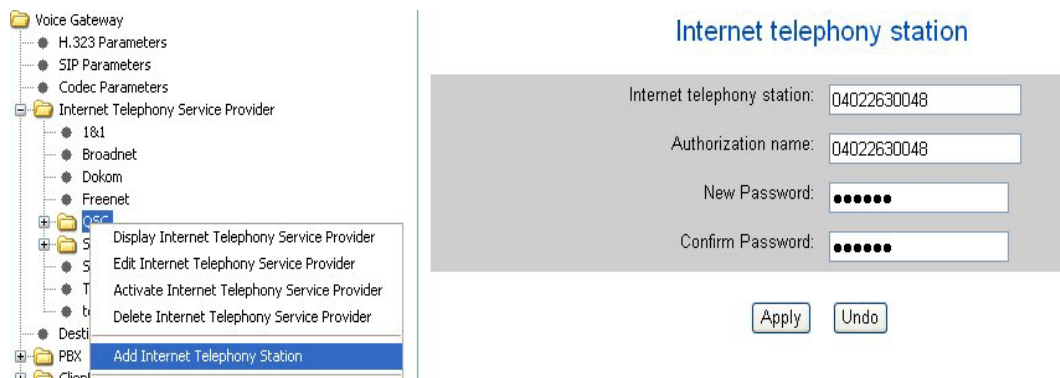
To ensure proper functioning of Internet telephony, the following settings should be checked.

1. Select: "Explorer > Basic Settings > Gateway".
2. The "protocol variants "Extendend Fast Connect" active", "RTP Proxy active" and "Adaptive Media Control" parameters must be activated.

Add Internet telephony subscriber

1. Select: "Explorer > Voice Gateway > Internet Telephony Service Provider > QSC (> right-click) > Add Internet telephony subscriber"
2. Enter the relevant parameters.

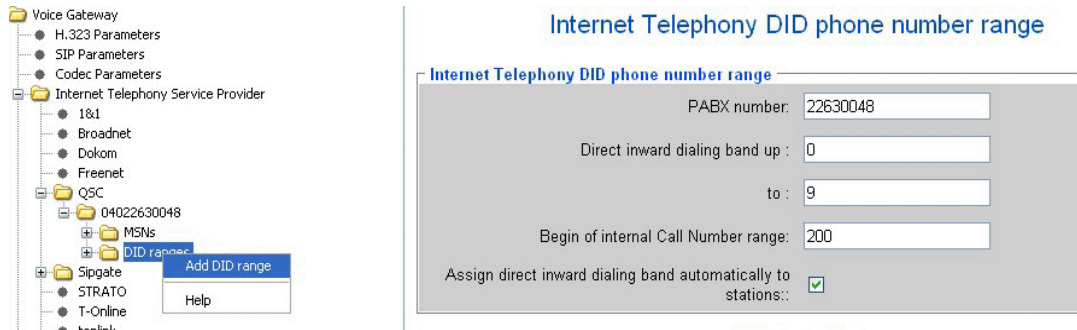
The ID assigned by the ITSP contains the subscriber ID and password.



Authentication/registration with the ITSP (Registrar server) may vary depending on the provider. For example, T-Online requires a valid e-mail address as the authorization name.

Add a DID range

1. Select: "Explorer > Voice Gateway > Internet Telephone Service Provider > (1) QSC > 04022630048 ... > DID range (> right-click > Add a DID range"
2. Enter the relevant parameters.

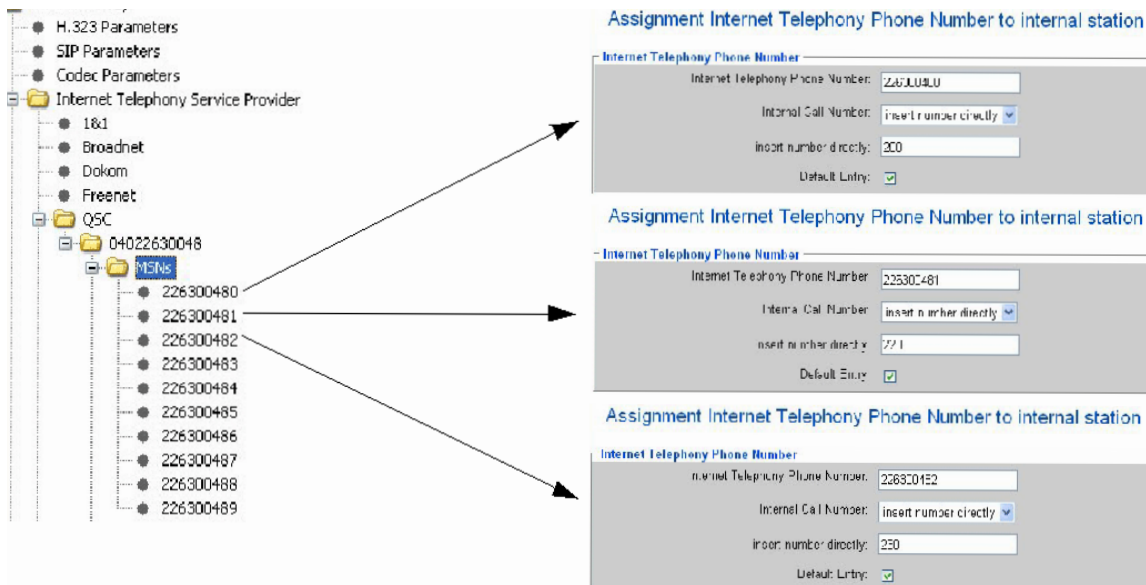


The format of the PABX number may vary depending on the provider. For example:

- Top link: +49xxxx (international)
- QSC: 040xxx (national).

Optional

Automatic assignment of the DID range from subscriber "200" onwards (the "default entry" is not automatically active).



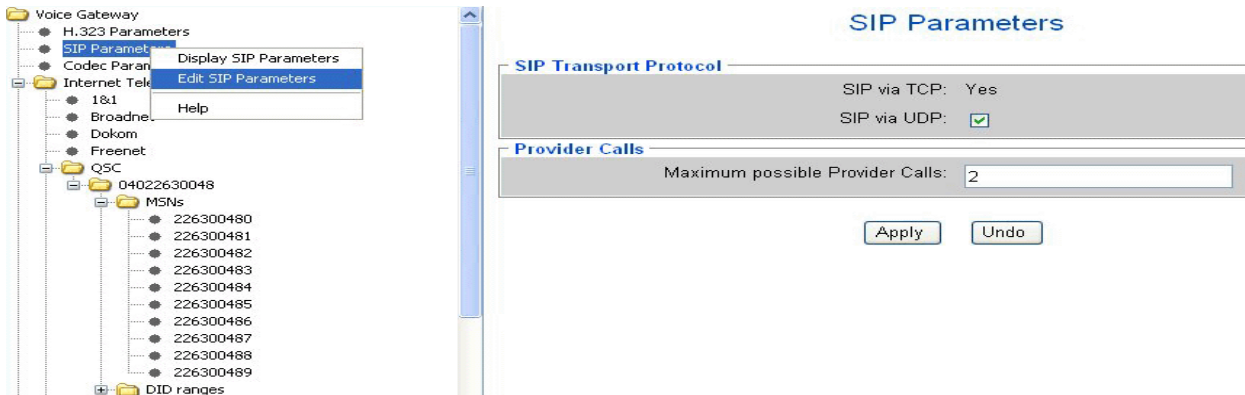
The number of connected stations generally exceeds the number of available Internet telephony phone numbers per provider. If a station does not have its own Internet telephony phone numbers, an outgoing PABX number is used as the default entry. The "default entry" must still be activated.

Practical Examples for HG 1500

Configuring an Internet Telephony System Connection

Edit SIP Parameters

1. Select:
"Explorers > Voice Gateway > SIP Parameters (> right-click) > Edit SIP Parameters".
2. Enter the relevant parameters.

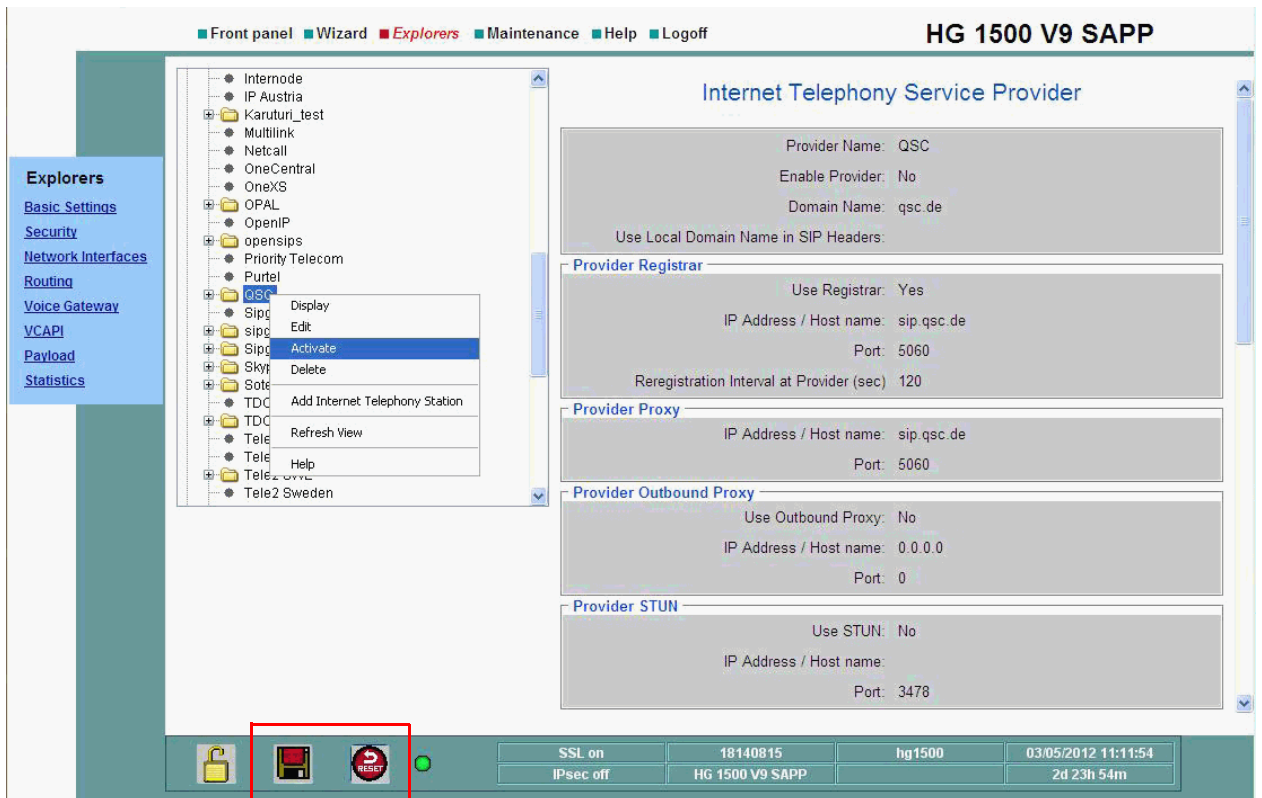


The default setting "0" in the field "Maximum possible Provider Calls" must be changed to the maximum number of calls possible.

The maximum number of calls possible via the provider (e.g. 2) corresponds to the maximum number of simultaneous calls in the direction of the SIP provider. Up to 128 Kbps upstream is reserved for each call. This value can vary depending on the codec used.

Activate SIP provider

1. Select
“Explorers > Voice Gateway > Internet Telephony Service Provider > QSC (> right click) > Activate
2. Enter the relevant parameters.



You may have to reset the HG 1500 after configuring the first SIP provider.

Practical Examples for HG 1500

Configuring an Internet Telephony System Connection

Configure STUN

1. Select:
"Explorers > Voice Gateway > SIP Provider (> right click) > Edit STUN Configuration"
2. Enter the relevant parameters.



Notes on configuring the STUN mode:

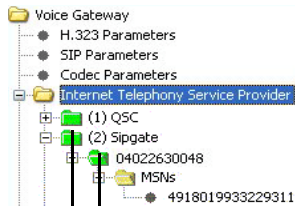
- *Always* – The STUN client is always active, even if no ITSP is active, for example. Regardless of the NAT type detected, parameters for NAT traversal in SIP messages are adapted.
- *Automatic* - the settings in the ITSP's profile are used (e.g., QSC without STUN, T-Online with STUN). If no ISTP is active, STUN is completely deactivated. If the ITSP is activated, STUN establishes the type of firewall (NAT type) used during system startup and identifies changes in the IP address at runtime. Depending on the NAT type detected (not if no NAT or Symmetric NAT is used), STUN modifies parameters for NAT traversal in SIP messages.
- *Use static IP* – This mode must be selected if a static IP address is being used at the ADSL modem/router. The static IP address and the port must be entered.
- *Router keeps port* – This mode must be selected if none of the previous settings work. There are some modems/routers that have a special port for NAT and need this setting to work properly.

STUN is not required with ITSPs which resolve NAT Traversal via infrastructure components in the provider network such as Session Border Controller (SBC).

2.8.5 Check Setup

Initial Setup Check

1. Select:
"Explorers > Voice Gateway > SIP Provider > (1) QSC > 04022..."
2. Check the initial setup.



Internet telephony subscriber registered (green)

Activated ITSP (green) in case all Internet telephone subscribers are functioning (also green!)

Folder status:

- Green: O.K.
- Yellow: Not activated/configured.
- Orange: Provider only.
At least one of the Internet telephony subscribers failed.

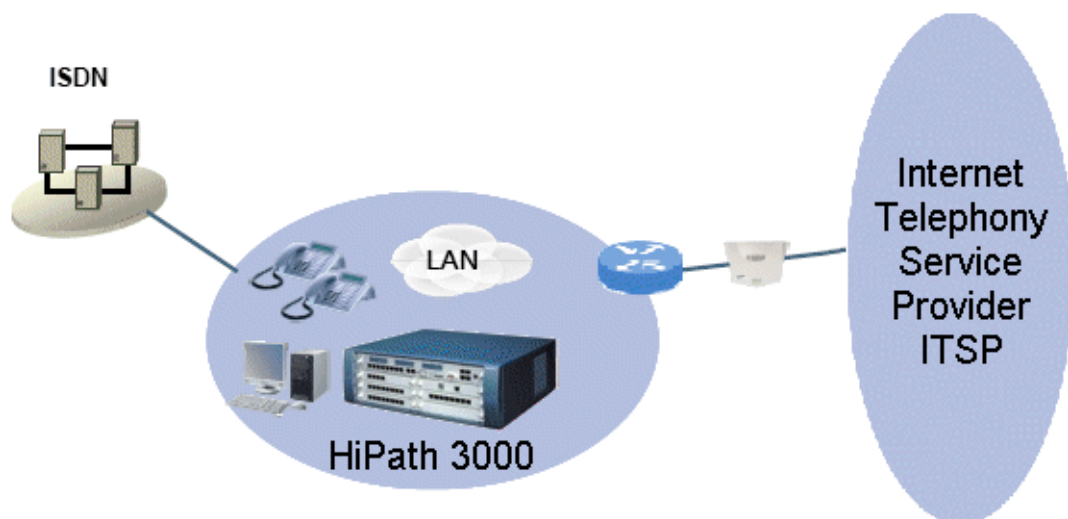
2.9 Adding Internet Telephony User Connections

2.9.1 Target Configuration

Internet telephony station connections should be configured for the HiPath 3000 communications system.



Further configuration example: Section 2.8, "Configuring an Internet Telephony System Connection"



Starting basis

An Internet telephony system connection is configured. The Internet telephony DID phone numbers are assigned to Richard, Stefan and Hannelore.

The Internet telephony user connection should be assigned to the subscriber "Richard" in the incoming direction. Outgoing dialing/voice should be possible for up to two simultaneous connections. STUN support should be activated in the HiPath 3000 system (STUN client).

In addition, HiPath 3000 voice subscribers should receive a "low cost" rate for making calls to the USA. An Internet telephony user connection (MSN basis) with individual registration for calls in the direction of the ITSP sippgate should be used.

ITSP sippgate features:

- Internet telephony subscriber ID: <Subscriber ID>
- Authorization name: <Subscriber ID>
- Password: <Password>

- Call number: 0180xxxxxxx (Germany, not geographic -> local area network: 0180 national)

The NAT implementation of the upstream customer router should be checked.

The following STUN server is available from the ITSP:

- IP address/FQDN: stun.sipgate.net.
- Port: 3478



Interoperability between providers is crucial for the successful establishment and usage of Internet telephony features. Refer to the ITSP's general terms and conditions.

The current list of approved ITSPs can be found here:

http://wiki.siemens-enterprise.com/index.php/Collaboration_with_VoIP_Providers

2.9.2 Configuration in HiPath 3000 Manager E

Configure trunk groups (configuration example "sipgate")

1. Go to "Settings -> Lines / networking ..." and select the "Routes" tab.
2. In the "Routes" display field, select Trk Grp 13 for the second ITSP and seizure code "82" for establishing calls from the "Missed Calls List" and dialing Trk Grp 13 (sipgate) directly.



Trk Grp 13 must be used for the second ITSP, Trk Grp 14 for the third and Trk Grp 15 for the fourth ITSP. You can configure up to four ITSPs. Trk Grp 16 is used for IP networking.

3. Apply the settings.

Practical Examples for HG 1500

Adding Internet Telephony User Connections

Configure routing parameters

1. Go to "Settings > Lines / networking ..." and select the "Routing parameters" tab.
2. Activate the routing type "CO" under "Route type".
3. Activate "Unknown" under "No. and type, outgoing".
4. Activate the type "Internal" under "Callnumber type".
5. Apply the settings.

Configure special networking

1. Go to "Settings > Lines / networking ..." and select the "Special" tab.
2. Deactivate the "Always use DSP " switch under "Switches".
3. Apply the settings.

Add trunks

1. Go to "Settings > Lines/networking" and select the "IP Trunks" tab. Trunks are automatically assigned to the route.
2. In the "Number" field, define the number of trunks (e.g. 2, SIP Provider 2) that should be configured. When you click the "Add" button, the trunks appear in the corresponding display field.
3. Enable the gateway resources.
4. Apply the settings.

Configure trunks

1. Go to "Settings > Lines / networking ..." and select the "Trunks" tab.
2. In the "Route" column, click the relevant row to assign a route to a configured trunk. The last route should always be used for IP trunking.
3. In the "Code" column, configure a trunk code if, for example, the trunks are to be monitored and switched via the TAPI/CSTA.
4. Apply the settings.

Configure dial plan

1. Go to "Settings > Least cost routing" and select the "Dial plan" tab.
2. Add an individual dial rule to the "Caller List" for calls from the same local network (see examples below) so that the call is conducted via the SIP provider.
 - Sample SIP ISDN dial rule:

Codes and flags | Classes of service | **Dial plan** | LCR - schedule

Digit analysis wizard

	Name	Dialed digits	Route table	Acc. code	COS	Emergency
1	Standard	0CZ	2	No	yes	No
2	Standard	0CONZ	3	No	yes	No
3	Standard	0C01Z	3	No	yes	yes
4	Standard	81CZ	4	No	yes	yes
5	Standard	81C1Z	5	No	yes	yes

Route table: 2 | Dial rule wizard | Dialing rules table

	Route	Dial rule	min. COS	Schedule	Warning
1	QSC	2 SIP-ISDN	15	-	None
2	Sipgate	2 SIP-ISDN	15	-	None
3	ISDN	4 ISDN	1	-	None

- Sample dial rule fore SIP areas:

Codes and flags | Classes of service | **Dial plan** | LCR - schedule

Digit analysis wizard

	Name	Dialed digits	Route table	Acc. code	COS	Emergency
1	Standard	0CZ	2	No	yes	No
2	Standard	0C1Z	3	No	yes	No
3	Standard	0C01Z	3	No	yes	yes
4	Standard	81CZ	4	No	yes	yes
5	Standard	81C1Z	5	No	yes	yes

Route table: 3 | Dial rule wizard | Dialing rules table

	Route	Dial rule	min. COS	Schedule	Warning
1	QSC	3 SIP-City	15	-	None
2	Sipgate	3 SIP-City	15	-	None
3	ISDN	4 ISDN	15	-	None

3. Apply the settings and load the data into the system.

2.9.3 Configuration via HG 1500 WBM

Add Internet telephony subscriber

1. Select:
"Explorers > Voice Gateway > SIP Provider > SIP Gate (> right click) > Add Internet Telephony Subscriber"
2. Enter the relevant parameters.

The screenshot shows the 'Voice Gateway' tree on the left with 'SIP' selected. A context menu is open over 'SIP Gate' with 'Add Internet Telephony Station' highlighted. On the right, the 'Internet telephony station' configuration window is displayed with the following fields:

- Internet telephony station: 1982112
- Authorization name: 1982112
- New Password: [masked]
- Confirm Password: [masked]

Buttons for 'Apply' and 'Undo' are visible at the bottom.



The "Internet Telephony Subscriber" and "Authorization Name" entries correspond to the subscriber names of the ITSP siggate.
The password corresponds to the subscriber password at the ITSP siggate.

Add MSN

1. Select:
"Explorers > Voice Gateway > SIP Provider > SIP Gate > 198... > MSN (> right click) > Add MSN"
2. Enter the relevant parameters.

The screenshot shows the 'Voice Gateway' tree on the left with 'Sipgate' selected. A context menu is open over '1982112' with 'Add MSN' highlighted. On the right, the 'Assignment Internet Telephony Phone Number to internal station' configuration window is displayed with the following fields:

- Internet Telephony Phone Number: 4918019933229311
- Internal Call Number: insert number directly (dropdown)
- insert number directly: 220
- Default Entry:

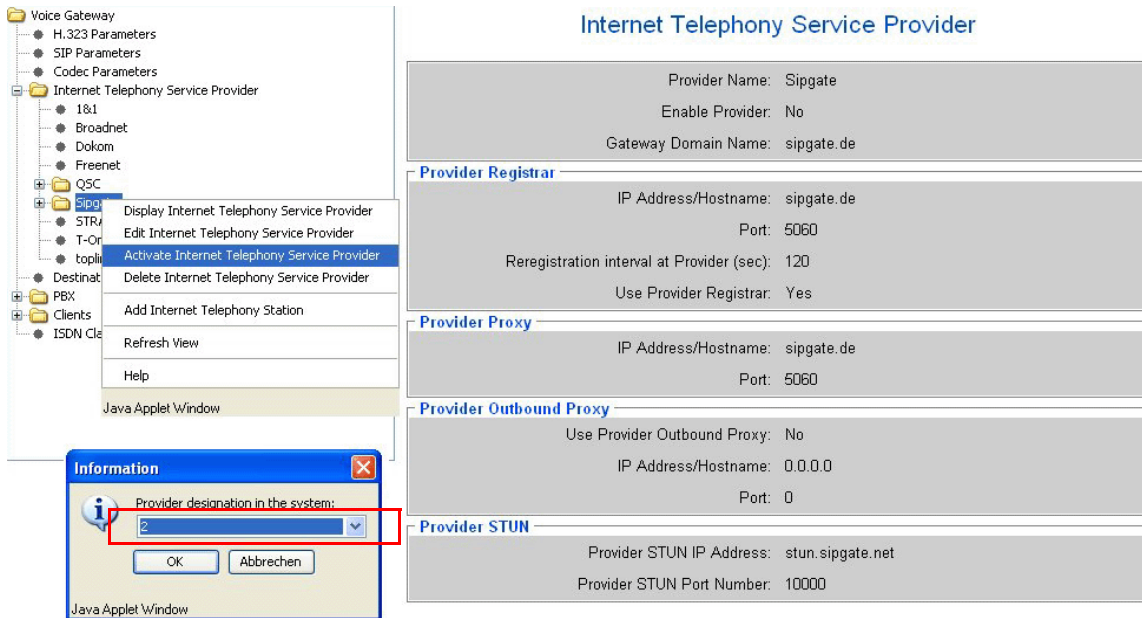


The format of the Internet telephony phone numbers may vary depending on the provider:

- Example siggate: 49xxxx (international)
- Example T-Online: 032xxx (national)

Activate SIP provider

1. Select:
"Explorers > Voice Gateway > SIP Provider > SIP Gate (> right click) > Activate SIP Provider > Information"
2. Enter the relevant parameters.



Configure STUN

1. Select:
"Explorers > Voice Gateway > SIP Provider (> right click) > Edit STUN Configuration"
2. Enter the relevant parameters under "STUN Configuration".



Notes on configuring the STUN mode: See Seite 2-38

2.9.4 Check Setup

Complete NAT detection for the upstream customer router is performed via the STUN client/server.

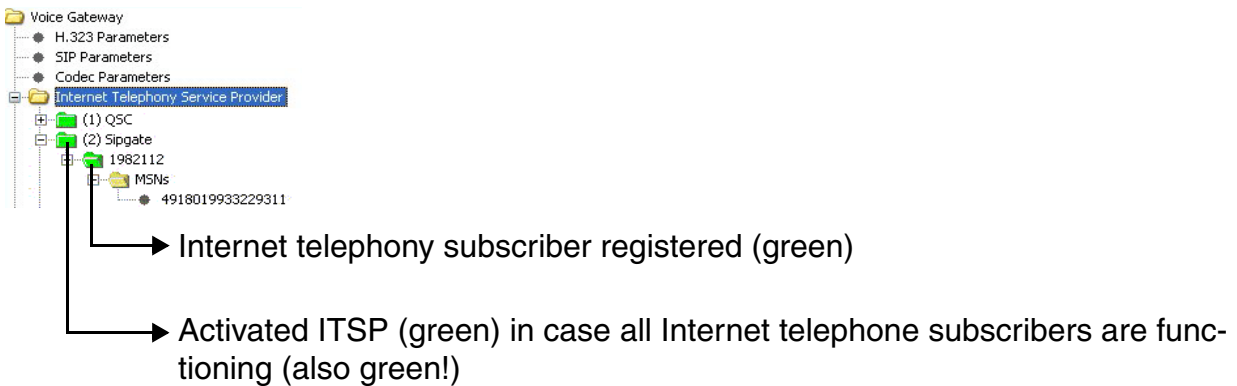
Detect NAT Type

1. Select:
 "Explorers > Voice Gateway > SIP Provider > Detect NAT Type"



Initial Setup Check

1. Select: "Explorers > Voice Gateway > SIP Provider > (2) SIP Gate > 198..."
2. Check the initial setup.



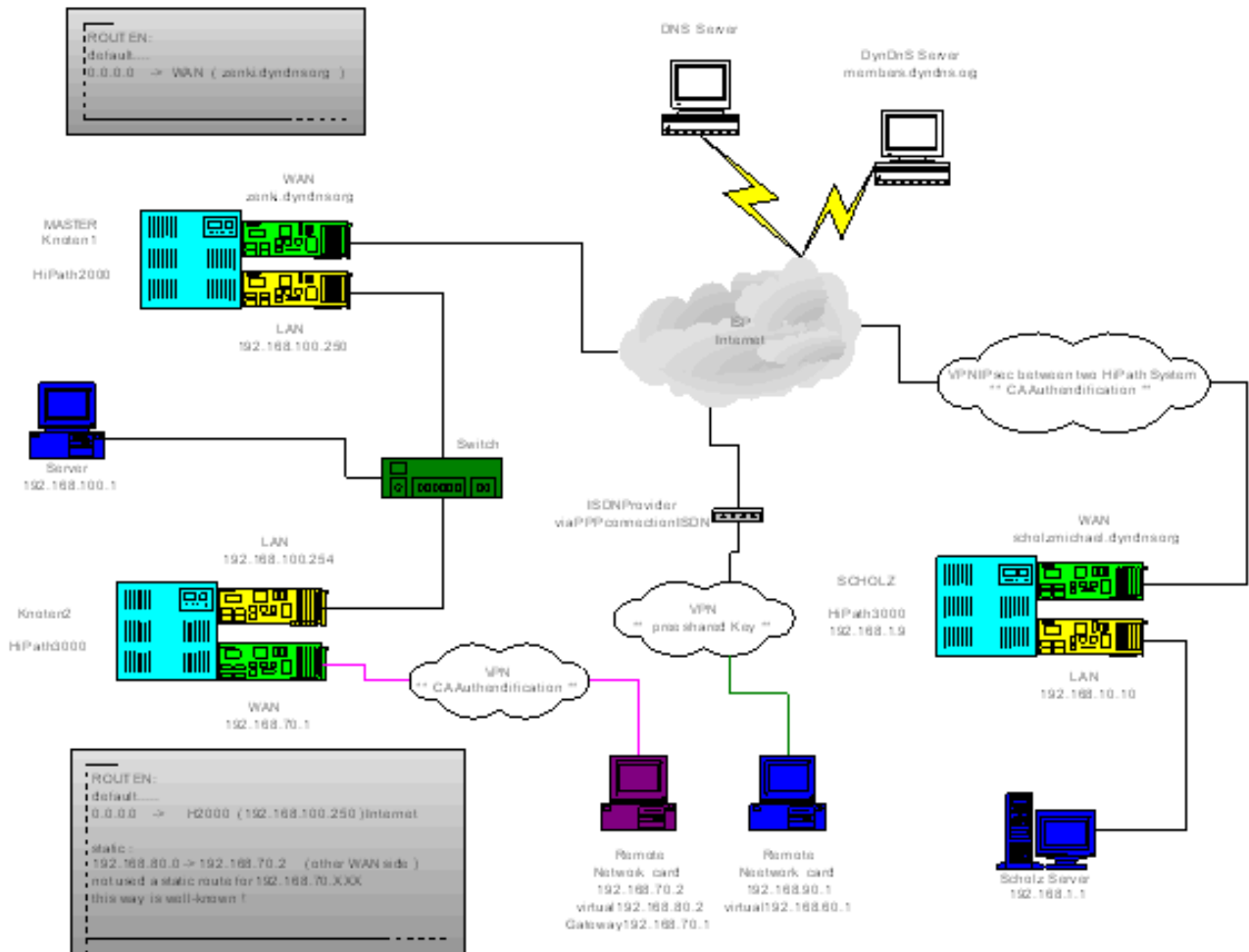
Folder status:

- Green: O.K.
- Yellow: Not activated/configured.
- Orange: Provider only.
 At least one of the Internet telephone subscribers failed.

2.10 HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

2.10.1 Target Configuration

A VPN remote client should be authenticated using digital signatures.



Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

Test configuration

In the test configuration, the various configurations of a VPN/IPsec connection between HiPath 2000/HiPath OpenOffice EE / HiPath 3000 V6.0 and a VPN remote client were tested.

The respective authentication was established with "Authentication with digital signatures" and "Pre-shared key" in different scenarios:

- HiPath 2000 / HiPath OpenOffice EE < --- > HiPath 3000 (DynDNS)
(dynDNS)
- HiPath 2000 / HiPath OpenOffice EE < --- > HiPath 2000 / HiPath OpenOffice EE fixed
(dynDNS) IP from the ISP
- HiPath 2000 / HiPath OpenOffice EE < --- > VPN client RDT dial-in to ISP
(dynDNS)
- HiPath 3000 WAN fixed IP < --- > VPN client connected to WAN H3000

Requisite licenses

The licenses required (IPsec/LWCA) must be available and activated.

The CA license is required so that a master can create a CA certificate once in the system network. The CA certificate created provides a basis for creating the other certificates (trusted CA / PEER / Denied nos. list). A CA license is not required for authentication with a pre-shared key; only the IPsec license is required in this case.

Example

In the example described, the HiPath 2000 / HiPath OpenOffice EE is considered to be the master, which creates and distributes the required CA certificate (Lightweight CA) for all HiPath systems and VPN clients networked via VPN.

Startup procedure

- Preparations / data backup for HiPath systems in operation
- Activate SSL Secure Access (via CLI)
- Create certificates for authentication with digital signatures
- Configure tunnel for VPN with corresponding authentication method
- Configure relevant services or apply the default
- Configure rules taking customer requirements into consideration
- Configure HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 dial rules / configure RSM 5000
- Install and configure the VPN remote client software
- Test using various authentication methods - trace and troubleshooting

2.10.2 Activate SSL Secure Access

A data backup should always be performed before switching the system to SSL (secure) mode.

Activate access

1. Reload the secure data in SSL mode via the WBM as the system only boots with the IP address after the command (reset secure) and the existing configuration rejects data.
2. Create an SSL certificate and activate SSL:

-CLI // get write access

-CLI // reset secure // system performs a reboot and starts in SSL mode

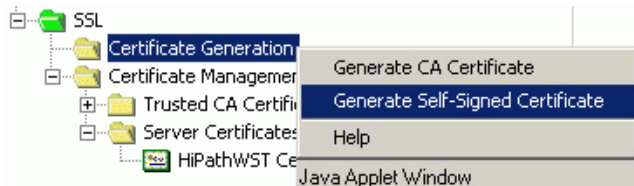
-CLI // generate your own SSL certificate for the IP address of the HXG

```
create ssl certificate hxg 1 "C=DE,O=local,OU=HXG,CN=192.168.1.10"
2005/01/01/00:00:00 2020/02/01/00:00:00
```



As SSL is activated by default on HiPath 2000 / HiPath OpenOffice EE, you can issue your own SSL certificate for your own IP address directly in the WBM. You can then activate this under SSL server certificates.

3. Issue your own SSL certificate for your own IP address.



4. Delete the existing certificate (Siemens certificate).

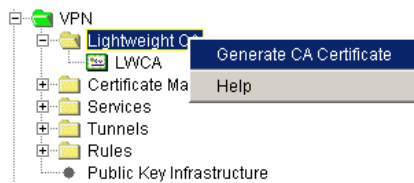
2.10.3 Create CA Certificates on the Master System

A CA certificate must only be created on the master system. All other HiPath systems or clients connected via VPN obtain the requisite certificates for authentication with digital signatures from the master.

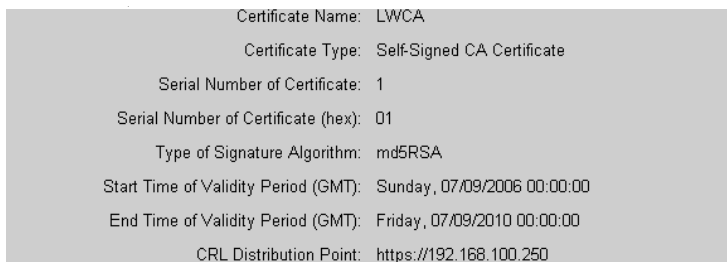
Create CA Certificates on the Master System

1. Select:

"Explorers > VPN > Lightweight CA > Generate CA Certificate".



You will obtain a CA certificate with serial number 1 that has been issued by the master:



Explanation: CRL Distribution Point = IP address of the HXG from the master system that created the CA certificates.

2. Change the public key length to 1536.

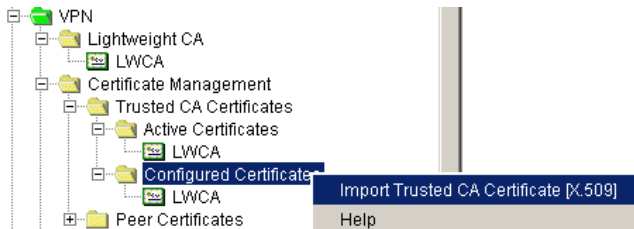
Type of Signature Algorithm:	md5RSA
Public Key Length:	1536
Issued by CA	
Country (C):	DE
Organization (O):	PRIVATE
Organization Unit (OU):	LOCAL
Common Name (CN):	LWCA
Subject Name	
Country (C):	DE
Organization (O):	PRIVATE
Organization Unit (OU):	LOCAL
Common Name (CN):	LWCA
Subject Alternative Name	
	192.168.100.250

Explanation: "Subject Alternative Name" is the IP address of the master HXG that issued the certificate.

- Go to "Explorers > VPN > LWCA" to export the certificate (X.509).

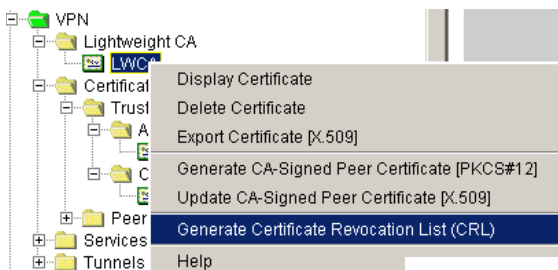


- Go to "Explorers > VPN > Certificate Management > Trusted CA Certificates" to re-import the certificate (X.509) back into your own (master) system and into the other systems.



This is also used for the VPN remote clients when "Authentication with digital signatures" is being used.

- Create the revocation lists associated with the certificate you have created.



Certificate Revocation List Information

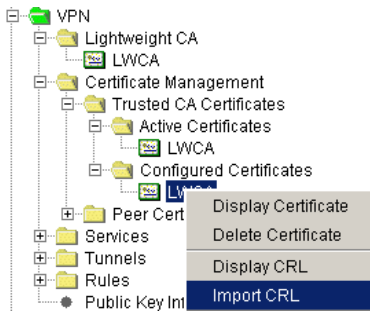
Certificate Name:			
Type of Signature Algorithm: md5RSA			
Timestamp of this CRL Update: Sunday, 07/09/2006 00:00:00			
Timestamp of next CRL Update: Monday, 07/09/2007 00:00:00			
Issued by CA			
Country (C): DE			
Organization (O): PRIVATE			
Organization Unit (OU): LOCAL			
Common Name (CN): LWCA			
List of the Certificates to be Revoked			
Serial Number of the Certificate	Serial Number of the Certificate (hex)	Revocation Time	Revocation Reason

The certificate revocation list (CRL) issued is imported into your own (master) system and into the other systems (Import CRL).

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

6. Import CRL



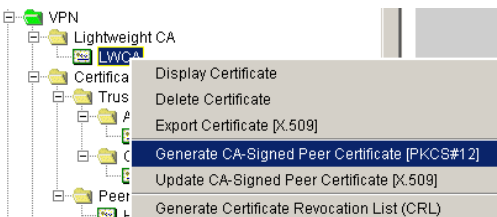
Revocation lists are not required for VPN remote clients.

Generate a PEER certificate

A PEER certificate (PKCS#12) is generated for every tunnel end point according to the tunnel configuration. The master generates this for itself and for every other involved system or the VPN remote client on the basis of the existing CA certificate.

For clarity, the names of the applicants should be used here:
"Subject Alternative Name" = Node 2 / Node 1 or VPN Client

1. Generate a peer certificate (PKCS#12).



2. Enter the relevant parameters.

Generate IPsec Peer Certificate

Passphrase for encryption:	<input type="text"/>
Reenter Passphrase for encryption:	<input type="text"/>
Serial Number of Certificate:	<input type="text"/>
Type of Signature Algorithm:	md5RSA
Public Key Length:	1536

Certificate Name:	H2000
Certificate Type:	CA-Signed Peer Certificate
Serial Number of Certificate:	1
Serial Number of Certificate (hex):	01
Type of Signature Algorithm:	md5RSA
Start Time of Validity Period (GMT):	Sunday, 07/09/2006 00:00:00
End Time of Validity Period (GMT):	Friday, 07/09/2010 00:00:00
CRL Distribution Point:	HTTPS://192.168.100.250

Issued by CA

Country (C):	DE
Organization (O):	PRIVATE
Organization Unit (OU):	LOCAL
Common Name (CN):	LWCA

Subject Name

Country (C):	DE
Organization (O):	PRIVATE
Organization Unit (OU):	LOCAL
Common Name (CN):	VPN

Explanation of input/specification for the peer certificate:

- **Passphrase for encryption**
If required, the master can also assign its own appropriate passwords or "passphrase for encryption" for each subject name (HiPath system / VPN remote client).
- **Serial number of certificate**
Serial number that should be assigned consecutively depending on the number of peer certificates issued.
- **Subject name**
Name of the relevant subject (Node X / VPN client).
- **Subject Alternative Name**
Name of the master that issued the CA.



Issued by CA and Subject Name must always be different in the peer certificate (different DN).

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

Generate a new peer certificate

A new peer certificate (PKCS#12) should be created for the other tunnel endpoint (HiPath 3000 node) and for a remote VPN client.

1. Go to "Explorers > VPN > LWCA" to generate a peer certificate.



2. Import the peer certificate created by the master with the relevant agreed password into the other tunnel endpoint (HiPath 3000 node) and enter the relevant parameters.

Generate IPsec Peer Certificate

Passphrase for encryption:	<input type="text"/>
Reenter Passphrase for encryption:	<input type="text"/>
Serial Number of Certificate:	<input type="text"/>
Type of Signature Algorithm:	md5RSA
Public Key Length:	1536

Explanation of input for peer certificate:

- **Passphrase for encryption**
If required, the master can also assign its own appropriate passwords or "passphrase for encryption" for each subject name (HiPath system / VPN remote client).
- **Serial number of certificate**
Serial number that should be assigned consecutively depending on the number of peer certificates issued.

The master has consequently created and distributed the relevant certificates, revocation lists, and peers. The relevant tunnel endpoints have imported the certificates created by the master and checked them using the fingerprint. This concludes certificate creation for "Authentication with digital signatures".

Configure and activate rules / services

Configuration of DynDNS and the default services and rules in the system is not dealt with in detail here. Services and rules are always configured on a customer-specific basis.

The rules, services and tunnels are always added first under the configured rules, services and tunnels, and are only actively loaded to the system via "Activate" after you have concluded configuration.



The first rule (Priority 1) described here guarantees the IP connections in your own subnet. This rule guarantees the IP traffic between all clients and systems in your own subnet 192.168.100.xxx if IPsec is activated.

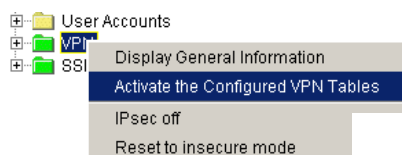
1. Go to "Explorers > VPN > Rules" to configure a rule.



Configured IPsec Rule

Priority:	1
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	No
Rule State:	Enabled
Source Address	
Type:	Subnet
IP Subnet Address:	192.168.100.0
Subnet Mask:	255.255.255.0
Destination Address	
Type:	Subnet
IP Subnet Address:	192.168.100.0
Subnet Mask:	255.255.255.0

2. Go to "Explorers > VPN" to activate the rule.



Active IPsec Rule

Priority:	6500
Service:	Any Service
Rule-Based Action:	DENY
Encryption Required:	No
Rule State:	Enabled
Source Address	
Type:	Host
IP Address:	0.0.0.0
Destination Address	
Type:	Host
IP Address:	0.0.0.0

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

If IPsec is activated, each IP packet runs through the configured rules in ascending order beginning with Priority 1. The activated rule (Priority 6500) guarantees that IP packets that not handled by a rule are rejected.



For security reasons, the last rule should always be activated (DENY).

If rules or services are configured and activated, you can begin configuring a VPN tunnel. You should perform a test beforehand using "ping" or "tracert" to check whether the desired destinations are still available.

2.10.4 HiPath 2000/HiPath OpenOffice EE to HiPath 3000 VPN Tunnel Configuration

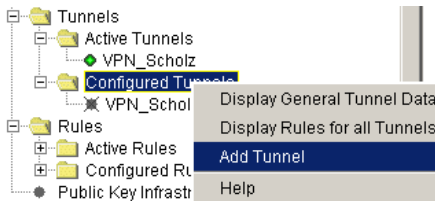
A VPN tunnel should be configured from a HiPath 2000 / HiPath OpenOffice EE to a HiPath 3000 that is set up for "Authentication with digital signatures".



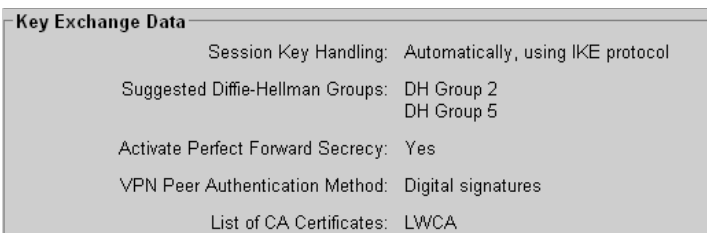
Tunnels are always added first under configured tunnels and are only actively loaded to the system via "Activate" after you have concluded configuration.

Configure VPN tunnels

1. Go to "Explorers > VPN > Tunnels" to configure a VPN tunnel.



2. Switch to Key Exchange Data.



3. Switch to Tunnel Data.

Active IPsec Tunnel

<input checked="" type="radio"/> Tunnel Data <input type="radio"/> Key Exchange Data	
General	
Name of the Tunnel:	VPN_Scholz
Type of the Local Tunnel Endpoint:	DNS Name
Local Tunnel Endpoint Address:	zenki.dyndns.org
Type of the Remote Tunnel Endpoint:	DNS Name
Remote Tunnel Endpoint Address:	scholzmichael.dyndns.org
Security	
Suggested Security Protocol:	ESP
Suggested Encryption Algorithms:	AES DES 3DES
Suggested Hash Algorithms:	MD5 SHA1
Session Key Handling:	Automatically, using IKE protocol
Suggested Lifetime of the Session Keys:	8 hours
Suggested Lifetime of the Key Exchange Session:	8 hours
Suggested Data Volume of the Session Keys:	unlimited

Explanation:

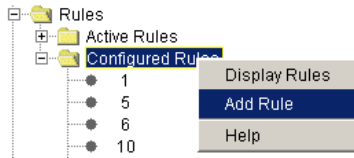
- Local Tunnel End Point Address
Local WAN Interface (zenki.dyndns.org).
- Remote Tunnel End Point Address
DynDNS name of the other WAN interface from the HiPath 3000 system (scholzmichael.dyndns.org).

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

Rule (Priority 100) VPN Tunnel between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000

1. Go to "Explorers > VPN > Rules" to create a rule.



Configured IPsec Rule

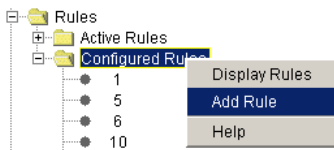
Priority:	100
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Rule State:	Enabled
Source Address	
Type:	Subnet
IP Subnet Address:	192.168.100.0
Subnet Mask:	255.255.255.0
Destination Address	
Type:	Subnet
IP Subnet Address:	192.168.1.0
Subnet Mask:	255.255.255.0
Tunnels for Encryption	
Tunnel on Receive Side:	No Tunnel Assignment
Tunnel on Transmit Side:	VPN_Scholz

Explanation: "Tunnel on Transmit Side" is the configured VPN Tunnel to the HiPath 3000.

Consequently only the other endpoint is entered. In the remote system only the "Tunnel on Transmit Side" is activated and entered via VPN.

If rule 100 is created, another rule for the opposite direction (from subnet 192.168.1.0 > 192.168.100.0) is added to it in order to handle the incoming packets from this subnet as well.

2. Go to "Explorers > VPN > Rules" to add one rule to another.



The configured services, rules or tunnels must be activated once they have been successfully configured.

2.10.5 Rules, Services, General

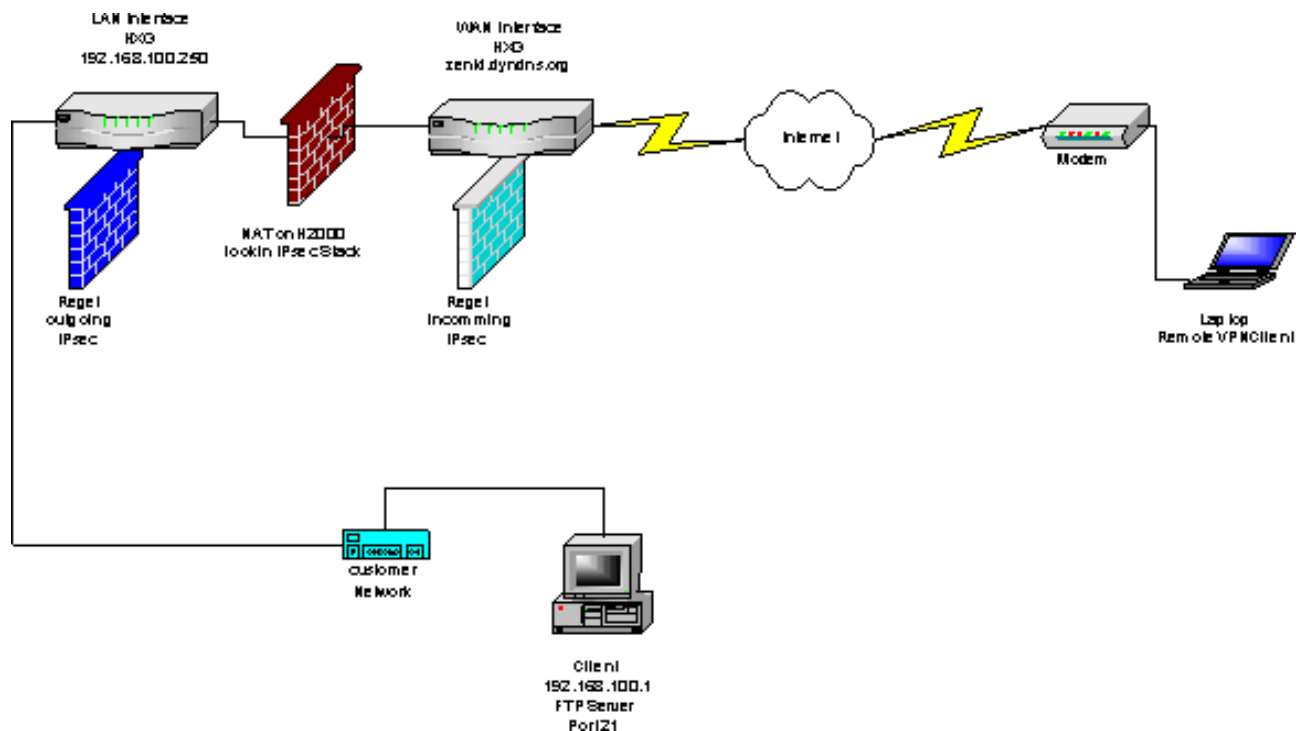
This overview is intended to simplify the "Creation" rule.

The following example is intended to illustrate how the IP packets run through the rules and the criteria they use to do this when IPsec is activated. You must always see the IP packet with the source IP and the destination IP. On the basis of the source and destination, the rules are processed and handled on the WAN and the LAN interface of the HXG.

The rules are always processed from the lowest to the highest priority. If an appropriate rule is found for an IP packet, it is used. The sequence of the rules for subnet or host must be considered in accordance with the priorities.

Example

If an IP packet reaches the WAN interface, it will have the DNS name "zenki.dyndns.org" as the destination and any host as a source IP (0.0.0.0).



2.10.6 Tracing, Troubleshooting and Checking the Configuration

The configuration should be checked for errors.

1. Go to "Maintenance > Traces" to start troubleshooting and to obtain trace information (trace profile).

Trace Profile: VPN_DynDNS

Profile Name: VPN_DynDNS
Profile is Read-Only: Yes
Start Profile: Yes

Trace Component	Level
DYNDNS_NRT	6
EVTLOG	3
IPSEC	7
PPP_STACK_DBG_IF	3
PPP_STACK_PROC	6
PPPM_TBAS	3
PPPOE_DBG_IF	6
PPPOE_PROC	3
SECURITY_SVC	9

2. Select "Maintenance > Appl. Diagnostics" to diagnose an application.

The screenshot shows the 'Maintenance' menu on the left with 'Appl. Diagnostics' circled in red. The main content area displays a tree view of diagnostic categories:

- MSC Trace: MSC API Trace
- MSC Loop: MSC Loop-Test Functions
- MSC DMC: MSC DMC-Test Functions
- MSC QDC: MSC QDC-Test Functions
- MSC SRTCP: MSC SRTCP-Test Functions
- MSC Misc.: MSC Miscellaneous
- IPSEC Show: IPSEC Show Routines
 - ipsecCMCaCertShow(void)
 - ipsecCMPeerCertShow(void)
 - ipsecCMCrIShow(void)
 - ipsecPMRulesShow(void)
 - ipsecPMTunnelsShow(rule_ID)
 - ipsecPMTunnelTableShow(void)
 - ipsecPMIfsShow(void)
 - ipsecPMServiceTableShow(void)
 - ipsecPMDnsNamesShow(void)
 - ipsecGlobalStatsValuesShow(void)
- IPSEC Test: IPSEC Test Routines
 - NRT-Msg: INTERNET_DISCONNECTED
 - NRT-Msg: IPSEC_INTERNET_CONNECTED
 - NRT-Msg: RESOLVE_NAMES
 - NRT-Msg: NRT_TIMER_EXPIRED
 - Nrt-Msg: DNS_UPDATE_TIMER

2.10.7 Configuring a VPN Remote Client on the HiPath 2000/ HiPath OpenOffice EE

A VPN remote client should be configured on the HiPath 2000 / HiPath OpenOffice EE (PPP via ISDN on an ISP) with a pre-shared key.

Starting basis

- The VPN remote client should be available via the IP address 192.168.60.1 from the internal subnet 192.168.100.0.
- The VPN remote client must be located in another subnet so that the packets are routed from the HXG via the VPN tunnel to the VPN client. It must therefore have another IP address that is not located in its own subnet.
- In the example, the IP address 192.168.60.1 is used for the VPN remote client.

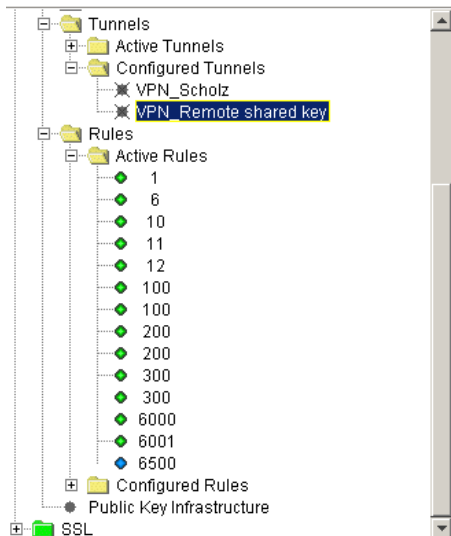
Rules

Since the connection between the VPN client and the HXG is established via a dynamic IP address assigned by the Internet Provider, two rules are required here:

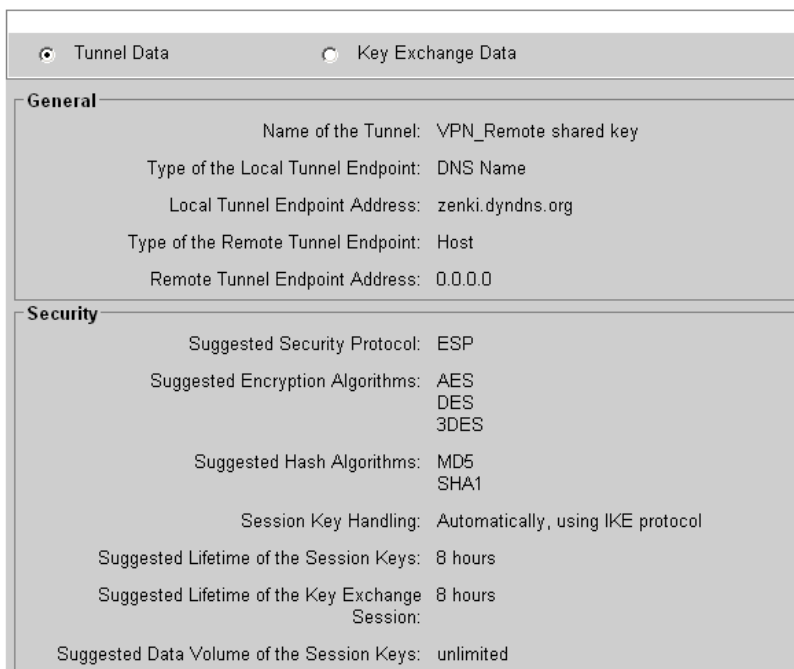
- Rule 200:
VPN Remote Client uses "dynam. IP" from the Internet Provider (Host 0.0.0.0) and negotiates both tunnel configuration and authentication.
- Rule 300: with counter rule
The VPN client has the IP address 192.168.60.1 and unrestricted access to the internal IP subnet 192.168.100.0.

Configure VPN remote client

1. Select:
"Explorers > VPN > Tunnels"

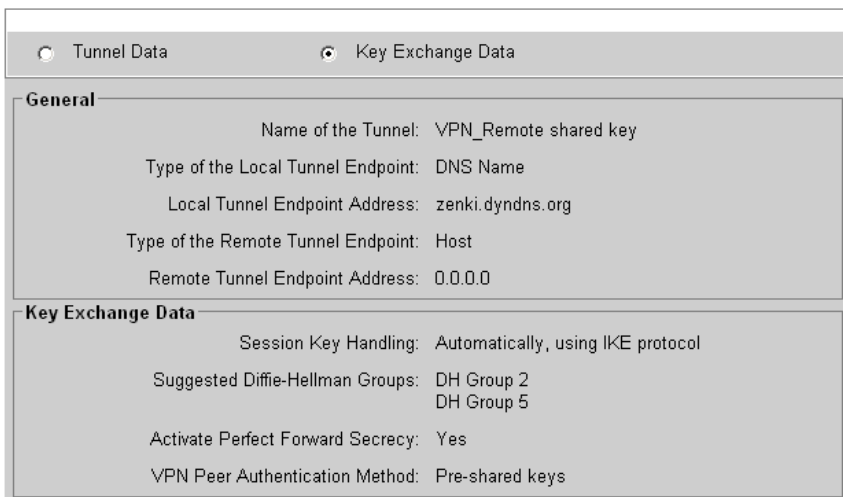


Configured IPsec Tunnel



2. Switch to Key Exchange Data.

Configured IPsec Tunnel



3. Switch to Tunnel Data.

Active IPsec Tunnel

<input checked="" type="radio"/> Tunnel Data <input type="radio"/> Key Exchange Data	
General	
Name of the Tunnel:	VPN_Scholz
Type of the Local Tunnel Endpoint:	DNS Name
Local Tunnel Endpoint Address:	zenki.dyndns.org
Type of the Remote Tunnel Endpoint:	DNS Name
Remote Tunnel Endpoint Address:	scholzmichael.dyndns.org
Security	
Suggested Security Protocol:	ESP
Suggested Encryption Algorithms:	AES DES 3DES
Suggested Hash Algorithms:	MD5 SHA1
Session Key Handling:	Automatically, using IKE protocol
Suggested Lifetime of the Session Keys:	8 hours
Suggested Lifetime of the Key Exchange Session:	8 hours
Suggested Data Volume of the Session Keys:	unlimited

Overview

The list below provides an overview of the relevant rules for the remote VPN:

200	Host	0.0.0.0	--	Subnet	192.168.100.0	VPN_Remote shared key	No Tunnel Assignment
300	Subnet	192.168.100.0	255.255.255.0	Subnet	192.168.60.0	No Tunnel Assignment	VPN_Remote shared key
300	Subnet	192.168.60.0	255.255.255.0	Subnet	192.168.100.0	VPN_Remote shared key	No Tunnel Assignment

2.10.8 VPN Remote Client Software

An IPsec VPN Client 3.1 is used as test software. The Sentinel VPN Client has been taken off the market and does not support W 2003 servers.

A different VPN client that was easy to configure was used; This VPN client can be found at:

http://www.thegreenbow.com/vpn_down.html

2.10.9 VPN Client Configuration for Tunnel with HiPath 2000

The target configuration involves configuring a VPN client for the tunnel with HiPath 2000 (PPP via ISDN on an ISP). We will explain the installation and configuration of a VPN client using "VPN NCP Secure Entry Client" as an example. Proceed as follows:

Installing the NCP Secure Entry Client software

1. Start the file `Setup.exe`. A window is displayed where you can select the installation language.
2. Make your selection from the list provided and click **OK**. An information window is displayed where the name and the version of the software to be installed are indicated.
3. Click **Next**. An important message is displayed: Ensure that neither a VPN client nor a personal firewall from another manufacturer are installed on your computer. This does not apply for Microsoft products.
4. To continue the installation, click **Yes**. The license agreement is displayed.
5. Read the license agreement. If you agree with it, click **Yes**. The installation begins and the window "Setup Type" is displayed.
6. Proceed as follows in the "Setup Type" window:
 1. Select the option "Typical".
 2. Click **Browse** and set the installation path.
 3. Click **Next**. The "InstallShield Wizard Complete" window is displayed once the software has been successfully installed.
7. You must restart your computer in order to use the installed program. Select "Yes, I want to restart my computer now" and click **Finish**. The computer is restarted.

Establishing a test connection without a certificate

The Initial Configuration Assistant automatically starts once you restart the computer and the "Create test connections" window appears.

1. Select the check box "Test connections should be made" and click **Next**. The "Select certificate type" window is displayed.
2. Select the option "Do not use a certificate" and click **Next**. The "Test connection finished" window is displayed.
3. Select the test connection that you would like to test and click **Test**. The "NCP Secure Entry Client" is displayed.
4. Click **Connect**. The selected test connection is tested.

If the connection is successful, a green display is shown along with the message "Connection has been established". Technical data for the connection are also shown.

5. Click **Disconnect**.

Configuring a personal VPN connection with a pre-shared key

1. Select **Configuration** -> **Profile Settings** in the "NCP Secure Entry Client" application. The "Profile Settings" window is displayed with the available profiles.
2. To create a new profile, click **New Entry**. The wizard for creating a new profile starts and the "Basic Settings" window is displayed.
3. Select the option "Link to Corporate Network using IPSec" and click **Next**. The "Connection Name" window is displayed.
4. Enter a unique name for the profile or the personal VPN connection and click **Next**. The "Link type (Dial up configuration)" window is displayed.
5. Select the connection medium, e.g. "LAN (over IP)" or "Modem". Click **Next**. The "VPN gateway parameters" window is displayed.
6. In the "Gateway" entry field, enter the DNS name or the IP address of the VPN gateway. Click **Next**. The "IPSec General Settings" window is displayed.
7. Proceed as follows in the "IPSec General Settings" window:
 1. Select **Main Mode** in the "Exch. mode" selection window and **None** in the "PFS group" selection window.
 2. Clear the check box "Use IP compression".
 3. Click **Next**. The "IPSec Configuration - Pre-Shared Key" window is displayed.

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

8. If you do not use certificates for authentication, a shared key is required for data encryption. Enter the pre-shared key and the local identity. Click **Next**. The "IPSec Configuration - IP Addresses" window is displayed.
9. Select **Manual IP address** in the "IP Address Assignment" selection window and enter your teleworker IP address data. Click **Next**. The "Link Firewall" window is displayed.
10. Select **off** in the "Enable Stateful Inspection" selection window and select the check box "Enable NetBIOS over IP". Click **Finish**. The "Profile Settings" window reappears. It contains the newly-configured profile.
11. Click **OK**. The "NCP Secure Entry Client" is displayed again.
12. Click **Connect** to test the VPN connection. The connection is tested.

If the connection is successful, a green display is shown along with the message "Connection has been established". Technical data for the connection are also shown.

13. Click **Disconnect**.

Linking certificates

1. Select **Configuration -> Certificates** in the "NCP Secure Entry Client" application. The "Certificates" window is displayed.
2. Proceed as follows in the "User Certificate" tab:
 1. Select **from PKCS#12 File** as the certificate type in the "Certificate" selection list.
 2. Set the path in the "PKCS#12 File Name" entry field. The default path is *<Inst-Dir>\NCP\SecureClient\CaCert*.
3. Click **OK** to save your entries.

Clearing "Use pre-shared key"

1. Select **Configuration -> Profile Settings** in the "NCP Secure Entry Client" application. The "Profile Settings" window is displayed with the available profiles.
2. Select the personal VPN connection you just created in the "Available Profiles" display field and click **Configure**.
3. The "Profile Settings *<personal VPN connection>*" window is displayed.
4. Select **Identities** in the selection window. To the right of the window area, the identity settings are displayed.
5. Clear the check box "Use pre-shared key".
6. Click **OK**. The window is closed.

Testing a personal VPN connection with a certificate

1. Start the "NCP Secure Entry Client".
2. Select the personal VPN connection you have configured in the "Profiles" selection list and click **Connect**. The "Enter PIN" window is displayed.
3. Enter the PIN for the certificate and click **OK**. The connection is tested.

If the connection is successful, a green display is shown along with the message "Connection has been established". Technical data for the connection are also shown.

Practical Examples for HG 1500

HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

2.10.10 Tunnel VPN client configuration with HiPath 2000/HiPath OpenOffice EE

The target configuration involves configuring a VPN client for the tunnel with HiPath 2000 / HiPath OpenOffice EE (PPP via ISDN on an ISP). We will explain the installation and configuration of a VPN client using "VPN NCP Secure Entry Client" as an example. Proceed as follows:

Starting basis

- In the test configuration, the remote client was connected directly with the HiPath 3000 WAN interface using a cross-over cable.
- The IP address of the network card on the remote client is 192.168.70.2.
- The IP address of the HiPath 3000 WAN interface is 192.168.70.1.
- If a VPN tunnel connection is established, the VPN remote client should be available via the virtual IP address 192.168.80.2 from the subnet 192.168.200.xxx.

Configuration for the WAN (LAN2) interface

The WAN is configured as illustrated below:

LAN2

```
Interface Is Active: Yes
IP Address: 192.168.70.1
IP Netmask: 255.255.255.0
MAC Address : 08:00:06:8d:7f:99
Ethernet Link Mode: Auto
Max. Data Packet Size (Bytes): 1500
Network Address Translation: No
QoS Capability of Peer: Identical
Bandwidth Control for Voice Connections: No
Bandwidth of Connection (Kbps): 10000
Bandwidth Used for Voice/Fax (%): 80
IEEE802.1p/q Tagging: No
```

Only one static route is required for the subnet 192.168.80.0. A static route is not required for the subnet 192.168.70.0 as the HiPath 3000 system recognizes the WAN interface.

Static Route Table

Route Index	Route Name	Destination Network/Host	Destination Netmask	Route Gateway
2	VPN_Remote	192.168.80.0	255.255.255.0	192.168.70.2

HiPath 3000 tunnel configuration for the VPN remote client

The tunnel for the VPN remote client is configured as illustrated below:

Active IPsec Tunnel

<input checked="" type="radio"/> Tunnel Data		<input type="radio"/> Key Exchange Data	
General			
Name of the Tunnel:	VPN_WAN Remote		
Type of the Local Tunnel Endpoint:	Host		
Local Tunnel Endpoint Address:	192.168.70.1		
Type of the Remote Tunnel Endpoint:	Host		
Remote Tunnel Endpoint Address:	192.168.70.2		

HiPath 3000 rule configuration for the VPN remote client

The following rules are required for the VPN or network connection and for configuring the tunnel to the VPN remote client via the HiPath 3000 WAN interface.

Since the connection between the VPN client and the HXG is established via the WAN interface, two rules are required here:

- Rule 100:
VPN remote client uses 192.168.70.2. and negotiates both tunnel configuration and authentication.
- Rule 200: with counter rule
The VPN client has the IP address 192.168.80.2 and unrestricted access to the internal IP subnet 192.168.100.0.

Overview

The list below provides an overview of the relevant rules.

100	Subnet	192.168.70.0	255.255.255.0	Subnet	192.168.100.0	--	--
200	Subnet	192.168.100.0	255.255.255.0	Subnet	192.168.80.0	No Tunnel Assignment	VPN_WAN Remote
200	Subnet	192.168.80.0	255.255.255.0	Subnet	192.168.100.0	VPN_WAN Remote	No Tunnel Assignment

Practical Examples for HG 1500

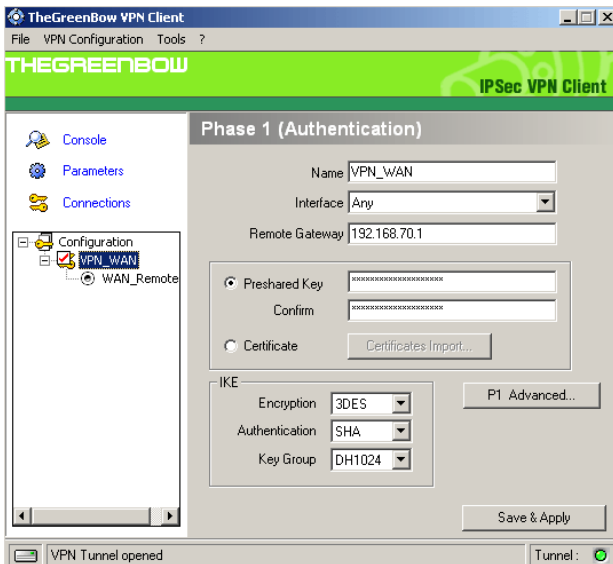
HiPath 2000 / HiPath OpenOffice EE / HiPath 3000 VPN Remote Client - Authentication

2.10.11 VPN Client Configuration for Tunnel with HiPath 3000

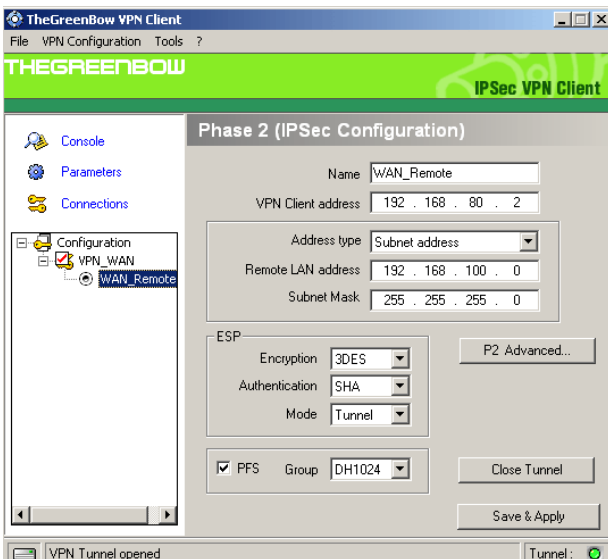
A VPN client should be configured with a pre-shared key for the HiPath 3000 tunnel (cross-over directly to WAN).

Configure a VPN client

1. Select: "Configuration > VPN_WAN"



2. Enter and store the relevant parameters.
3. Select: "Configuration > WAN_Remote"

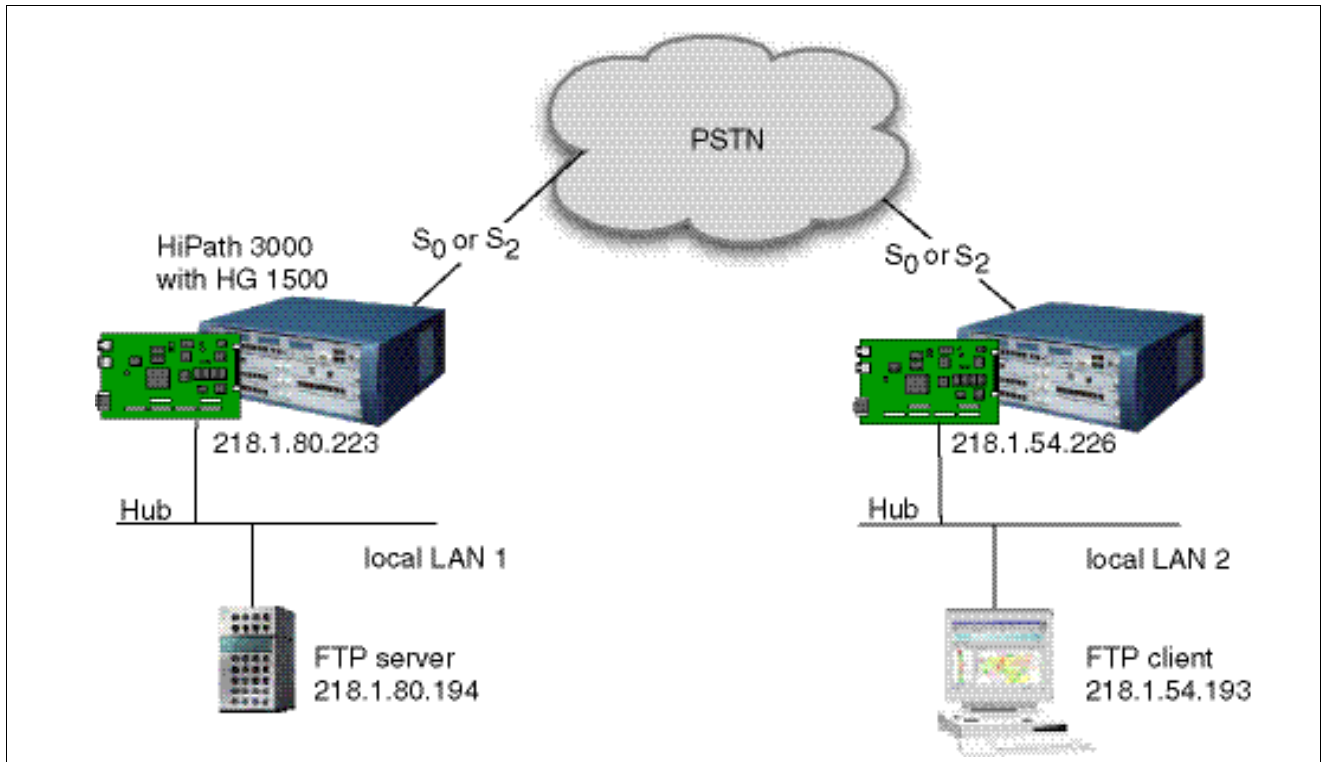


4. Enter and store the relevant parameters.

2.11 ISDN-Based Connection Between LANs

2.11.1 Target Configuration

In this configuration, two local LANs (LAN1 and LAN2) are connected to each other via PPP. The HG 1500 boards are the terminals of the PPP connection.



2.11.2 Configuration Steps

HiPath 3000 Manager E

1. Set the parameters for lines/networking of the LAN1 HiPath.
2. Set the parameters for the subscribers on the LAN2 HiPath.
3. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM browser

1. Suppress the use of a proxy server for the IP addresses that are used in both LANs.

Settings in WBM for both HG 1500 boards used

1. Insert a PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > (right-click) Add PSTN Peer".
2. Add a station number for the new PSTN peer.
3. Add a static route that replaces the default gateway of the bootline.
4. Save the settings.

PC settings

1. Enter the IP address of the first HG 1500 board as the default gateway for the TCP/IP Internet protocol used in the first LAN's PC.
2. Configure a route for the first HG 1500 board.

2.12 Firewall Functionality (Authorization Firewall)

2.12.1 Target Configuration

The firewall functions as a barrier to protect against unauthorized access. In this case, the internal LAN (LAN1), for example, is to be protected against external access such as Internet-based access via DSL.

The objective of this configuration is to allow individual, specified computers to access an insecure network (e.g. Internet). At the same time, it prevents access in the reverse direction (from the Internet to these computers). The board features two different protection mechanisms for implementing this security.

The firewall in this security function is a so-called authorization firewall. In other words, as soon as the function is activated, only configured components can access board services. All board services are automatically denied to unregistered LAN components.



WARNING: The activation and deactivation of IP and MAC filters may severely restrict the functionality of the board (for example LAN-based administration may not be possible any more) or may enable access to sensitive data.

Firewall functionality comprises the following two steps:

- IP routing authorization

IP filters can give individual IP addresses or groups of addresses access to specific destinations. (For the sake of simplicity, the following description only speaks of a single IP address, but entire networks can also be released.)

This too is an authorization list, that is only IP addresses that are listed here are assigned access to the defined service(s). The IP filter can check IP protocols and the associated services (port numbers).

- MAC verification

The MAC verification procedure checks whether IP packets transferred from the LAN interface are valid in relation to their IP address and MAC address combination.

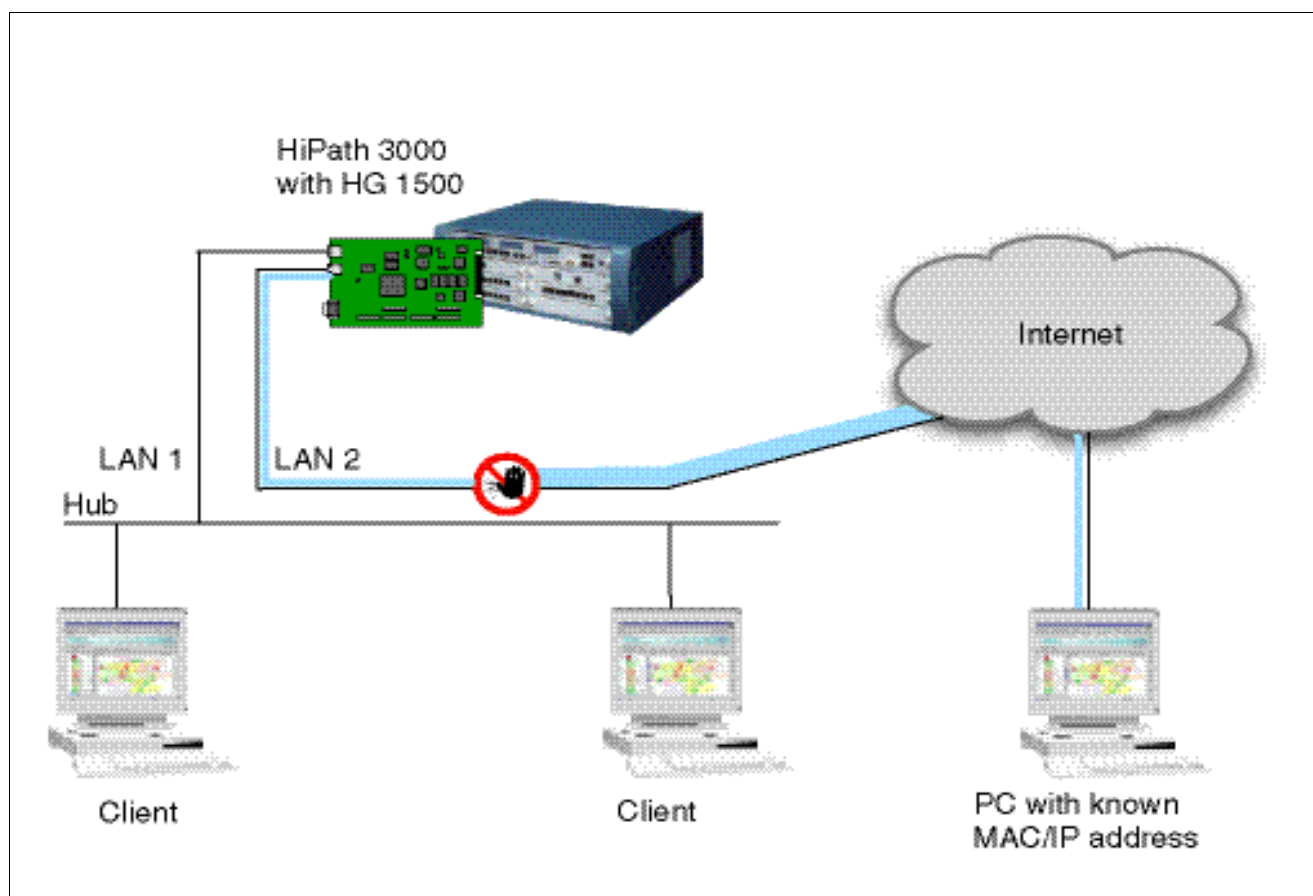
The protection here lies in the fact that MAC addresses are permanently assigned to a network interface and cannot be configured. This method **cannot**, however, restrict the Internet services that can be used.



The MAC address filter must **not** be enabled if the LAN 2 interface is used for PPPoE connections (for example, DSL).

Practical Examples for HG 1500

Firewall Functionality (Authorization Firewall)



Prerequisites

- To be able to define an exact selection of the required function, you must know not only the destination IP address, but (where applicable) also the authorizing protocol and the port number.
- To configure MAC verification, you need a list of the MAC and IP address combinations of the installed LAN cards which are to be granted access to the board services. You will find the MAC addresses in the documentation provided by your Ethernet card manufacturer.

2.12.2 Configuration Steps for IP Filter

WBM Settings

1. In WBM, go to "Explorers", select "Security" and then select the function "Add Rule for IP Address Filtering".
2. First enter the upper and lower limits of the outbox address field. The filtering rule only permits packets containing IP addresses with sender addresses that originate in a defined area.
3. In this field, determine the IP address to which the permitted packets should be sent. If you enter 0.0.0.0 and 255.255.255.255, packets may be sent to all IP addresses.
4. Enter the accepted IP protocol and the permitted port number. For ICMP protocols, you can also restrict the ICMP type and the ICMP code.



Please note that for some Internet protocols, multiple port numbers must be released in order to be able to use the appropriate Internet service (e.g. FTP port 20 and 21).

5. Enable the "Activate Rule" function and click "Apply".
6. Repeat this step to configure additional filter rules.
7. Save the settings.



To disable, edit or delete an existing IP filtering rule, please refer to the relevant description in the Administration Manual, "IP Address Filtering".

2.12.3 Configuration Steps for MAC Filter

WBM Settings

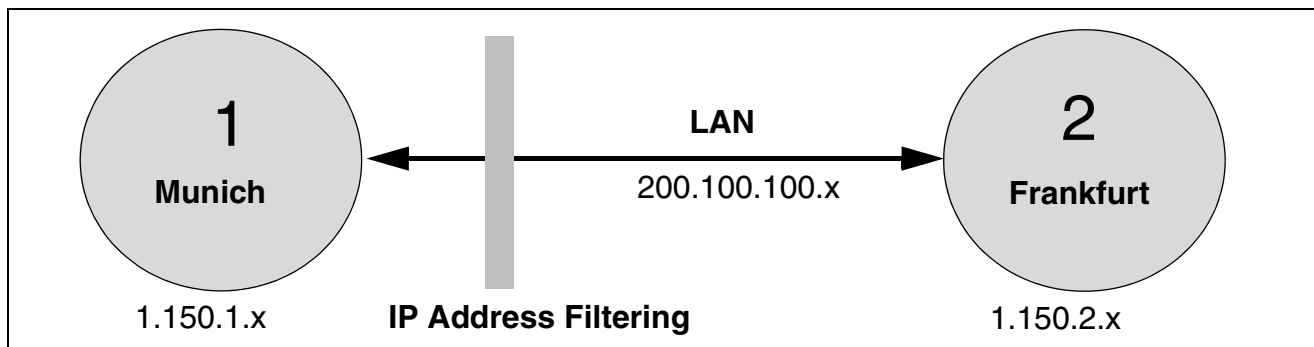
1. Enter the IP and MAC addresses to which you want to grant access rights.
2. Enable the "Activate Rule" function and click "Apply".
3. Repeat the first two steps for all IP/MAC address combinations for which you want to configure a filter rule.
4. Save the settings.

2.13 IP Firewall

The following example is based on the Administration Manual, "LAN-LAN Routing". The example shows the system in Munich (server) with the system in Frankfurt (client).

2.13.1 Target Configuration

A local telnet server is to be configured on a PC belonging to the system in Munich. Testing is to be carried out to determine whether access from the system in Frankfurt to the telnet server of the system in Munich is possible via the LAN-LAN routing. The IP firewall should then be configured so that the telnet server on the PC belonging to the system in Munich can only be accessed by the PC with the IP address 1.150.102.10. The IP firewall should then be configured so that only UDP protocols are possible with all ports. Testing should then be carried out to determine whether the telnet connection is still possible.

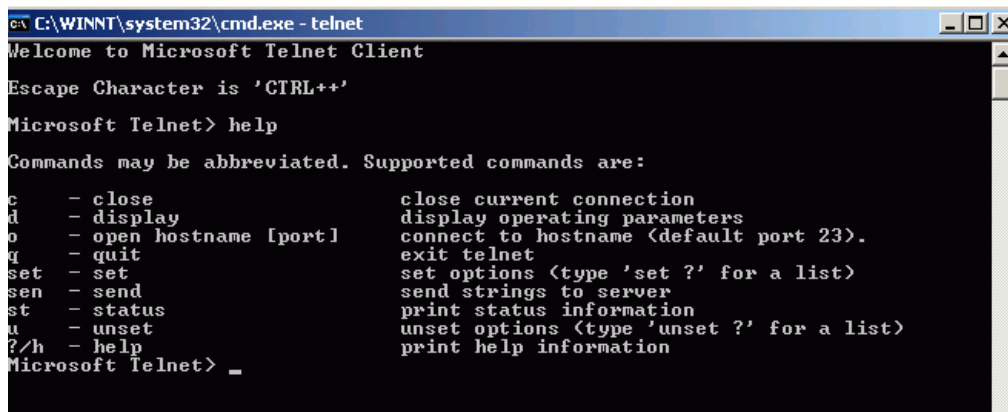


2.13.2 Configuration Steps

Configure and check telnet

1. Configure a local telnet server on a PC belonging to the Munich system. The service can be started by calling "tlntadm.exe".

In an MS-DOS window, call the "tlntadm.exe" service and start it with the option "4) Start Service".

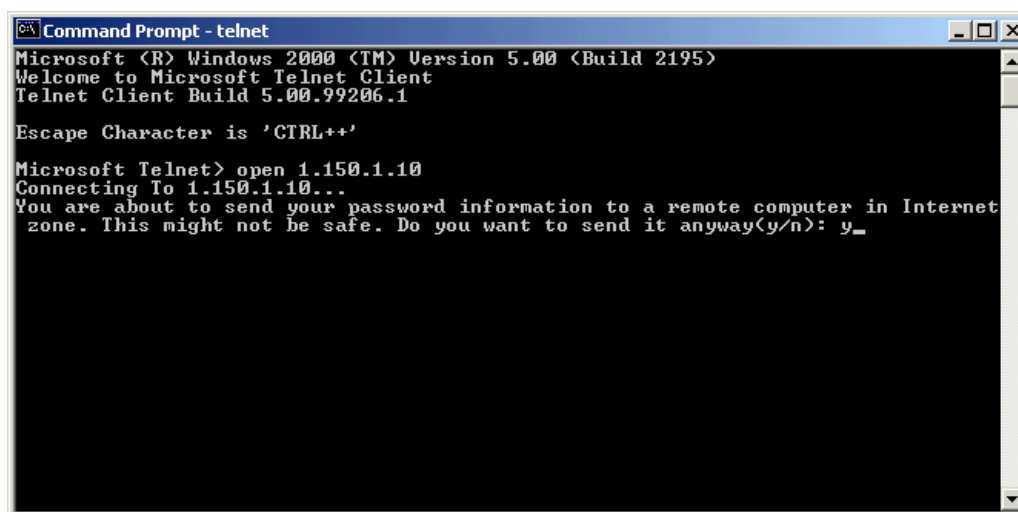


```
Microsoft Windows [Version 5.00.99206.1]
(c) 1999 Microsoft Corporation. All rights reserved.

C:\WINNT\system32\cmd.exe - telnet
Welcome to Microsoft Telnet Client
Escape Character is 'CTRL++'
Microsoft Telnet> help
Commands may be abbreviated. Supported commands are:
c      - close                close current connection
d      - display              display operating parameters
o      - open hostname [port] connect to hostname (default port 23).
q      - quit                 exit telnet
set    - set                  set options (type 'set ?' for a list)
sen    - send                 send strings to server
st     - status               print status information
u      - unset                unset options (type 'unset ?' for a list)
?/h   - help                  print help information
Microsoft Telnet> _
```

2. Check whether access from the system in Frankfurt to the telnet server of the system in Munich is possible via the LAN-LAN routing.

Open an MS-DOS window on the PC belonging to the system in Frankfurt and enter the parameter "telnet".

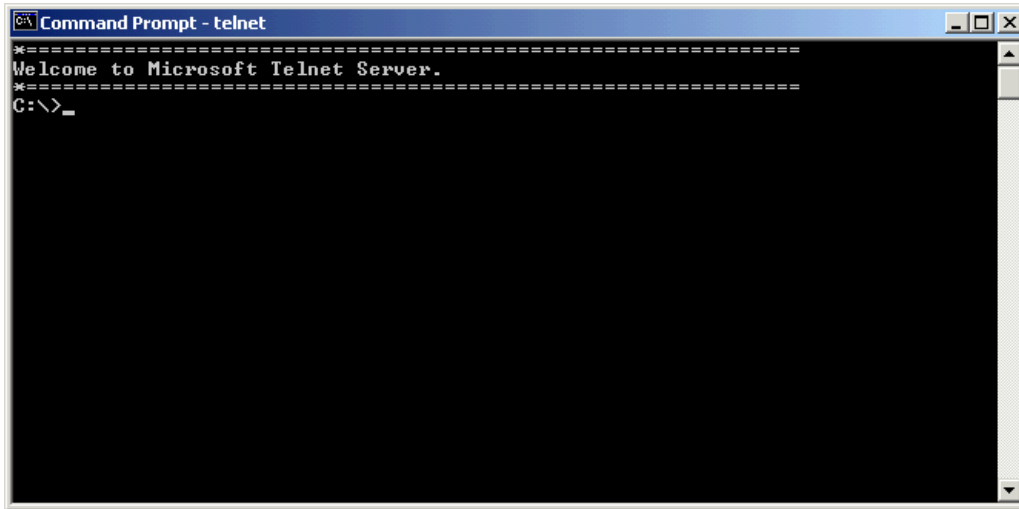


```
Microsoft Windows [Version 5.00.99206.1]
(c) 1999 Microsoft Corporation. All rights reserved.

Command Prompt - telnet
Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Client
Telnet Client Build 5.00.99206.1
Escape Character is 'CTRL++'
Microsoft Telnet> open 1.150.1.10
Connecting To 1.150.1.10...
You are about to send your password information to a remote computer in Internet
zone. This might not be safe. Do you want to send it anyway(y/n): y_
```

Practical Examples for HG 1500

IP Firewall



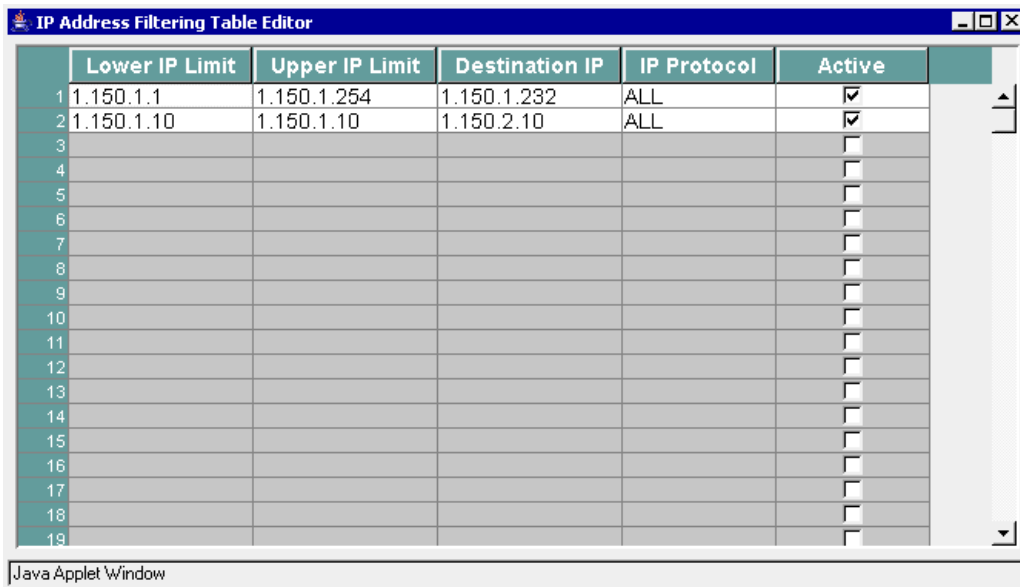
You can view the contents of the "C:\\" directory on the PC belonging to the system in Munich with the "dir" command.

Configuring an IP Firewall Using WBM

1. Configure firewall entries in the form of IP address filters using the WBM of the HG 1500.

You can use the table editor for IP address filtering for this purpose:


"Explorers > Security > IP Address Filtering > (right-click) IP Address Filtering Table Editor".



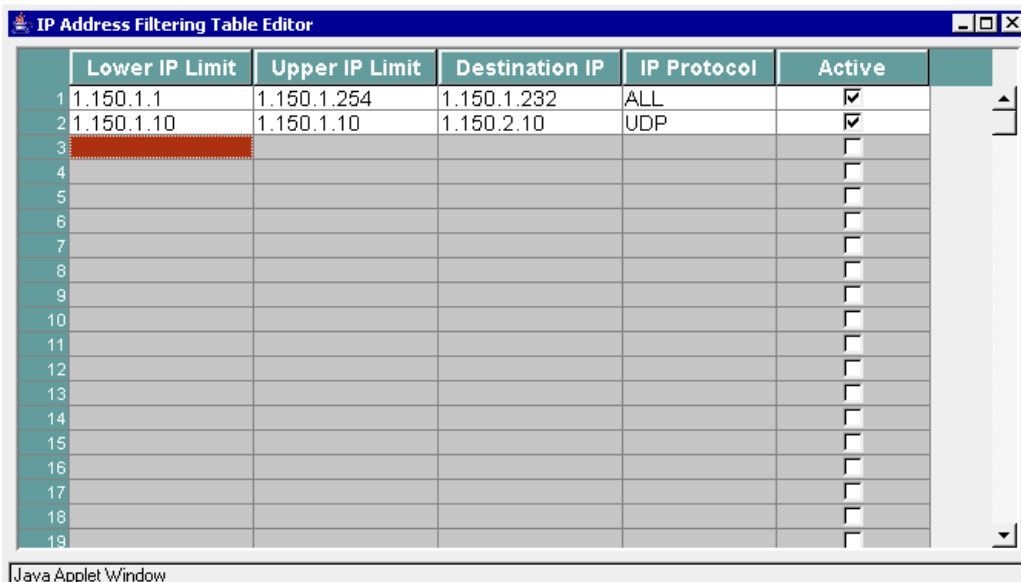
	Lower IP Limit	Upper IP Limit	Destination IP	IP Protocol	Active
1	1.150.1.1	1.150.1.254	1.150.1.232	ALL	<input checked="" type="checkbox"/>
2	1.150.1.10	1.150.1.10	1.150.2.10	ALL	<input checked="" type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>
17					<input type="checkbox"/>
18					<input type="checkbox"/>
19					<input type="checkbox"/>

The entry in row 1 is required so that a PC from the local network can access the HG 1500. The entry in row 2 describes the route of the APP from group 1 to the APP in group 2.

- Exit the table editor and then activate IP address filtering for the HG 1500 with "Explorers > Security > IP Address Filtering > (right-click) Enable IP Address Filtering".

 If you find yourself "locked out" due to an incorrect firewall configuration, you can disable the configured firewall at any time using the CLI parameter "disable firewall".

- Now edit the IP firewall so that only UDP protocols are possible with all ports. You can once again use the table editor for IP address filtering.



	Lower IP Limit	Upper IP Limit	Destination IP	IP Protocol	Active
1	1.150.1.1	1.150.1.254	1.150.1.232	ALL	<input checked="" type="checkbox"/>
2	1.150.1.10	1.150.1.10	1.150.2.10	UDP	<input checked="" type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>
17					<input type="checkbox"/>
18					<input type="checkbox"/>
19					<input type="checkbox"/>

You can set "UDP" in the "IP Protocol" column.

- Test whether the telnet connection is still functioning.

You will discover that a connection from the system in Frankfurt to the system in Munich via telnet is no longer possible, as the TCP/IP or ICMP protocol used for this purpose is no longer released.

2.14 Call-By-Call Internet Connection

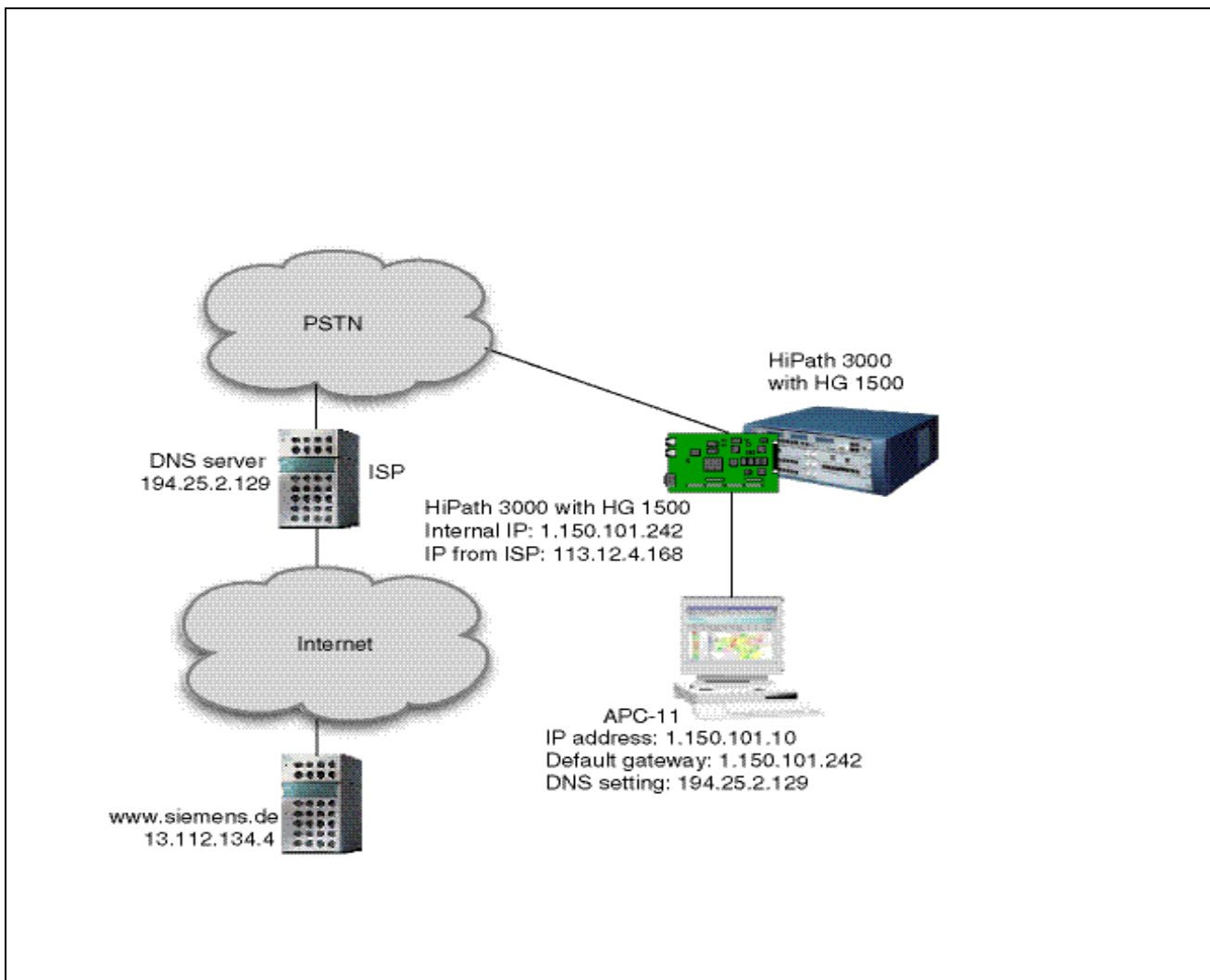
2.14.1 Target Configuration

Internet access should be set up via a call-by-call provider for all PCs in the LAN. You want to use two B channels that can be dynamically set up and cleared down for the connection if possible. The upper threshold for the second B channel should be 80% for 15 seconds, the lower threshold should be 60% for 10 seconds.

Short hold should be activated and clear down the connection after 60 seconds if no data is transferred on the line.

Short hold charge pulse analysis should not be performed.

The router call number for HiPath 3000 is 199.



Prerequisites

- The service provider (ISP) must enable two B channels to be set up for the Internet connection.

Function

- The PC forwards the request `www.siemens.de` to the DNS. The name of the IP address is resolved here (in the present example: 13.112.134.4).

- The PC forms the four address elements:

Source: 1.150.101.10 Port: 1024 PC
destination: Port: 80 www.siemens.de
13.112.134.4

- Since the IP address destination of the PC making the request cannot respond, the four address elements are converted within the HG 1500.

Source: 113.12.4.168 Port: 1025 IP address of the service provider
destination: Port: 80 www.siemens.de
13.112.134.4

- In HG 1500, a table with the following information is created for connection:

Port 1025 belongs to: 1.150.101.10 with port 1024 PC

- If a packet is sent back from the Internet, the HG 1500 can send the data to the correct PC in the LAN.

2.14.2 Configuration Steps

HiPath 3000 Manager E

1. Configure the router call number 199 as the S_0 subscriber for the HG 1500 board. Ensure that only one station number "no port/no access" can be configured on the correct HG 1500 (slot) and that this number is also subject to dial monitoring and the LCR tables.
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

1. Insert a PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > (right-click) Add PSTN Peer".
2. Enter an administrative name under "Peer Name".
3. Apply the default settings in the area "IP Parameters". However, activate the option "Negotiate IP Address".

Practical Examples for HG 1500

Call-By-Call Internet Connection

4. Change the default values in the "General PPP Parameters" section as follows:
Select the entry "Default Router/Internet" under "PSTN Connection Type" so that requests that cannot be processed by HG 1500 are forwarded to the default router (in this case to the Internet connection).
Enter 2 for "B Channels" if the service provider supports this function.
5. Activate "Short Hold". Enter 60 for "Short Hold Time (sec)". Deactivate "Short Hold Charge Pulse Analysis". The short hold activated automatically clears down the connection if no data has been transferred for 60 seconds.
6. Activate "PPP Authentication". Select the entry "PAP Client" under "PAP Authentication Mode". Enter the user name under "PPP User Name" and the password for call-by-call access under "PAP Password".
7. Activate "Multi-Link". Do not change the default values for channel allocation and segmentation. Enter 80 for "Upper Multi-Link Threshold (%)", 15 for "Upper Multi-Link Time Limit (sec)", 60 for "Lower Multi-Link Threshold (%)", and 10 for "Lower Multi-Link Time Limit (sec)".
8. Save the settings.
9. Edit the global PSTN data:
"Explorers > Routing > PSTN > (right-click) Edit Global PSTN Data".
10. Select 199 for "Pause between Redial Attempts (sec)". Enter 5 for "Number of Redial Attempts" and "Router Call Number". The fields in the "Scripting" section remain blank.
11. Save the settings.

PC settings for call-by-call access

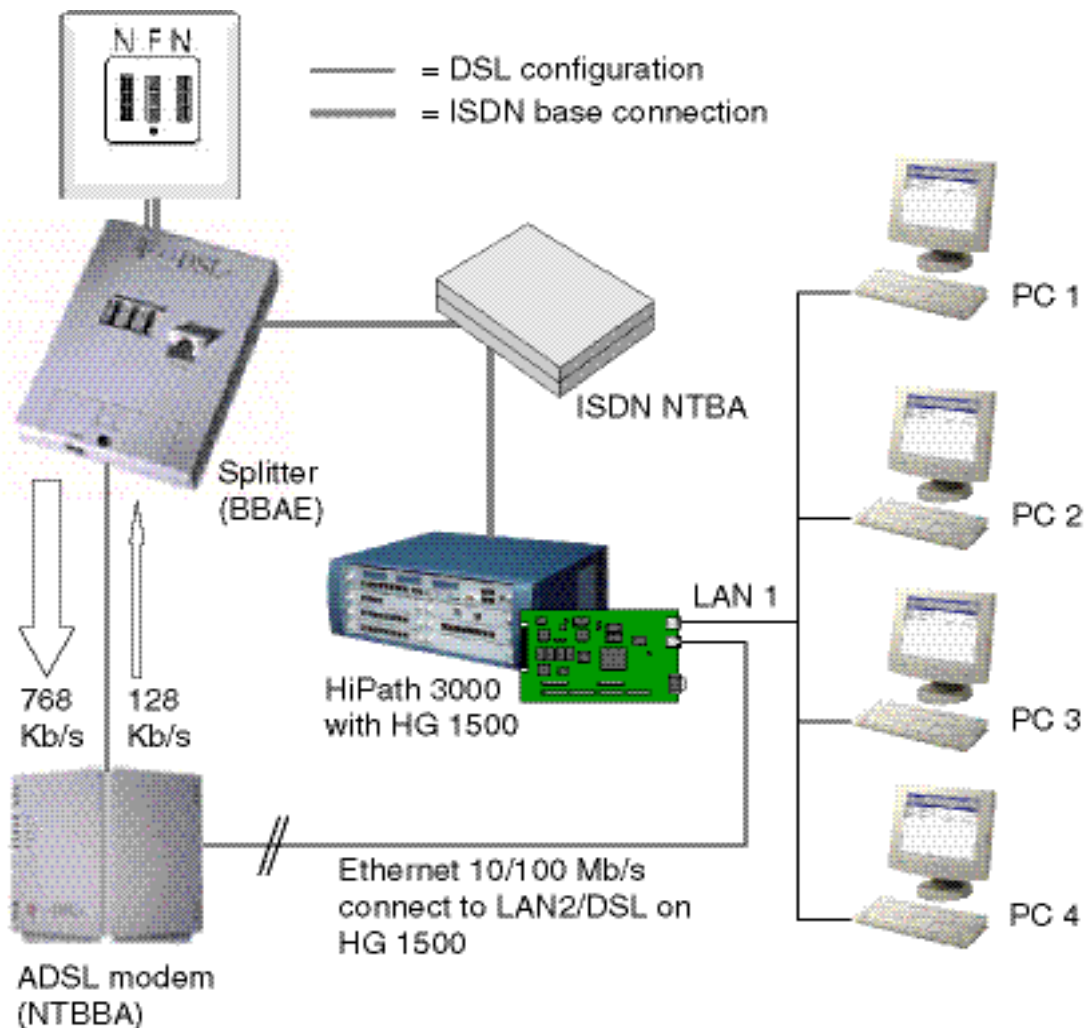
1. In the TCP/IP Internet protocol settings, specify the IP address of the service provider under DNS and enter the IP address of the HG 1500 as the default gateway.
2. You can specify a proxy server if one is offered by your service provider (in MS Internet Explorer: "Tools > Internet Options > Connections > Settings > 'Proxy Server' section").

2.15 ISP Access over ADSL

2.15.1 Target Configuration

In this configuration, a client PC connected to the local LAN1 can access the Internet over HiPath 3000. In the example, the Internet connection is set up by an ISDN/DSL access from Deutsche Telekom.

Both the terminal adapter (NTBA) of the ISDN base connection and the ADSL modem are connected to the HiPath 3000. The DSL modem is connected to the HG 1500 LAN2/DLS interface. The NTBA and ADSL modem are both connected to the splitter (BBAE). The splitter is connected to the Deutsche Telekom TAE line jack unit.



Restrictions

- Maximum one DSL connection is possible.

Practical Examples for HG 1500

ISP Access over ADSL

Prerequisites

- In the RJ45 jacks on the splitter and ADSL modem, only pins 4 and 5 (UKA'a and UKA'b) are used for transmitting DSL signals. You need a two-wire connection cable.
- You must not use a crossover cable between the ADSL modem and HG 1500. The pin assignment on the DSL modem's RJ45 jack is as follows:
 - Pin 1 = RX+ (plus pin for receipt),
 - Pin 2 = RX- (minus pin for receipt),
 - Pin 3 = TX+ (plus pin for transmission),
 - Pin 6 = TX- (minus pin for transmission).RX and TX are therefore transposed in comparison to the Ethernet standard. You need a 1:1 cable.

2.15.2 Configuration Steps

WBM Settings

1. Configure the LAN2 interface for DSL connections:
Explorers > Network Interfaces > (right-click) LAN2 > Edit LAN2 Interface.
2. Select *DSL Connection Type PPPoE*. Please note that a default gateway already configured with CLI or Boot CLI is overwritten by the addition of the DSL connection. Confirm the system message.
3. Apply the default settings in the area *General DSL Parameters*.
4. Activate *Short Hold*. Enter the value *180* under *Short Hold Time (sec.)*.
5. Activate *PPP Authentication*. Select the entry *PAP Client* under *PAP Authentication Mode*. Make an entry, such as *52009653544335467540001@t-online.de* under *PPP User Name*. For Deutsche Telekom DSL connections, the PPP user name consists of the connection ID, T-Online number, user and *@t-online.de*. Enter the password you received from Deutsche Telekom under *PAP Password*.
6. Activate *NAT Enabled*. The *Address Mapping Enabled* option must remain disabled.
7. Activate the two options *Default Router* and *Internet Access with DNS Request*.
8. Save the settings.

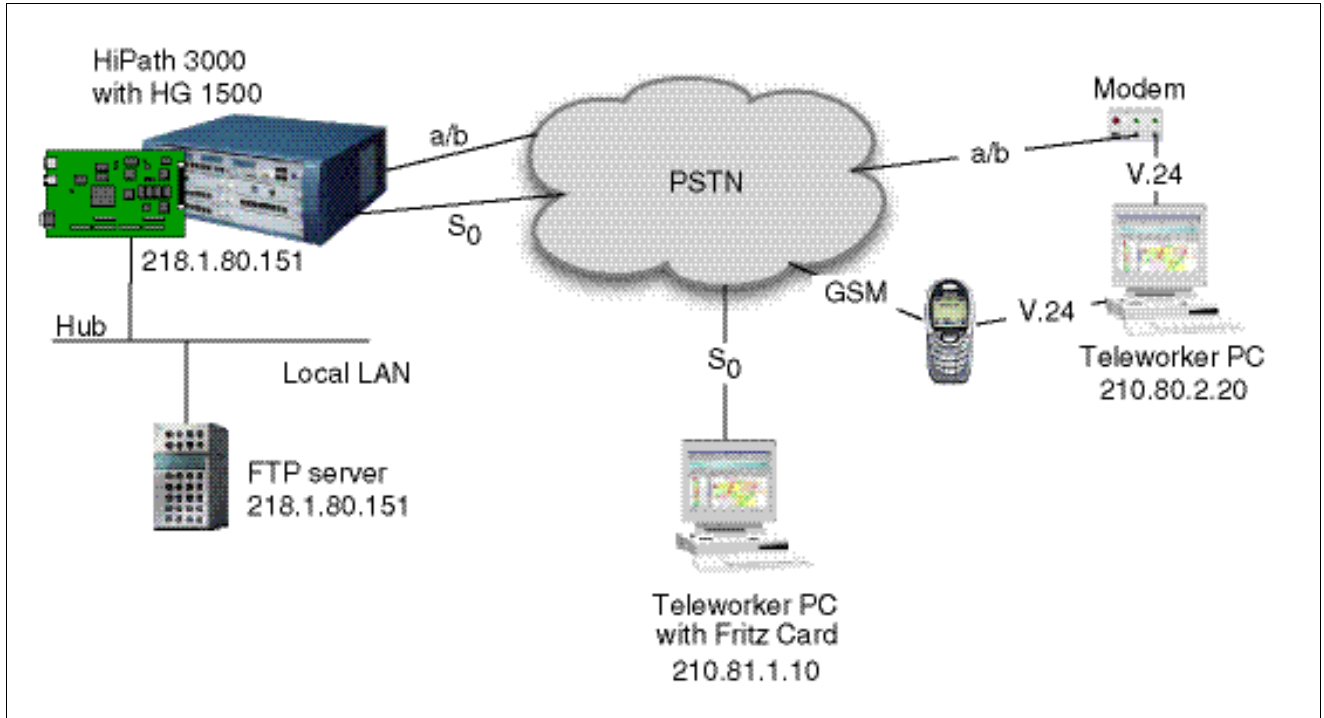
PC settings for ADSL access

1. In the TCP/IP Internet protocol settings, specify the DNS server's IP address assigned by T-Online (194.25.2.129) and enter the IP address of the HG 1500 as the default gateway.
2. You can also set the proxy server provided by T-Online in MS Internet Explorer: "*Tools > Internet Options > Connections > Settings > 'Proxy Server' section*". The address of the proxy server is *www-proxy.t-online.de*, port 80.

2.16 Teleworking via PPP (ISDN, Analog Modem, GSM)

2.16.1 Target Configuration

In this scenario, an external PC client can dial into the HiPath system and use the local LAN as if this PC were directly connected to the LAN. In this case the HG 1500 board is the terminal of the PPP connection.



Restrictions

- Channel bundling (Multilink) is not possible with an analog modem and GSM operation (only one B channel is available).

2.16.2 Settings for PPP Connection with Analog Modem or GSM

HiPath 3000 Manager E

1. Enter a station number for the connection with an analog modem.
2. Enter a DID number for the HG 1500 board.
3. Use HiPath 3000 Manager E to transfer the modified database back to the system.

Practical Examples for HG 1500

Teleworking via PPP (ISDN, Analog Modem, GSM)

WBM Settings

1. Insert a PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > (right-click) Add PSTN Peer".
The PSTN connection type is set to "Normal" for teleworking. Enter the IP address of the peer. The V.34 peer should be selected for the connection of analog modems, while the V.110 peer should be selected for connection via GSM. Script processing is only necessary in the case of Internet access. Multilink must not be activated in this scenario.
2. Add a station number for the new PSTN peer. The connection from the HXG3 to the PC client is set up with this station number.
3. Save the settings.

PC settings

1. Configure the network and dial-up connection in the PC. Enter the IP address that you already entered for the PSTN peer in WBM for the TCP/IP Internet protocol used.

2.16.3 Settings for PPP Connection with ISDN

HiPath 3000 Manager E

1. Set up a subscriber station for the HG 1500 board (e.g. subscriber 600).
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

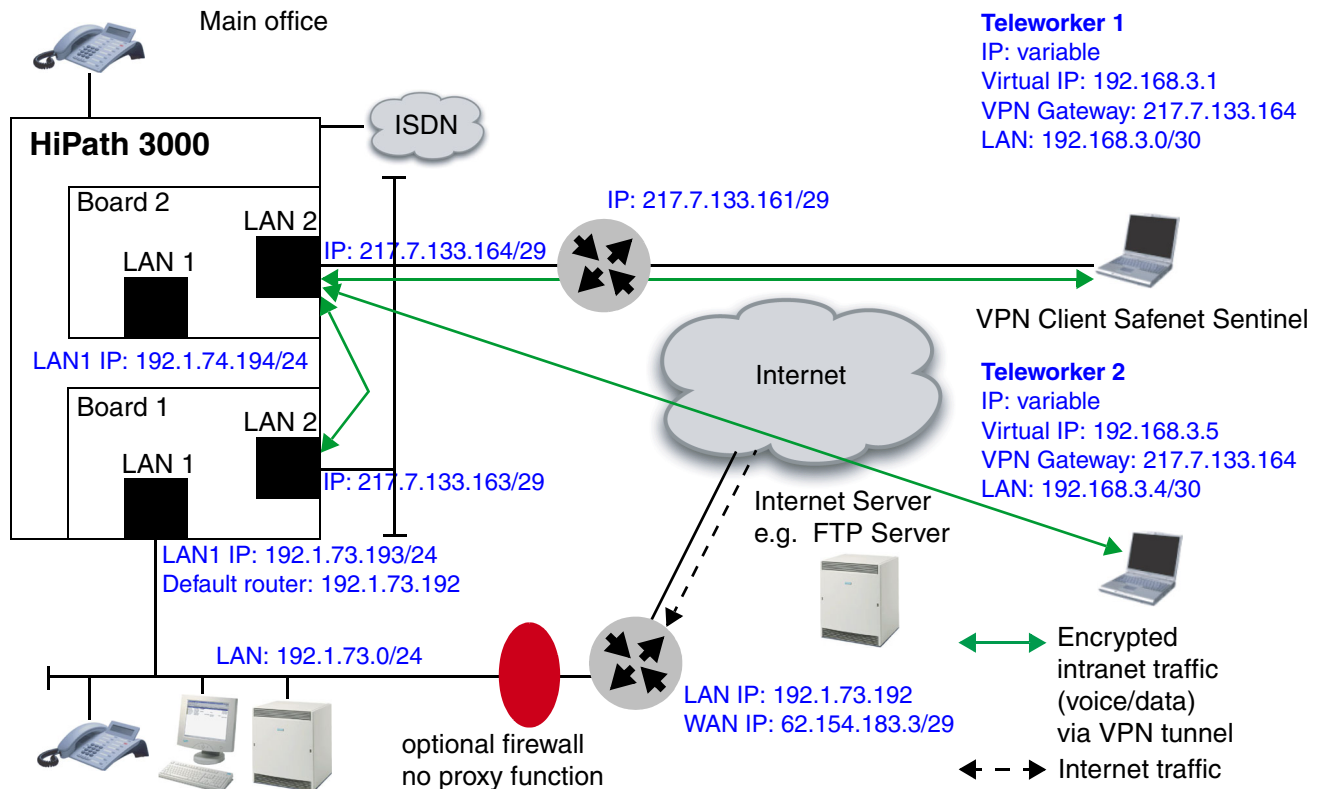
1. Insert a PSTN peer:
"Explorers > Routing > PSTN > PSTN Peers > (right-click) Add PSTN Peer".
The PSTN connection type is set to "Normal" for teleworking. Specify the IP address of the peer and enter the subscriber number of the board in the DID Number field (in our example: 600).
2. Add a station number for the new PSTN peer. The connection from the HXG3 to the PC client is set up with this station number.
3. Save the settings.

PC settings

1. Configure the network and dial-up connection in the PC. Enter the IP address that you already entered for the PSTN peer in WBM for the TCP/IP Internet protocol used.
2. Enter the parameters for the connection destination in the ISDN software used (for example NetwaysISDN).

2.17 Connecting Teleworkers when Using VPN and Firewall

The customer has a central Internet access protected by a proprietary firewall at the main office. This access is represented by the router with the IP 192.1.73.192 and should, for security reasons, also be used by teleworkers ("split tunneling" is not allowed). Two HG 1500 boards are required to combat the routing problem caused by this scenario (default router is in LAN1, Internet in LAN2).



2.17.1 Basic Requirements

Conditions for teleworkers

- A virtual IP address is configured for each teleworker on the SSH-Sentinel client. Each of these addresses must be located in a separate subnet as otherwise routing is not possible between the teleworkers.
- The teleworkers use the LAN2 interface on the teleworker HG (board 2) as a VPN gateway.
- If the teleworkers are using the only IP phones in the network, the optiClient 130 is logged on at the teleworker HG (board 2). If there are more IP phones available in the LAN, the teleworker's optiClient 130 must be logged on at the routing HG (board 1).

Practical Examples for HG 1500

Connecting Teleworkers when Using VPN and Firewall

Conditions for the HG boards

- Both boards are connected to an Internet telephony connection via the LAN2 interface. As the use of ISP access routers with NAT involves too many restrictions, only scenarios without NAT are permitted on the access router. For this reason, the ISP must provide two additional fixed IP addresses which should be located in the same IP subnet.
- The IP of board 2's LAN1 interface must be located in a separate subnet that also differs from the customer LAN.
- Due to the IP address of LAN1, board 2 should not be the first HG in the system as this restricts access to the HIP interface.
- The default router for board 1 is the central Internet access in LAN1 (192.1.73.192).
- Static routes must be configured on board 1 for the virtual IP addresses of the teleworkers. In this case, the gateway is board 2's LAN2 interface.
- The default router for board 2 is the ISP access router.
- NAT can be deactivated on the LAN2 interfaces on HG 1500. This results in a slight increase in performance. The VPN rules must then be used to ensure that no unauthorized attempts are made to access the HG 1500 boards.

Bandwidth for DSL connections

- The total upstream data rate for all teleworkers (typically: number of teleworkers * 128 Kbps) to board 2 should not exceed the downstream data rate set by the Internet provider for the main location. The volume of data sent by board 1 should continue to never exceed the volume that can comfortably be received downstream by a teleworker (typically: 768 Kbps or 1024 Kbps). Otherwise, this can have a negative impact on voice quality. The HG bandwidth in the transmit direction may have to be restricted accordingly. This rule cannot be implemented for teleworkers that dial into the Internet over narrowband connections (for example, over ISDN), as otherwise the HG would have to be too heavily restricted.
- Except for payload switching and IP traffic between the teleworkers, board 2 does not need to control (restrict) bandwidth. All other IP traffic is sent by board 1 where it is assigned priority and limited. To simplify configuration, data/bulk traffic between teleworkers is ignored. Consequently, the default value (10,000 Kbps) can be left for board 2's LAN2 bandwidth.

VPN rules

- Note that for VPN rules, "more precise" rules must have higher priority than "non-specific" rules.
- The VPN rules specify that the address entry "Host = 0.0.0.0" must not be used to send data. An address range should always be used in this case (for example, "Range = 0.0.0.1 - 255.255.255.254").

Central Internet access

- The central Internet access (here 192.1.73.192) is used by the local computers in LAN1 as the default router.
- Static routes must be configured on this router for the virtual IP addresses of the teleworkers and for board 2's LAN1. These static routes indicate the routing HG (board 1). This routing can also be performed by another router (for example, board 1).

Digital signatures

- Digital signatures (certificates) should be used for authentication in the teleworker tunnel. This is because individual certificates can be blocked which is not the case for pre-shared keys.
- Each teleworker receives an individual certificate with a unique serial number for authentication. Proceed as described in the HG 1500 Configuration Manual to create certificates with lightweight CA.

2.17.2 "Routing HG" Configuration (Board 1)

Network interfaces

1. Enter the LAN1 IP address. 192.1.73.193/24
2. Enter the LAN2 IP address. 217.7.133.163/29
3. Activate NAT only if required (NAT offers enhanced security even when IPsec is deactivated).
4. Activate the bandwidth control.
5. Set the interface bandwidth on the basis of the Internet provider's maximum values available and the upstream calculation specified above. Deduct 5-10% from the calculated bandwidth. The reason for this is that the bandwidth is measured on board 1's LAN2 interface for DES encryption. Board 2's LAN2 uses AES encryption, however, for Internet transmission. For smaller IP packets (G.723/30 ms, for instance), DES requires approximately 10% less bandwidth than AES. For bigger IP packets, the bandwidth discrepancy is significantly lower (around 1%).

Practical Examples for HG 1500

Connecting Teleworkers when Using VPN and Firewall

Routing

Default router: Internet	Internet router via LAN1: 192.1.73.192	
Static route: Teleworker	Target network: 192.168.3.0/24	Gateway via LAN2: 217.7.133.164
Static route: Board 2	Target network: 192.1.74.0/24	Gateway via LAN2: 217.7.133.164

"Internal" VPN tunnel

- Board 1 communicates with board 2 over the "internal tunnel". If HG 1500's two LAN2 addresses are both located in the same subnet, the packets are routed locally over the switch and not over the Internet. As an exception to the rule, DES encryption should be used here for the "internal tunnel" specifically to relieve the teleworker HG. As the packets are not routed over the Internet, DES encryption poses no security risks.

Name:	Internal
Terminal Device:	Host: 217.7.133.164
Encryption algorithm:	DES
Session key validity period:	8 hours
VPN Peer Authentication:	any

VPN rules

- PASS rules for accessing HG 1500 and HIP over LAN1.
 Default settings:

Service: Any Service

Rule State: Enabled

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
1	PASS	No	Subnet	192.1.73.0	255.255.255.0	---	---

- Tunnel rule for IP packets from the customer LAN to Board 2's LAN1.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
5	PASS	Yes	Subnet	192.1.73.0	255.255.255.0	---	Internal
			Host	192.1.74.194	---		
5	PASS	Yes	Host	192.1.74.194	--	Internal	---
			Subnet	192.1.73.0	255.255.255.0		

- Tunnel rule for IP packets from the customer LAN and Internet to the teleworker's virtual IP addresses. Although the virtual IP addresses of the teleworkers are located in different subnets, this is shown here as a subnet with a corresponding netmask (255.255.255.0).

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
1000	PASS	Yes	IP Addr. Range	0.0.0.1	255.255.255.254	---	Internal
			Subnet	192.168.3.0	255.255.255.0		
1000	PASS	Yes	Subnet	192.168.3.0	255.255.255.0	Internal	---
			IP Addr. Range	0.0.0.1	255.255.255.254		

Practical Examples for HG 1500

Connecting Teleworkers when Using VPN and Firewall

- DENY rule for blocking residual IP traffic.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
65000	DENY	No	Host	0.0.0.0	--	--	--

2.17.3 "Teleworker HG" Configuration (Board 2)

Network interfaces

1. Enter the LAN1 IP address. 192.1.74.194/24
2. Enter the LAN2 IP address: 217.7.133.164/29
3. Activate NAT only if required (NAT offers enhanced security even when IPSec is deactivated).
4. Activate the bandwidth control.
5. You can set the bandwidth on the interface to the default (10,000 Kbps), (see [Section 2.17.2](#)).

Routing

Default router: Internet	ISP access router via LAN2: 217.7.133.161	
Static route: LAN 1	Target network: 192.1.73.0/24	Gateway via LAN2 from board 1: 217.7.133.163

NAT (if active)

- NAT is not permitted for IKE negotiation either in the incoming or outgoing direction for port 500. Port 500 is therefore open for NAT in the incoming direction.

NAT entry	local: 217.7.133.164	local port: 500	global port: 500
-----------	-------------------------	--------------------	---------------------

"Internal" VPN tunnel

- Board 2 communicates with board 1 over the "internal tunnel". If HG 1500's two LAN2 addresses are both located in the same subnet, the packets are routed locally over the switch and not over the Internet. As an exception to the rule, DES encryption should be used here for the "internal tunnel" specifically to relieve the teleworker HG. As the packets are not routed over the Internet, DES encryption poses no security risks.

Name: Internal
 Terminal Device: Host:
 217.7.133.163
 Encryption algorithm: DES
 Session key validity period: 8 hours
 VPN Peer Authentication: any

"Teleworker" VPN tunnel

Name: Teleworker
 Terminal Device: Host:
 0.0.0.0
 Encryption algorithm: AES, 3DES, DES (Default)
 Session key validity period: 15 minutes
 (maximum timeout after changing
 the IP for a teleworker)
 VPN Peer Authentication: "Digital signatures" preferred

VPN rules

- PASS rules for accessing HG 1500 over LAN1.
 Default settings:

Service: Any Service
 Rule State: Enabled

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
1	PASS	No	Subnet	192.1.74.0	255.255.255.0	::	::

Practical Examples for HG 1500

Connecting Teleworkers when Using VPN and Firewall

- Tunnel rule for IP packets from board 2's LAN1 to the customer LAN.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
5	PASS	Yes	Subnet	192.1.73.0	255.255.255.0	Internal	---
			Host	192.1.74.194	---		
5	PASS	Yes	Host	192.1.74.194	---	---	Internal
			Subnet	192.1.73.0	255.255.255.0		

- Tunnel rule for IP packets between the teleworker's virtual IP addresses (subnets).

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
100	PASS	Yes	Subnet	192.168.3.0	255.255.255.252	Tele-worker	Tele-worker
			Subnet	192.168.3.4	255.255.255.252		
100	PASS	Yes	Subnet	192.168.3.4	255.255.255.0	Tele-worker	Tele-worker
			Subnet	192.168.3.0	255.255.255.252		

- Tunnel rule for IP packets from the customer LAN and Internet to teleworker 1's virtual IP.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
1000	PASS	Yes	IP Addr. Range	0.0.0.1	255.255.255.254	Internal	Tele-worker
			Subnet	192.168.3.0	255.255.255.252		
1000	PASS	Yes	Subnet	192.168.3.0	255.255.255.252	Tele-worker	Internal
			IP Addr. Range	0.0.0.1	255.255.255.254		

- Tunnel rule for IP packets from the customer LAN and Internet to teleworker 2's virtual IP.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
1004	PASS	Yes	IP Addr. Range	0.0.0.1	255.255.255.254	Internal	Teleworker
			Subnet	192.168.3.4	255.255.255.252		
1004	PASS	Yes	Subnet	192.168.3.4	255.255.255.252	Teleworker	Internal
			IP Addr. Range	0.0.0.1	255.255.255.254		

- Tunnel rule for IP packets from the teleworker, needed for IKE phase1 (virtual IP still unknown).

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
64999	PASS	Yes	Host	0.0.0.0	::	Teleworker	::

- DENY rule for blocking residual IP traffic.

Priority	Rule-Based Action	Encryption Required	Type	Address (Lowest in Range)	Subnet Mask/ (Highest Add. in Range)	Tunnel on Receive Side	Tunnel on Transmit Side
65000	DANY	No	Host	0.0.0.0	::	::	::

2.18 Home Workstation / Remote Service

2.18.1 Target Configuration

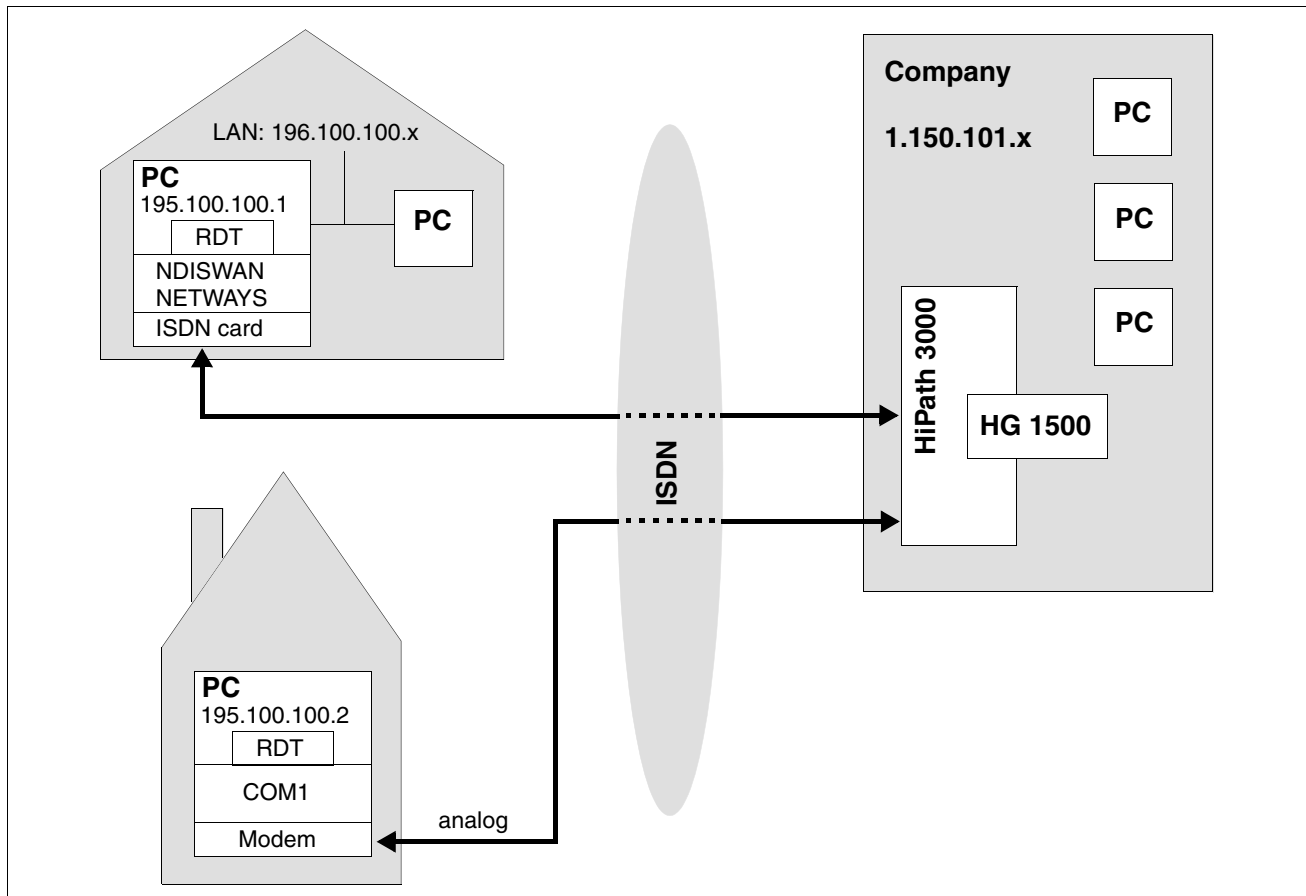
An IP routing is configured in the HG 1500 for the home workstation and/or remote service. The home workstation or remote PC IP address used must not be an IP address of the local LAN (local IP addresses are not routed).

If a local LAN is also used on the home workstation, this LAN must use a separate IP address range (must not be the same as the RDT IP range).

An ISDN adapter or modem must be installed on the home workstation. If an ISDN adapter is used, the driver NDISWAN must be added as a network card by the manufacturer of the ISDN adapter (not Windows 2000/XP). A corresponding RDT connection must be configured.

The settings required on the HG 1500 for the home workstation must be made. 195.100.100.1 should be used as the IP address. The subscriber should be identified using the PAP pr The subscriber should be identified using the PAP procedure with user and password "hipath".

An RDT network connection should also be configured for the home workstation.



2.18.2 Configuration Steps

WBM Settings

1. Insert a PSTN peer:

"Explorers > Routing > PSTN (right-click) PSTN Peers > Add PSTN Peer".

Configure the following data for the PSTN peer:

- Peer Name: Homeworker
- IP Address of PSTN Peer: 195.100.100.1
- IP Address of Local PSTN Interface: 0.0.0.0
- Maximum Data Packet Size (Byte): 1500
- Negotiate IP Address: deactivated
- PSTN Connection Type: normal
- Short Hold Mode: activated
- Short Hold Time (sec): 60
The "Short Hold Time" should be set to at least 60 seconds, otherwise the connection may be aborted as connection setup may take longer than 30 seconds.
- PPP Authentication: activated
- PAP Authentication Mode: PAP Host
- PAP Password: hipath
- PPP Username: hipath

The default values are used for all other parameters.

2. Configure the IP routing.

"Explorers > Routing > IP Routing > Static Routes > (right-click) Add Statistic Route".

Configure the following data for the static route:

- Route Index: 1
- Route Name: Homeworker
- Destination IP Network/Host: 195.100.100.1
- Destination Netmask: 255.255.255.0
- Route Gateway: 195.100.100.1

Practical Examples for HG 1500

Home Workstation / Remote Service

3. Configure a PSTN station number for the PSTN peer:
"Explorers > Routing > PSTN > PSTN Peer > 'Homeworker' > (right-click) Add Station Number".

Enter the station number of the homeworker's trunk connection, e.g. 07807242190.

PC settings

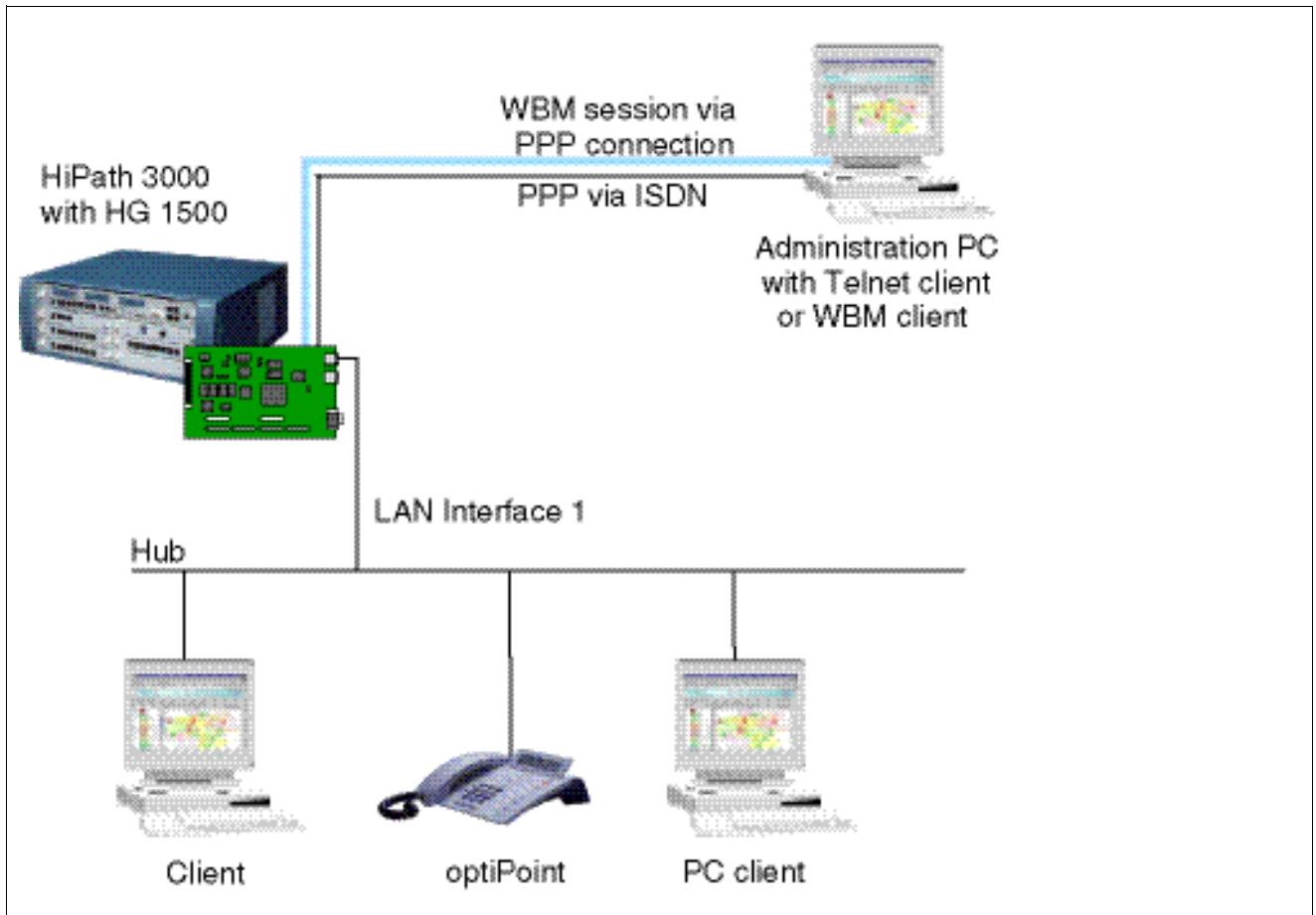
1. Configure an RDT network connection for the home workstation.

Create a new RDT connection using the Network Connection Wizard. Choose the AVM NDIS WAN CAPI driver as the device for this connection.

2.19 Administration via RDT Connection (Remote Access)

2.19.1 Target Configuration

With this configuration, you can administer a HG 1500 board connected via ISDN/PPP from a PC.



Prerequisites

- To create a service entry with HiPath 3000 Manager E an empty database must be available on the board.
- To create a service entry with WBM, the PSTN peer being used must have an MSN. PAP or CHAP authentication must also be activated.

Practical Examples for HG 1500

Administration via RDT Connection (Remote Access)

2.19.2 Configuration Steps

HiPath 3000 Manager E

1. Specify the S₀ expansions and the ISDN parameters for the call numbers to be used.
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

1. Set the general data for the PSTN route: "Explorers > Routing > PSTN > (right-click) Edit Global PSTN Data".
2. Insert a PSTN peer:
"Explorers > Routing > PSTN > (right-click) PSTN Peers > Add PSTN Peer".
The PSTN peer must have an MSN. PAP or CHAP authentication and the "Service Entry" function must be activated for the PSTN peer.
3. Configure an administrator access in the WBM for the IP address of the administration PC.
4. Save the settings.

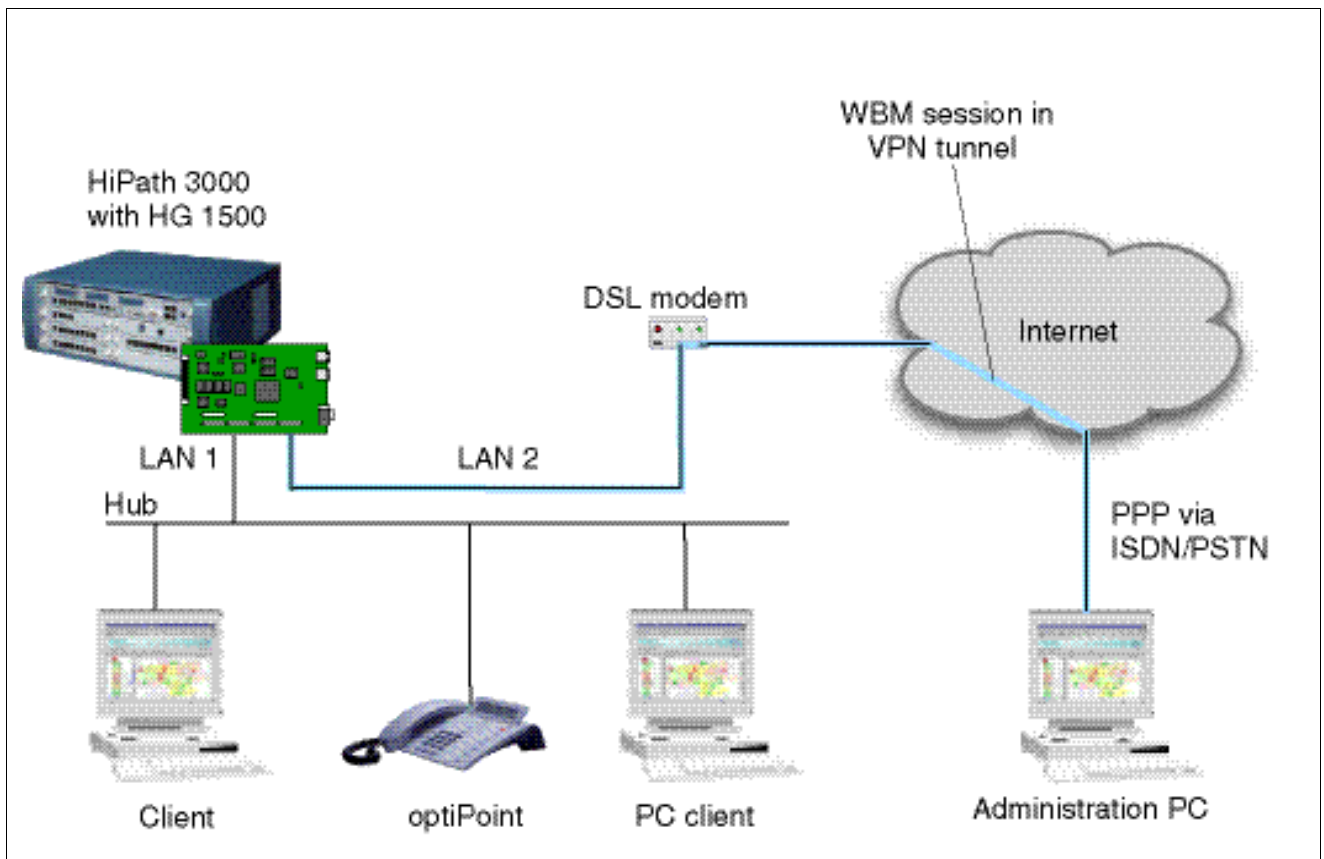
Administration PC

1. Specify the parameters for the dial-up connection to the HG 1500 board.
2. Where applicable, enter routes on the client PCs used.
3. Start the WBM session on the PC and perform the administration tasks.

2.20 Internet-Based Administration

2.20.1 Target Configuration

With this configuration, you can administer a HG 1500 board that can be accessed from a PC via the Internet.



Prerequisites

- An xDSL modem is connected.
- The HG 1500 board features a PPTP connection to the Internet.
- The administration PC is connected to the Internet via an ISDN connection.

2.20.2 Configuration Steps

WBM Settings

1. Switch the second LAN interface to a DSL application.
2. Set the relevant PSTN routing parameters in the LAN mask.
3. Configure an administrator access in the WBM for the IP address of the administration PC.
4. Add a suitable NAT entry:
Local IP Address: IP address of the gateway's LAN 1 interface,
Local Port/Global Port: 8085,
Protocol: TCP.
These settings apply to unencrypted HTTP access, that is, without SSL and VPN.
5. Save the settings.

Administration PC

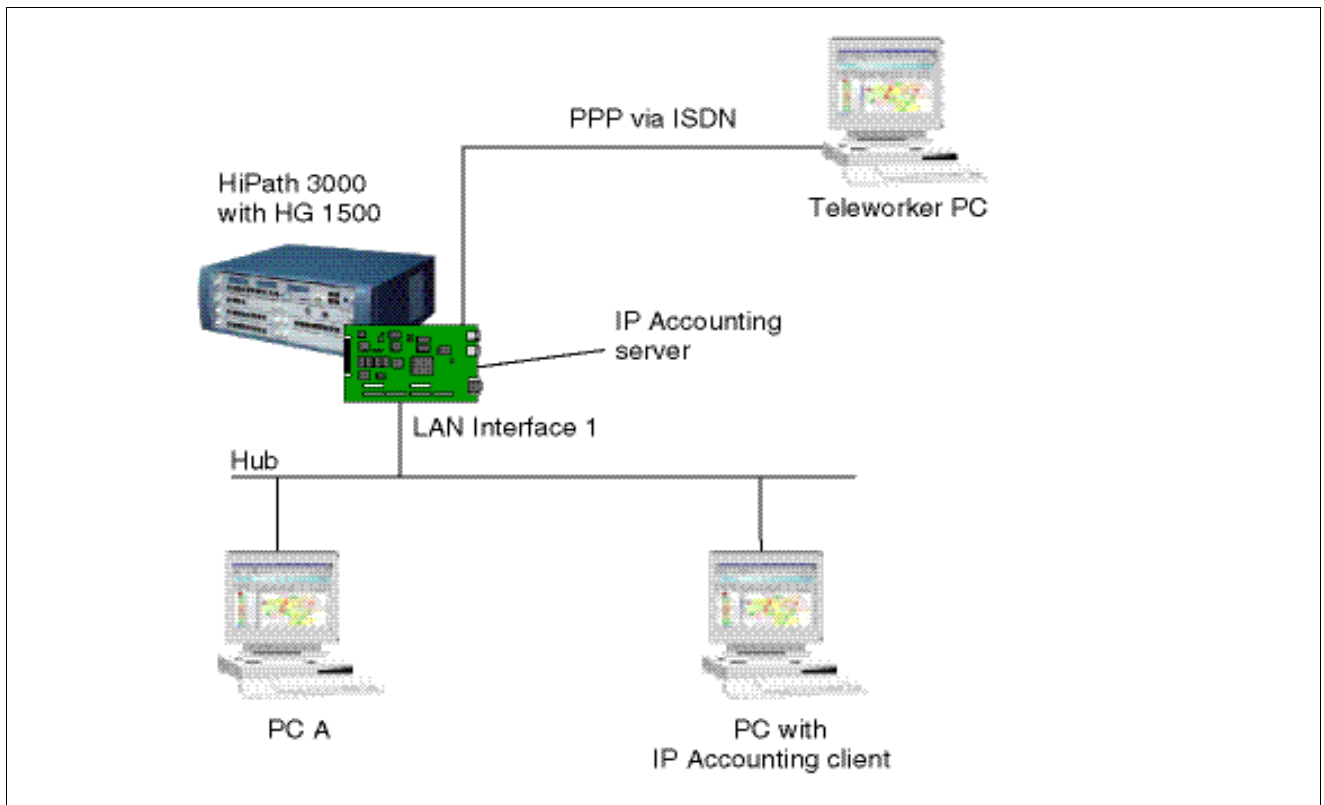
1. Where applicable, enter routes on the client PCs used.
2. Start the WBM session on the PC and perform the administration tasks.

2.21 IP Accounting at Teleworker PCs

2.21.1 Target Configuration

The HG 1500 board counts the IP traffic bytes received and sent via the PPP connections. This happens for all data traffic between IP address pairs. The information on IP packets sent is saved on the HG 1500 board and can be transferred to an IP Accounting client connected to the board.

In the following scenario, a teleworker PC is connected to a HG 1500 board via ISDN/PPP.



Prerequisites

- An ISDN card is installed on the teleworker PC.
- IP Accounting client software (for example MSI teledata) is installed on the IP Accounting client PC).
- The HG 1500 board is allowed to access the teleworker PC.
- The S₀ expansions and ISDN parameters for the relevant call numbers are configured in HiPath 3000 Manager E.

Practical Examples for HG 1500

IP Accounting at Teleworker PCs

2.21.2 Configuration Steps

HiPath 3000 Manager E

1. Specify the S₀ expansions and the ISDN parameters for the call numbers to be used.
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

1. Configure an IP Accounting client.
2. Set the general data for the PSTN route: "Explorers > Routing > PSTN > (right-click) Edit Global PSTN Data".
3. Insert a PSTN peer:
"Explorers > Routing > PSTN > (right-click) PSTN Peers > Add PSTN Peer".
4. Save the settings.

IP Accounting client PC

1. Specify the parameters for accessing the IP Accounting server.
2. Specify the parameters for the data source and ISP.
3. Specify the parameters for transferring the billing data.

Teleworker PC

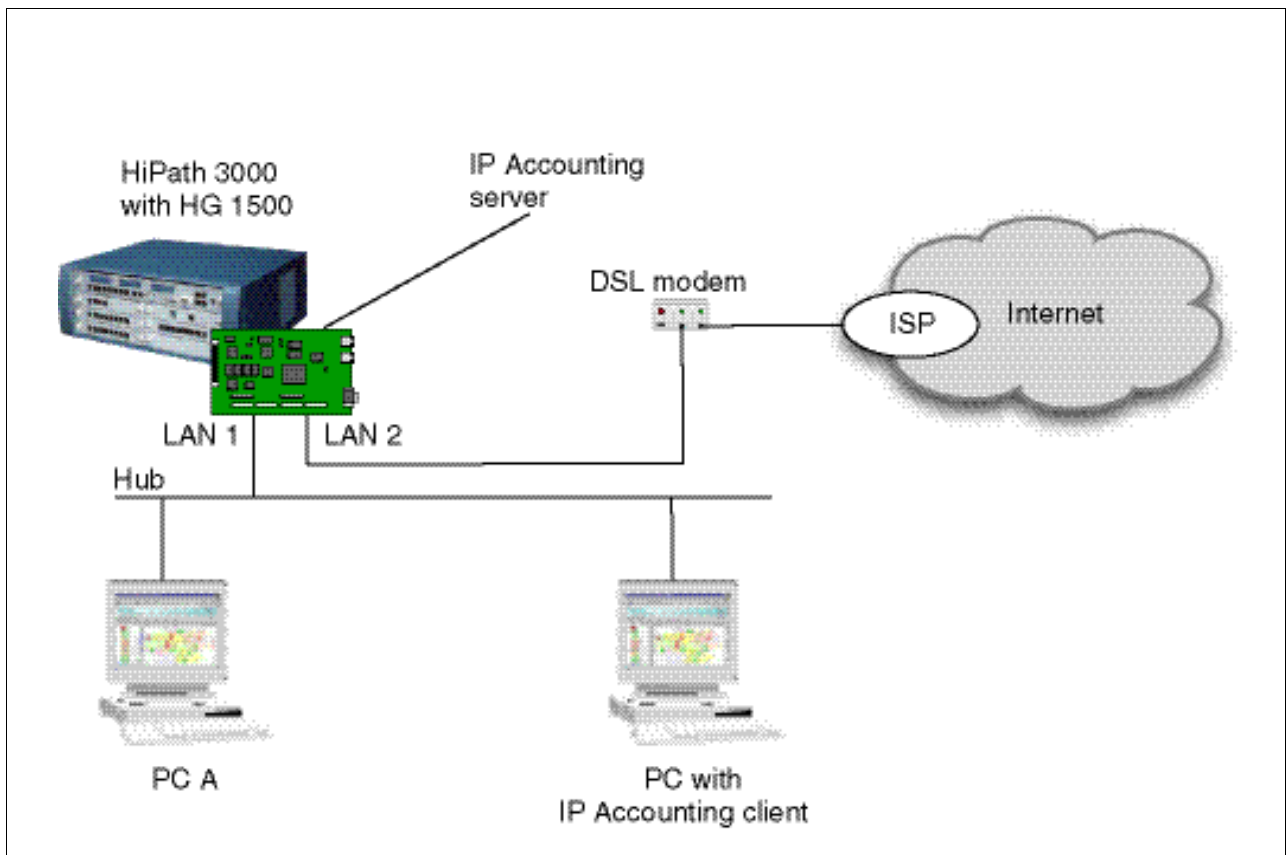
1. Specify the parameters for dial-up access via the HG 1500 board.
2. Where applicable enter routes on the PCs used.

2.22 IP Accounting at the Internet Connection

2.22.1 Target Configuration

The HG 1500 board counts the IP traffic bytes received and sent via the PPP connections. This happens for all data traffic between IP address pairs. The information on IP packets sent is saved on the HG 1500 board and can be transferred to an IP Accounting client connected to the board.

In the following scenario, the HG 1500 board is connected to the ISP/Internet via a DSL modem. The IP traffic from/to the Internet is counted.



Prerequisites

- An xDSL modem/splitter is installed.
- The HG 1500 board is connected to the Internet via a PPPoE or PPTP connection.
- An Internet account is created.

Practical Examples for HG 1500

IP Accounting at the Internet Connection

2.22.2 Configuration Steps

WBM settings for HG 1500

1. Configure an IP Accounting client.
2. Switch the second LAN interface to a DSL application.
3. Set the relevant PSTN routing parameters in the LAN mask.
4. Save the settings.

IP Accounting client PC

1. Specify the parameters for accessing the IP Accounting server.
2. Specify the parameters for the data source and ISP.
3. Specify the parameters for transferring the billing data.

Other PCs

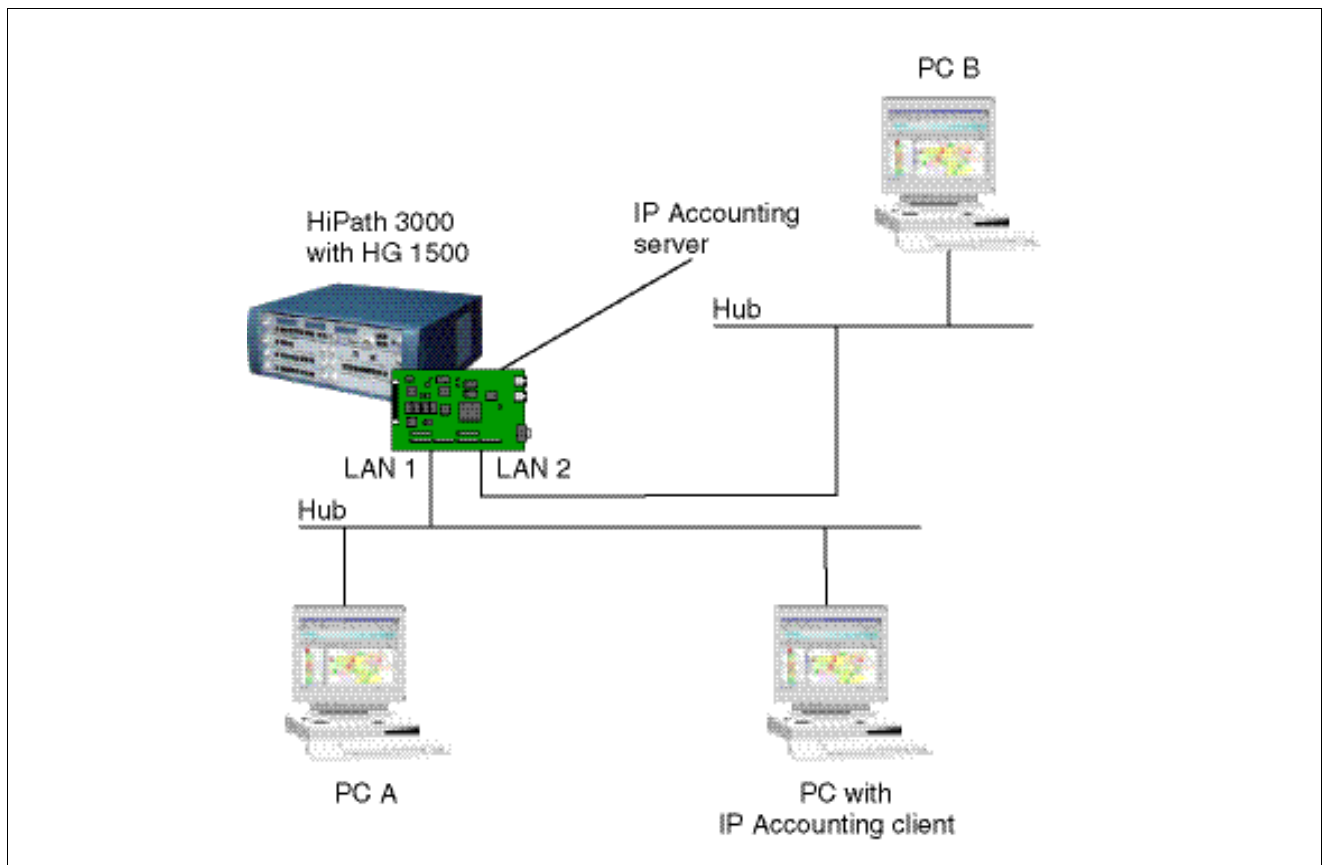
1. Where applicable enter routes on the PCs used.

2.23 IP Accounting Between LAN 1 and LAN 2

2.23.1 Target Configuration

The HXG3 board counts the IP traffic bytes received and sent via the PPP connections. This happens for all data traffic between IP address pairs. The information on IP packets sent is saved on the HG 1500 board and can be transferred to an IP Accounting client connected to the board.

In the following scenario, the HG 1500 board is connected to two LANs. The IP traffic between these LANs is counted.



Prerequisites

- At least one LAN is available in each PC.
- The HG 1500 board is connected to both LANs.

Practical Examples for HG 1500

IP Accounting Between LAN 1 and LAN 2

2.23.2 Configuration Steps

HiPath 3000 Manager E

1. Specify the S₀ expansions and the ISDN parameters for the call numbers to be used.
2. Use HiPath 3000 Manager E to transfer the modified database back to the system.

WBM Settings

1. Configure an IP Accounting client.
2. Activate IP Accounting for the second LAN interface.
3. Switch the second LAN interface to a LAN application.
4. Save the settings.

IP Accounting client PC

1. Specify the parameters for accessing the IP Accounting server.
2. Specify the parameters for the data source and ISP.
3. Specify the parameters for transferring the billing data.

Other PCs

1. Where applicable enter routes on the PCs used.

2.24 Setting up a VPN Configuration

2.24.1 Target Configuration

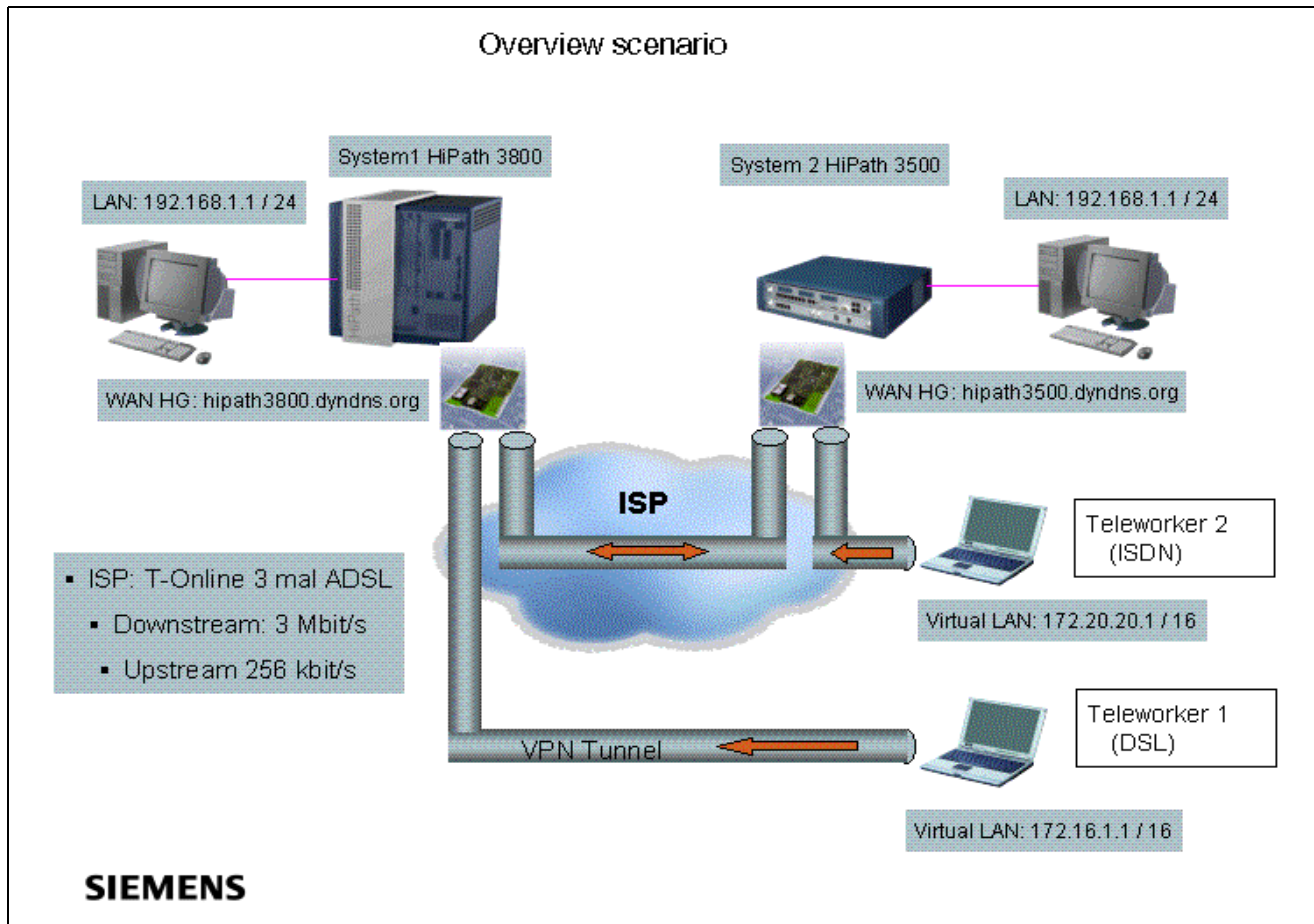


The STMI2 card on the HiPath 3800 is referred to as a HG 1500 throughout this document.

- Two HG 1500 boards on different HiPath systems should be switched to secure mode. Appropriate certificates for access over SSL are generated via the CLI interface.
- VPN functionality should be enabled on the HG 1500 boards in both systems.
- The first configuration example illustrates tunnel configuration via a pre-shared key.
- A Lightweight CA should be activated; the relevant peer certificates and a CRL list are generated. X.509 and PKCS#12 certificates should be exported and imported.
- Internet access should be set up for the corporate network.
- SSH Sentinel VPN clients (teleworkers) and the associated tunnels and rules should be activated according to the following specifications:
 - Communication between the VPN client and the HiPath 3000 target system provided for this.
 - No communication between VPN clients.
 - Allow communication between VPN clients.
 - Configure Internet access for the VPN client.
- Server certificates should be generated for secure data exchange between the two gateways.

Practical Examples for HG 1500

Setting up a VPN Configuration



2.24.2 Setting up SSL via a V.24 Interface and CLI

1. Set up access to the HG 1500 in HiPath 3800 via the V.24 cable connected and enter the CLI command `reset secure`.

This deletes all configuration data associated with the board apart from the IP address. The board reboots and is set to the SSL Enabled mode. The V.24 interface is now the only means of access for board administration.

You can use the `show mode` CLI command to check whether the board is really in secure state. You will see that only V.24 mode is enabled and all other modes, such as Telnet and HTTP, are disabled.

2. To administer the HG 1500 via SSL, create and activate a self-integrated SSL server certificate via CLI, which may look like this for instance:

```
create ssl cert HG_Group_1 1 "CN=192.168.1.242" 2006/06/12/00:00:00
2008/07/01/00:00:00
```

As you can see, no information about the type of signature algorithm or the length of the public key is specified. These values are automatically assigned by the HG 1500. This certificate should only be used for accessing the HG 1500 initially and should be subsequently replaced by a certificate generated via the HG 1500 that contains all of the required data (such as issuer and subject names for instance).

The name `HG_Group_1` is for administrative purposes only and will subsequently appear in the WBM to identify the certificate.

The LAN 1 IP address of the HG 1500 must be entered as the Common Name (CN) for this certificate. Please observe the date format Year / Month / Day.

Once the command is entered, the fingerprint of the certificate that has just been generated is displayed. Make a note of this hexadecimal numeral.



The fingerprint is important for checking the generated certificate at a later time. Only an unmodified certificate shows exactly the same fingerprint.

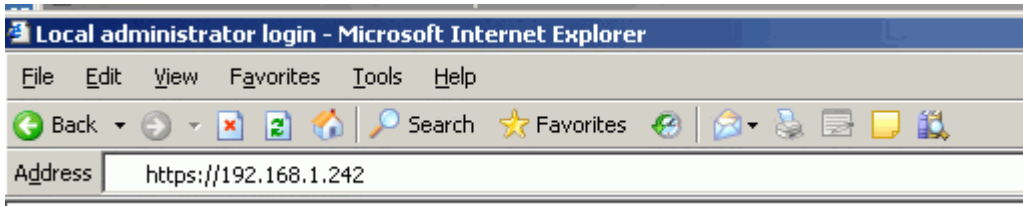
You can output the fingerprint of the certificate **currently active** with the `show fingerprint` CLI command. Please note that if you create and activate multiple certificates one after the other with CLI, the fingerprint output only ever refers to the last certificate activated.

3. Use the `enable ssl` CLI command to switch the board to secure mode and then use `show mode` to check the operating states now set after the board restart. The following operating states are correct:
 - V24 enabled
 - Telnet disabled
 - HTTP disabled
 - HTTPS enabled
 - IPsec disabled

The board can now also be administered via WBM and the HTTPS protocol. All functions that require a TFTP server (`download software` for instance) are no longer available after SSL has been activated.

2.24.3 Additional Administration Steps over WBM and HTTPS

1. Use Internet Explorer to establish a connection to the HG 1500 in HiPath 3800 using the HTTPS protocol. Enter https:// and the correct IP address in the browser's address line as depicted in the following figure:



Check the originator information and validity data for the certificate offered. It must match the self-signed SSL server certificate generated via CLI. Click "Details". Browse to the end of the list with the scroll bar and click the entry "Fingerprint".

The complete fingerprint is displayed as a hexadecimal numeral in the lower window. Compare this numeral with the hexadecimal numeral that you noted when the SSL server certificate was created with the CLI command.



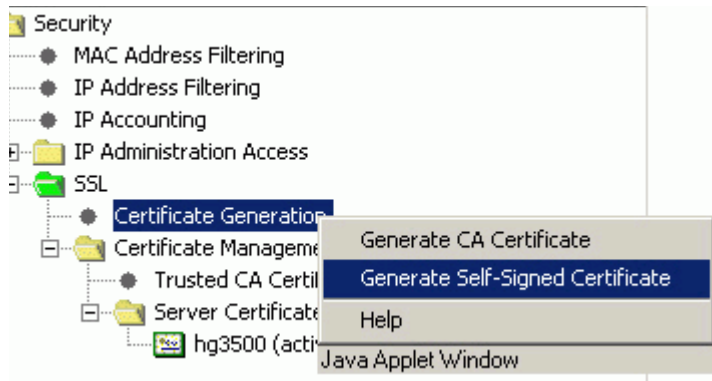
If the two fingerprints are identical, the certificate is unchanged and you can accept it. If the two fingerprints are **not** identical, this may indicate an attempted attack. Appropriate measures should be taken. Under no circumstances should you continue with the configuration.

You can log on to the WBM once you have confirmed the certificate fingerprint.

2. Since the certificate just created via the CLI is only a "minimal certificate", you must now generate a self-signed server certificate for the HG 1500 in the HiPath 3800 with all of the relevant data:
"Explorers > Security > SSL > (right-click) Certificate Generation > Generate Self-Signed Certificate".



All of the data in these sample configurations are only intended as examples. The actual data (such as the type of signature algorithm, the beginning and end of certificate validity or the length of the public key for instance) for your customer certificates is described in the requirements specifications for your installation.



Certificate Information

Certificate Name:	SSL-Server-certificate
Certificate Type:	Self-Signed Peer Certificate
Serial Number of Certificate:	2
Serial Number of Certificate (hex):	02
Type of Signature Algorithm:	md5RSA
Start Time of Validity Period (GMT):	Thursday, 02/01/2007 00:00:00
End Time of Validity Period (GMT):	Tuesday, 02/01/2011 00:00:00
CRL Distribution Point:	
- Issued by CA -	
Country (C):	DE
Organization (O):	Siemens Enterprise
Organization Unit (OU):	TI
Common Name (CN):	192.168.1.242
- Subject Name -	
Country (C):	DE
Organization (O):	Siemens Enterprise
Organization Unit (OU):	TI
Common Name (CN):	192.168.1.242
- Subject Alternative Name -	

Practical Examples for HG 1500

Setting up a VPN Configuration

3. Set md5RSA as a signature algorithm (with a public key length of 1536 bits) with a validity period of four years (beginning and end of certificate validity).

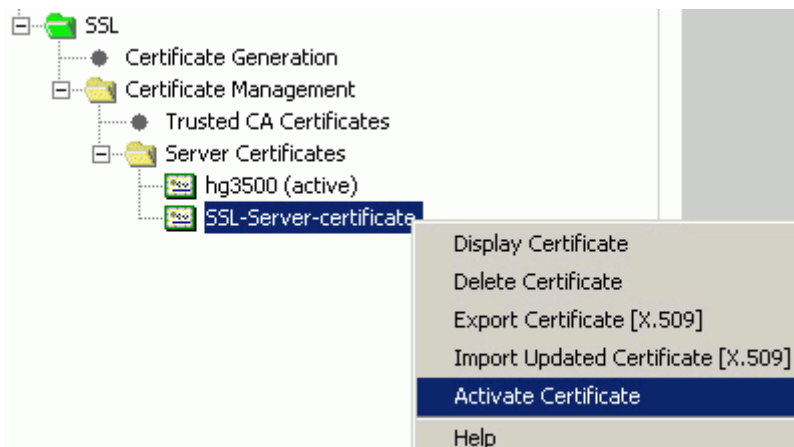
The serial number is an important element. Each certificate must have a unique serial number for each system. The network administrator must keep a list of all certificates with their serial numbers and validity periods.

4. Enter the IP address of the HG 1500 under CN in the "Subject Name" field. This ensures that the certificate does not need to be accepted each time the WBM is registered via SSL once it has been permanently installed in Internet Explorer.

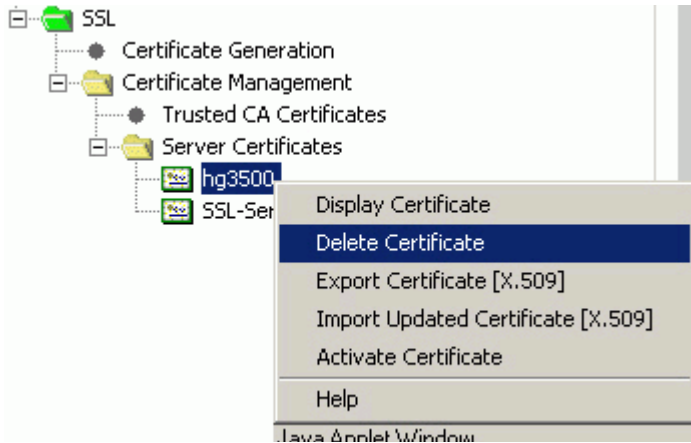
The Subject Alternative Name should contain the IP address of the PSTN peer for remote access.

5. Make a note of the fingerprint of the certificate generated.
6. Now activate the server certificate you have generated:

"Explorers > Security > SSL > Certificate Management > Server Certificates > right-click the certificate already generated > Activate Certificate". This automatically deactivates the certificate generated via CLI.



7. Delete the inactive certificate originally generated via CLI:
"Explorers > Security > SSL > Certificate Management > Server Certificates > right-click the certificate generated via CLI > Delete Certificate".



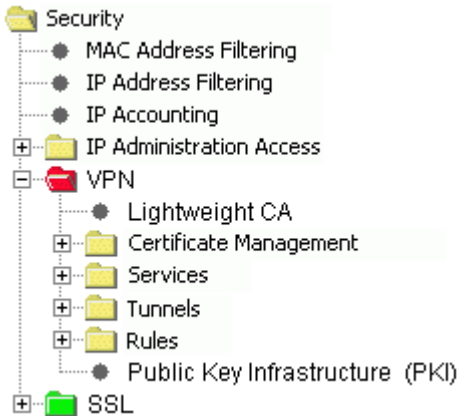
8. The certificate generated and activated with WBM should now be permanently installed in Internet Explorer. To do this, log off from the WBM and close the Internet Explorer. You will see the new certificate the next time you log on to the WBM. Compare the fingerprint and install the certificate permanently. To do this, follow the instructions in the installation routine.
Once the certificate is installed on your PC, it can be viewed at any time in Internet Explorer under "Tools - Internet Options - Content - Certificates".

2.24.4 Configuring Tunnels with Pre-Shared Keys



Never enable IPsec before all the rules required for smooth operation have been set. The rules act like firewall entries and can restrict access to the board. If you enable IPsec too soon and thereby prevent access to the board, you can use the command `disable ipsec` over V.24/CLI to disable the IPsec function.

First of all add one IPSEC license to each of the HiPath systems. A CA license is not required for configuring a tunnel with pre-shared keys.



1. **Set the LAN2 interfaces** for the HG 1500 boards to "**DSL Connection Type PPPoE**":
"Explorers > Network Interfaces > (right-click) LAN2 > Edit LAN2 Interface".

You must enter the following data for the HG 1500 of the HiPath 3800 in the example:

Use the Second LAN as: DSL Connection Type PPPoE

IP Parameters

Remote IP address of the PPP connection:	1.0.0.2
Local IP Address of the PPP Connection:	1.0.0.1
Maximum Data Packet Size (Byte):	1492
Negotiate IP Address:	request a new IP address

General PPP Parameters

Default router:	yes
Internet Access with DNS Request:	yes
Name of the Internet Service Provider:	ISP name
PPP Default Header:	yes

IP Header Compression:	no
Send LCP Echo Request:	yes
Automatic PPP Connection:	yes
Automatic PPP Reconnection:	yes

Short Hold

Short Hold:	no
Short Hold Time (sec):	no input

Authentication

PPP authentication:	yes
PPP User Name:	assigned by the ISP
PAP Authentication Mode:	PAP Client
PAP Password:	assigned by the ISP
CHAP Authentication Mode:	not used
CHAP Password:	no input

Data Compression

STAC Data Compression:	no
MPPC Data Compression:	no

Address Translation

NAT:	yes
Address Mapping:	no

QoS Parameters of Interface

Bandwidth of Connection (Kbps):	256 (as agreed by the ISP)
Bandwidth Control for Voice Connections:	yes
Bandwidth Used for Voice/Fax (%):	80
QoS Capability:	Identical

Practical Examples for HG 1500

Setting up a VPN Configuration

Information on the fields:

- The defaults for "**Remote IP Address of the PPP Connection**" and "**Local IP Address of the PPP Connection**" should not be changed, even if "**Negotiate IP Address**" is set to "request new IP address". These entries are needed for the PPPoE interface if there is no IP address available for the PPPoE interface.
- "**Default router: yes**" means that all IP data traffic is routed to remote IP subnets (such as the Internet). "**Default Routing via: DSL**" then appears when you select "Explorers > Routing > IP Routing > (right-click) Default Router". The option "IP Address of Default Router: 1.0.0.1" is not used here.

Activating "**Bandwidth Control for Voice Connections**" gives priority to Voice over IP. The number of calls permitted is limited by the bandwidth.

If "**Bandwidth of Connection (Kbps)**" is set, the correct value must be set for the upstream speed for the Internet connection.

The "Bandwidth Used for Voice/Fax (%)" option sets a restriction for the maximum amount of bandwidth that can actually be used for Voice over IP.

Note: Incoming traffic shaping cannot be performed on the HG 1500 WAN interface.

2. **Configure "Automatic Control of Disconnect (ACD)"** so that the Internet Service Provider does not clear down the DSL PPPoE connection at an unsuitable time (generally every 24 hours).

In our example, the time of the clear down and redial is set to 03:00 (hour = 3, minute = 0, seconds = 0):

"Explorers > Network Interfaces > LAN2 (DSL-PPPoE) > (right-click) Edit ACD".

ACD Configuration

Connection Time: (connection time display only)

Force Reconnect at: 3 0 0

3. Click "Apply" now.

4. **Configure the DynDNS Service** so that your dynamic IP address assigned by the ISP can be entered in the DNS.

"Explorers > Basic Settings > DynDNS > DynDNS Service > (right-click) Edit DynDNS Configuration".

User name: <Logon User DynDNS>

Password: <Password>

Retype Password: <Password>

Host name: hipath3800

Domain name: dyndns.org

Last update: (if completed)

IP Address at DynDNS: (display only)

Own dynamic IP Address:	(display only)
Enable Wildcard:	no
Mail Exchanger:	no
Backup MX:	no
Use HTTPS for Update:	yes

Information on the fields:

- "<Logon User DynDNS>" is the **user name** (User) and <Password> is the **password** (PASS) that you selected when you logged onto the DynDNS service (here dyndns.org). You must have a valid user name and a valid password.
 - **Host name** is the first part of the DNS name of the LAN2 interface. In the example, the entire DNS name is therefore "**hipath3800.dyndns.org**".
 - **Last Update** contains the date and time of the last update (if completed).
5. Configure the **Update Timer DNS Names** for updating the DNS name periodically. The updating time only applies to VPN rules and the DynDNS names used in them. An IP address that may have been recently assigned by the Internet Service Provider is therefore updated at least every 10 minutes:
"Explorers > Basic Settings > DynDNS > Update Timer DNS Names > (right-click) Edit Update Timer for DNS Names".

Update Timer for DNS Names:

Update DNS Names:	yes
Update Timer Value for DNS Names (sec):	180

6. Now click "Apply" and then click "OK" in the "Action completed successfully" window.

Practical Examples for HG 1500

Setting up a VPN Configuration

- To use DNS names, the **"DNS"** service must be activated in a PASS rule. The "DNS" service and the associated PASS rules are already configured by default (Rule Priority 10). An additional rule is required to register and update a DynDNS (Rule Priority 6490). This is also provided in the default. Both rules must be activated:
"Explorers > Security > VPN > Rules > Configured Rules > (right-click) Edit Rule > Activate Rule" (Rules 10 **and** 6490).
- Configure a tunnel from the HiPath 3800 to the HiPath 3500:
"Explorers > Security > VPN > Tunnels > (right-click) Configured Tunnels > Add Tunnel".

The following is an example of the settings for the HG 1500 in the HiPath 3800. Please note that all settings must also be made on the remote station in line with the correct values.

Tunnel Name:	toHiPath3500
Local Tunnel Endpoint Type:	DNS Name
Local Tunnel Endpoint Address:	hipath3800.dyndns.org
Remote Tunnel Endpoint Type:	DNS Name
Remote Tunnel Endpoint Address:	hipath3500.dyndns.org
Suggested Encryption Algorithms:	AES and DES and 3DES
Suggested Hash Algorithms:	MD5 and SHA1
Session Key Handling:	Automatically, using IKE protocol
Suggested Lifetime of the Session Keys:	8 hours (default)
Suggested Lifetime of the Key Exchange Session:	8 hours (default)
Suggested Data Volume of the Session Keys:	unlimited (default)
Select the option "Key Exchange Data" and enter the key exchange parameter for this new tunnel:	
Activate "Perfect Forward Secrecy":	yes
VPN Peer Authentication Method:	Pre-shared keys
Pre-Shared Key:	*****
Suggested Diffie-Hellman Groups:	DH Group 2, DH Group 5

Information on the fields:

- The local tunnel endpoint address contains the DynDNS name of the local LAN2 interface.
- The remote tunnel endpoint address contains the DynDNS name of the LAN2 interface on the remote station.

- Do not change the default values for encryption and hash algorithms. DES is only listed for compatibility reasons and should not be used as an encryption algorithm.
- Select "Pre-shared keys" as the VPN Peer Authentication Method and enter a sufficiently long and secure password for the pre-shared key. Make a note of this data. The same password must also be entered in the tunnel in the remote system.
- Accept the suggested Diffie-Hellman groups.

9. **Define all rules** that are required to enable both HiPath systems to communicate via the tunnel:

"Explorers > Security > VPN > Rules > (right-click) Configured Rules > Add Rule".

Start with a **rule for accessing the administration PC on the HG 1500**. This rule should have second highest priority. The following is a list of the inputs in the individual fields for this kind of rule using the HG 1500 in HiPath 3800 as an example:

Priority:	2
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	No
Enable Rule:	Yes
Source Address Type:	Subnet
Source Address IP Address: Subnet Address:	192.168.1.0
Source Address Subnet Mask:	255.255.255.0
Destination Address Type:	Subnet
Destination Address IP Address:	192.168.1.0
Source Address Subnet Mask:	255.255.255.0

Information on the fields:

- **Priority:** The highest priority is 1, while the lowest is defined as 65000. The more precise the rule, the higher the priority should be. A rule for a subnet (for example, from source 192.168.1.0 to destination 192.168.2.0) must therefore be assigned a lower priority than a rule that only affects a single computer (for example, source 192.168.1.10 to destination 192.168.2.20).
- **Enable Rule:** If this option is activated, this rule automatically becomes effective when IPsec is activated.
- **Encryption Required:** This is not needed in the current scenario because the rule is only used for accessing the HG 1500 from the home subnet.

Practical Examples for HG 1500

Setting up a VPN Configuration

10. Configure a **rule for communication with the other HiPath systems via the configured tunnels** using the following data:

Priority:	100
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	yes
Enable Rule:	yes
Source Address Type:	Subnet
Source Address IP Address: Subnet Address:	192.168.1.0
Source Address Subnet Mask:	255.255.255.0
Destination Address Type:	Subnet
Destination Address IP Address: Subnet Address:	192.168.2.0
Subnet Mask:	255.255.255.0
Tunnel on Receive Side:	No Tunnel Assignment
Tunnel on Transmit Side:	toHiPath3500



This rule makes it possible to access the administration PC on the HG 1500 and to access all network components on the HG 1500 (such as IP telephones).

Information on the fields:

- **Priority:** In this scenario, the priority is set to 100. This leaves enough space (from priority 3 to 99) to add any rules with higher priority to the configuration.
- **Encryption Required:** Of course the data should be encrypted between the two subnets. The encryption process was previously defined in the tunnel configuration.
- **Tunnel on Receive Side:** No tunnels are assigned. The entry is needed for the counter rule.
- **Tunnel on Transmit Side:** The previously defined tunnel named "toHiPath3500" is assigned here. The assignment of a tunnel to a rule can read as follows: "I, the **Source Address** with subnet 192.168.1.0, wish to send data to the **Destination Address** with subnet 192.168.2.0. I am sending the data (from the transmit side) to the tunnel with the name "toHiPath3500".

11. Now configure a counter rule for the source address 192.168.2.0 to the subnet 192.168.1.0 so that it is also possible to configure a tunnel from the remote station (HiPath 3500). "Explorers > Security > VPN > Rules > Configured Rules > (right-click) selected rule > Add Rule for Opposite Direction".

A rule with the following data is created automatically and simply needs to be accepted:

Priority:	100
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	yes
Enable Rule:	yes
Source Address Type:	Subnet
Source Address IP Address: Subnet Address:	192.168.2.0
Source Address Subnet Mask:	255.255.255.0
Destination Address Type:	Subnet
Destination Address IP Address: Subnet Address:	192.168.1.0
Subnet Mask:	255.255.255.0
Tunnel on Receive Side:	toHiPath3500
Tunnel on Transmit Side:	No Tunnel Assignment

Information on the fields:

- The values for "Tunnel on Receive Side" and "Tunnel on Transmit Side" in the previously defined rule are swapped. A tunnel on the transmit side is not assigned because the rule has already been defined for the transmit direction.
- Rules for the opposite direction receive the same priority as the rules from which they were derived.
- "NAT" is not performed for tunnel rules.



Set the alive monitoring procedure to TCP for IP networking or IP trunking (Explorers > Voice Gateway > PBX > IP Networking Data). Additional VPN rules would otherwise be needed for the ICMP procedure.



A static route can only be configured with fixed IP addresses. As a result, all destinations must be reachable over the "default router" when using dynamic IP addresses. The default router is transferred by the ISP to the gateway during PPPoE configuration.

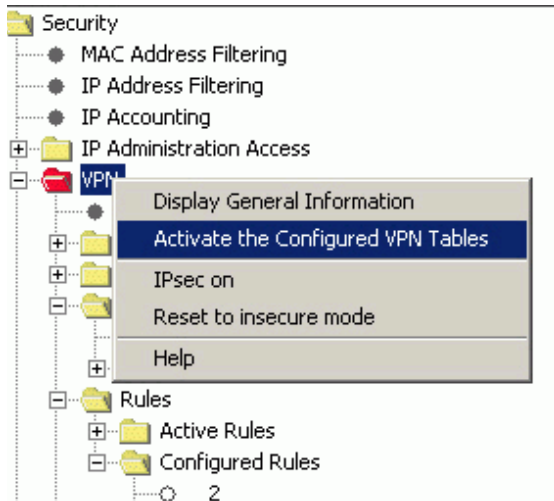
Practical Examples for HG 1500

Setting up a VPN Configuration

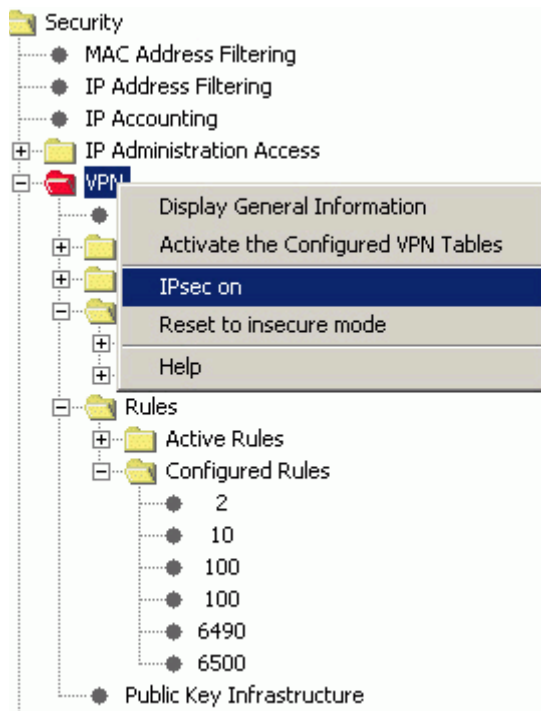


In HG 1500 V5.0 and later, a NAT rule is not required for UDP Port 500 (= ISAKMP / IKE). The port is automatically opened on the WAN interface and "NAT" is no longer performed for ISAKMP packets (hard coded).

12. If all rules and tunnels have been configured correctly, then activate the tables configured. This transfers all rules and tunnels to the "Active Rules" and "Active Tunnels" folders:
"Explorers > Security > (right-click) VPN > Activate the Configured VPN Tables".

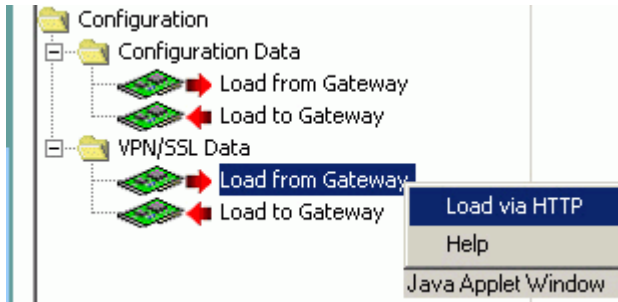


13. Activate the IPsec function: "Explorers > Security > (right-click) VPN > IPsec on".



14. Save your configuration by clicking the red diskette icon in WBM.

15. Save the configuration to an external data medium:
"Maintenance > Configuration > VPN/SSL Data > (right-click) Load from Gateway > Load via HTTP".



16. Now set up the remote station as appropriate.
To check the routing function using the tunnel you have created, start a ping to an IP address on the remote side.

2.24.5 Deleting Tunneling and Rules

A tunnel with digital signatures should be used instead of a tunnel with pre-shared keys. Because it is not possible to change a tunnel once it has been set up and activated, this tunnel must first be deleted. However, it is only possible to delete a tunnel if no rules are assigned to it. This means that all associated rules must also be deleted.

1. Delete all rules for the tunnel previously created in all HG 1500 boards in your network. (Alternatively, you can also configure just the new tunnel, reassign the rules to the new tunnel and then delete the old tunnel):

"Explorers > Security > VPN > Rules > Configured Rules > (right-click) selected rule > Delete Rule".

Rule 2 only governs access from the administration PC to the HG 1500 and thus has no connection with any tunnel. Do not delete this rule.

2. Delete the tunnel on all HG 1500 boards in your network:
"Explorers > Security > VPN > Tunnels > Configured Tunnels > (right-click) selected tunnel > Delete Tunnel".

3. The rules and tunnels are still contained in the "Active" folder. Up to now, you could only delete references to these tunnels and rules. The original configuration, however, remains active. You must activate the deleted VPN tables in order finally to deactivate the tunnels and rules. Activate the new configuration:

"Explorers > Security > (right-click) VPN > Activate the Configured VPN Tables".

4. Save your configuration by clicking the red diskette icon in WBM.

2.24.6 Setting up a Tunnel with Digital Signatures

1. Add the CA license to one of the HiPath systems in your network. In the sample scenario, this should be performed in the HiPath 3800.
2. Generate a self-signed lightweight CA certificate via HG 1500 WBM administration on this system:
"Explorers > Security > VPN > (right-click) Lightweight CA > Generate CA Certificate".

The certificate should contain the following data:

Certificate Name:	IPsec LW CA
Serial Number of Certificate:	1
Type of Signature Algorithm:	sha1RSA
Validity period:	10 years
CRL Distribution Point:	(leave empty)
Country (C):	DE
Organization (O):	Siemens
Organization Unit (OU):	TI
Common Name (CN):	LWCA
Subject Alternative Name:	Space for additional information (alternative)
Public key length:	1536 bits

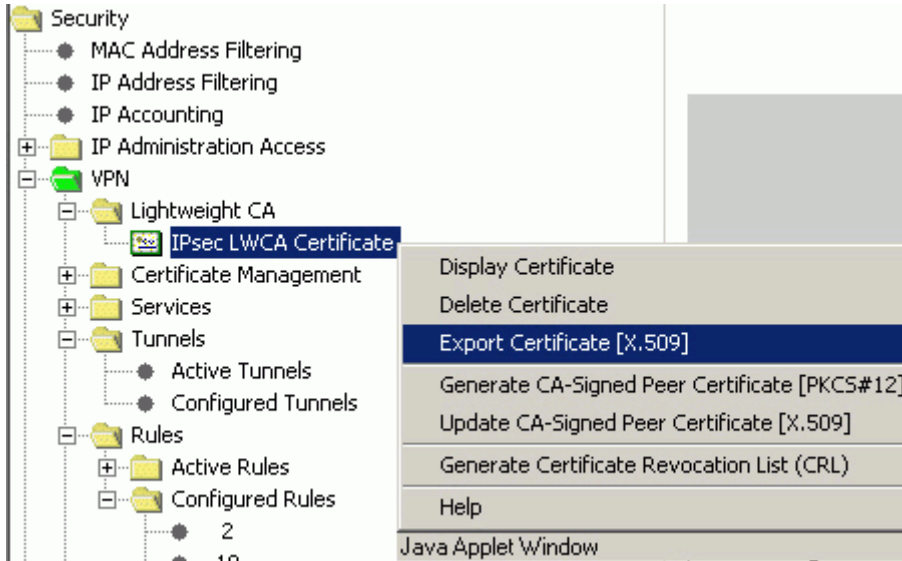
Information on the fields:

- Enter a unique name for the certificate. This makes identification much easier at a later stage.
 - If the customer wants to set up VPN clients for teleworkers, you should note that the Safenet Sentinel SSH client does not support certificates with a digital signature algorithm or **DSA**.
 - Serial Number: You can assign 1 as the serial number even though you have already defined a CA certificate with this number under SSL CA. However, there is no connection between an SSL CA and a lightweight CA. The same applies for the server and peer certificates.
 - Certificate validity cannot be extended at a later point.
3. Make a note of the fingerprint of the certificate you have just created.

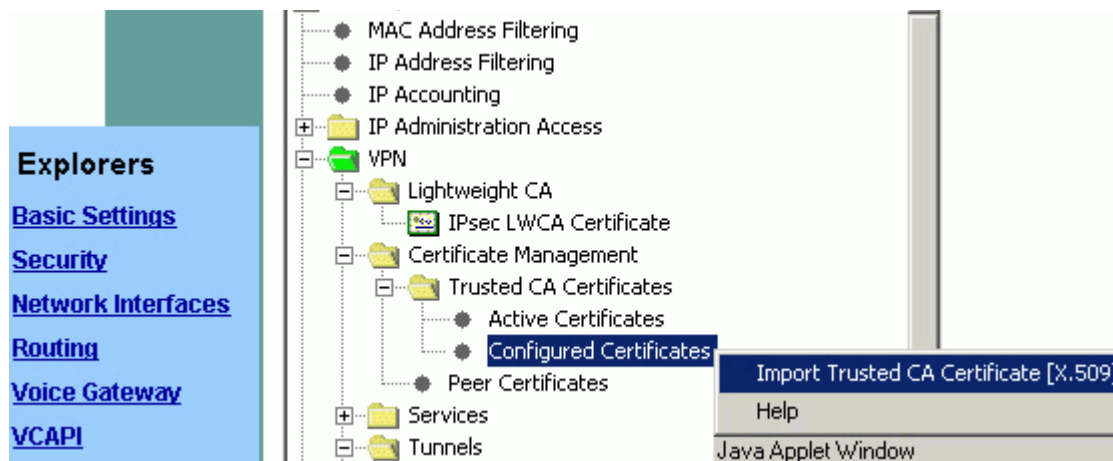
Practical Examples for HG 1500

Setting up a VPN Configuration

- Next export this self-signed lightweight CA as an X.509 certificate:
"Explorers > Security > VPN > Lightweight CA > (right-click) selected certificate > "Export Certificate [X.509]"



- Save the certificate shown in the ensuing dialog on a data medium.
- Now import the lightweight CA you just exported as a trusted CA certificate to all HG 1500 boards in your network:
"Explorers > Security > VPN > Certificate Management > Trusted CA Certificates > (right-click) Configured Certificates > Import Trusted CA Certificate [X.509]"
Enter a descriptive, meaningful name for the certificate such as LWCA for instance.



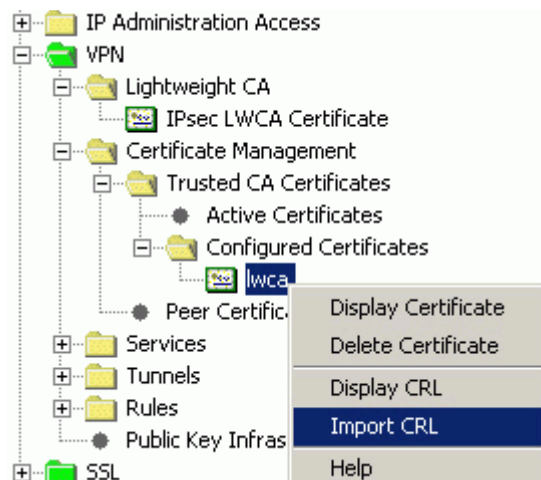
Always remember to compare the fingerprint with the one noted in step 3 when importing certificates. The certificate is only trustworthy if both fingerprints are identical.

- Generate an empty certificate revocation list:
"Explorers > Security > VPN > Lightweight CA > (right-click) selected certificate > Generate Certificate Revocation List (CRL)".



A practical validity period for a certificate revocation list will depend on the customer's security requirements with regard to the likelihood that certificates issued will need to be entered in the list (if an unreliable or dismissed employee should be denied access to the system for instance). High security with a certificate revocation list validity period of a few days means that a new list needs to be generated, saved and imported into all HG 1500 boards before the validity period expires. In the example, the validity period should be one year.

8. Save the certificate revocation list to a data medium.
9. Import this certificate revocation list into the trusted CA certificate associated with all HG 1500 boards in your network:
"Explorers > Security > VPN > Certificate Management > Trusted CA Certificates > Configured Certificates > (right-click) selected certificate > Import Certificate Revocation List (CRL)".



You can display this certificate revocation list anytime.

If a certificate (for example, belonging to a teleworker) should be declared as blocked, then a new certificate revocation list must be created via the lightweight CA which then contains this expired peer certificate.

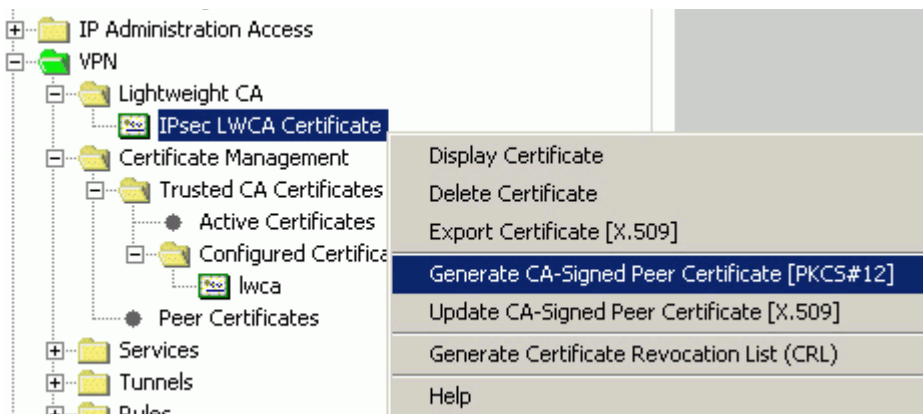
After this, the new certificate list must be re-imported into all trusted CA certificates.

Practical Examples for HG 1500

Setting up a VPN Configuration

Warning: By definition, a certificate revocation list (CRL) is not replaced before its validity period elapses. Two valid CRLs would then be in circulation, which means that theoretically a man-in-the-middle attack could take place even after certificates are replaced. The relatively short CRL validity (a few days for instance) would provide effective protection, but would also involve having to replace the CRL more frequently. Alternatively, the HG 1500 can be integrated into PKIs. LDAP access allows the HG 1500 to retrieve the CRL from a remote CA (PKI). The old CRL is only deleted when the HG 1500 is reset. However, this does not guarantee that the CRL has been removed from remote components (theoretical attack scenario).

10. Generate a PKCS#12 peer certificate for all the HG 1500 boards in your network: "Explorers > Security > VPN > Lightweight CA > (right-click) selected certificate > "Generate CA-Signed Peer Certificate [PKCS#12]".

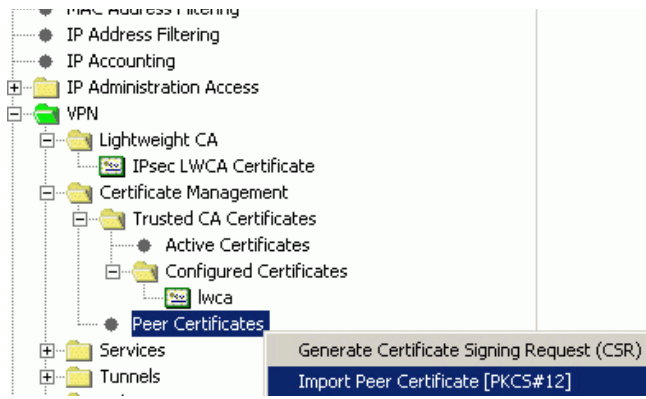


The certificate should contain the following data:

Password:	should be sufficiently long and secure
Serial Number:	should be unique and greater than 1
Validity period:	for example, 1 year
CRL Distribution Point:	URL of the HG 1500 that issues this certificate. It is therefore always clear from the certificate which CA (HG 1500) issued the peer certificate. This is only an information field.
Public key length:	1536 bits
Subject Name:	Enter a unique name, such as "peer cert for HiPath3800". The subject name (CN) must differ from the issuer's CN.

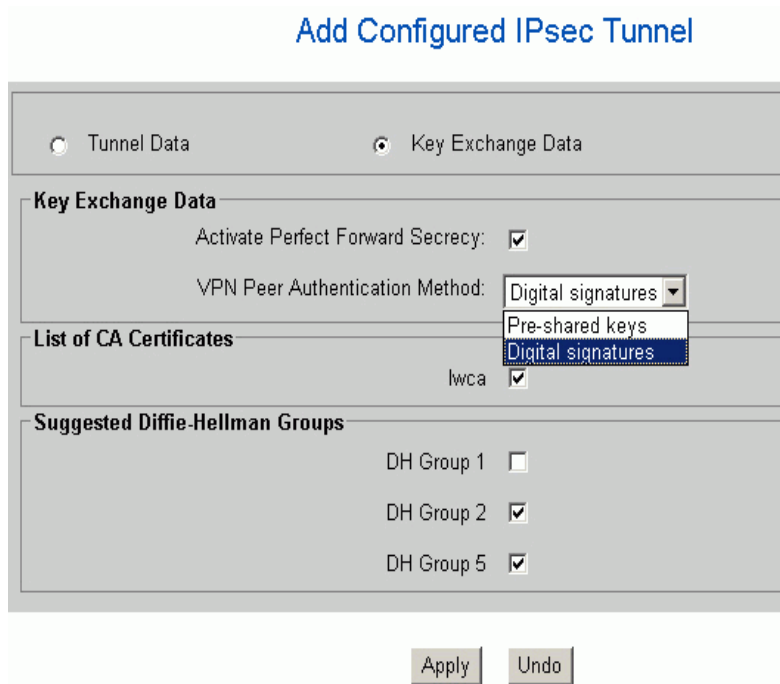
11. Select a location where it is saved on a data medium.
12. Make a note of the fingerprint of the certificate you have just created.

13. Now import the PKCS#12 peer certificate that you generated and saved earlier for each HG 1500 into the relevant HG 1500 in your network:
"Explorers > Security > VPN > Certificate Management > (right-click) Peer Certificates > Import Peer Certificate [PKCS#12]".



14. Set up a tunnel to the remote station:
"Explorers > Security > VPN > Tunnels > (right-click) Configured Tunnels > Add Tunnel".

Proceed as described in the section on tunnel configuration with pre-shared keys. However, select digital signatures as the authentication process for the VPN peers. You should also select the trusted CA certificate from the list of CA certificates.

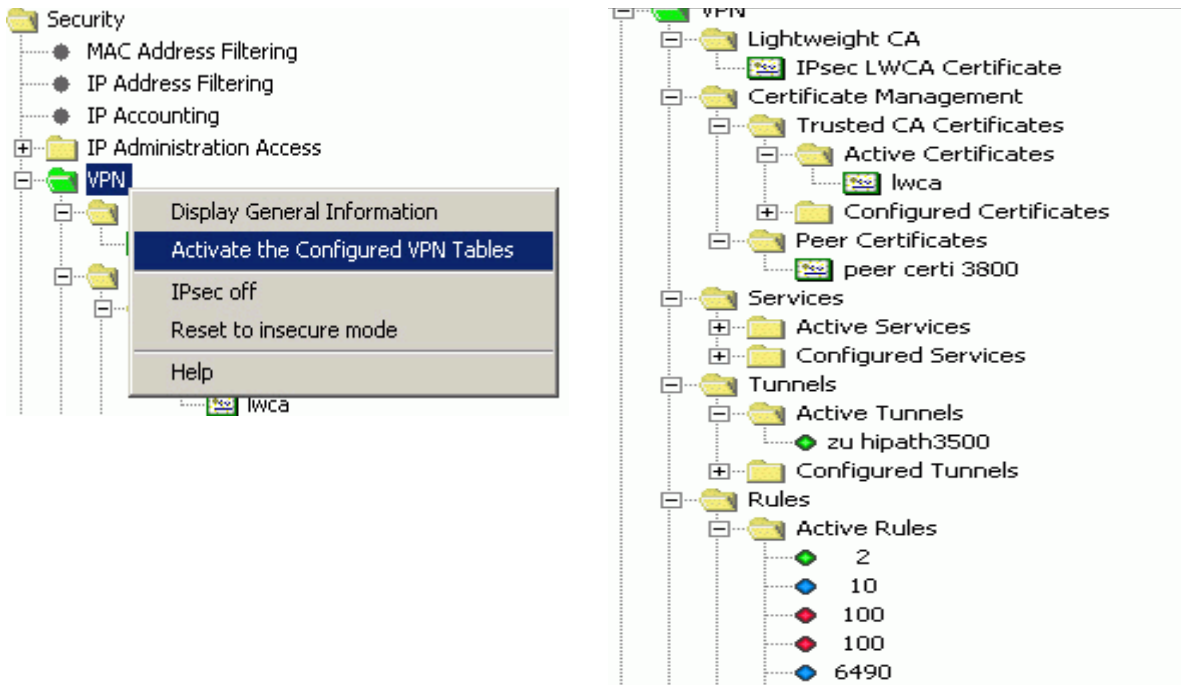


15. Define all the rules and routes necessary to configure the tunnel. To do this, proceed as described in the section on tunnel configuration with pre-shared keys.

Practical Examples for HG 1500

Setting up a VPN Configuration

16. Activate the rules and tunnels. To do this, proceed as described in the section on tunnel configuration with pre-shared keys.



17. Check the function with a ping to the partner system. Please note that some configuration steps will have to be repeated on the other systems in your network.

2.24.7 Internet Access for the Corporate Network

Now configure the two rules that permit Internet surfing for the station in the customer LAN. The sample configuration illustrates the breakout of the respective customer LAN used (here: HiPath 3800) via the local Internet telephony connection.

- **Sample configuration 1**

Priority:	6000
Service:	Any Service
Rule-Based Action:	PASS_INCOMING
Encryption Required:	No
Enable Rule:	Yes
Source Address Type:	Subnet
Source Address IP Address: Subnet Address:	192.168.1.0
Source Address Subnet Mask:	255.255.255.0
Destination Address Type:	Host
Destination Address IP Address:	0.0.0.0

- **Sample configuration 2**

Priority:	6001
Service:	Any Service
Rule-Based Action:	PASS_OUTGOING
Encryption Required:	No
Enable Rule:	Yes
Source Address Type:DNS Name	DNS Name
Source Address IP Address: DNS Name	Hipath3500.dyndns.org
Destination Address Type:	Host
Destination Address IP Address:	0.0.0.0

Information on the fields:

Rule-Based Action "PASS_INCOMING" means that from the HG 1500 viewpoint the rule only applies to packets coming from the network. Accordingly, "PASS_OUTGOING" means that from the HG 1500 viewpoint the rule applies to packets that are being sent to the network.

Practical Examples for HG 1500

Setting up a VPN Configuration

Explanation: The rule with priority 6000 and the "PASS_INCOMING" action enables access from the local subnet 192.168.1.0 to the HG 1500 (IP stack). If a valid rule (such as 6001 for instance) is operative, a "pass" to the destination IP address 0.0.0.0 (Internet for instance) is enabled. The priority 6001 rule and the "PASS_OUTGOING" action now allows other networks to be reached (such as the Internet for instance) via "NAT". If you could not activate VPN rule 6001 (unresolved DNS name), the last "deny" rule 65000 will prevent the transmission of unauthorized data packets (for example: packets intended for the tunnel are transmitted to the Internet as "unNATted").

2.24.8 Configuring Teleworkers for HiPath 3800 and HiPath 3500

The scenario below illustrates the configuration of two teleworkers with access to the HG 1500 on the respective HiPath 3000. The example illustrates the configuration of Teleworker 1 (DSL) for the HG 1500 of the HiPath 3800. Teleworker 2 (ISDN) is then configured on the HG 1500 of the HiPath 3500.

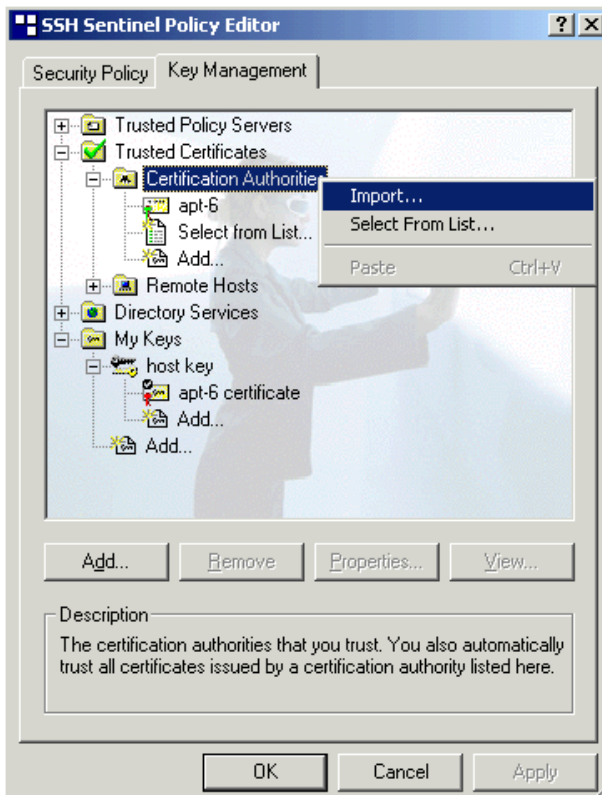
1. Generate another peer certificate for the teleworkers using the LW CA in your network and save them on a data medium:
"Explorers > Security > VPN > Lightweight CA > (right-click) selected certificate > "Generate CA-Signed Peer Certificate [PKCS#12]".
2. If you haven't already done so, export the X.509 certificate for the LW CA to your data medium.
"Explorers > Security > VPN > Lightweight CA > (right-click) selected certificate > Export Certificate [X.509]".
3. Install the VPN client software. To do this, follow the installation routine. Please skip the following installation steps. Please note that a certificate does not need to be generated using the VPN client software because you have already created a PKCS#12 certificate using the lightweight CA.

The VPN client icon appears in the tray bar following successful installation and after the computer has been restarted.



4. Start the Policy Editor (right-click the icon > "Run Policy Editor").

5. Import the CA certificate generated in the lightweight CA (X509 certificate) under Trusted Certificates as follows:



"Trusted" means that peer certificates issued by this CA are accepted by the VPN client during authentication.

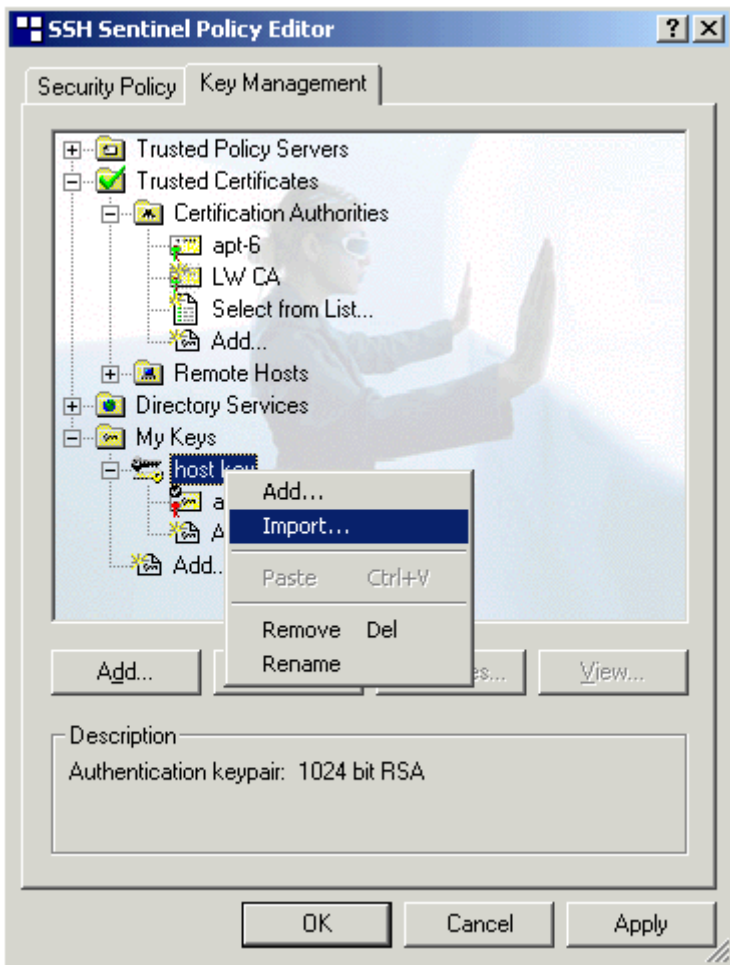
Once you have selected the certificate you want to import, its fingerprint is displayed.

6. Compare this fingerprint with the one you noted down earlier. Click "Yes" in the dialog showing the fingerprint if both fingerprints match.

Practical Examples for HG 1500

Setting up a VPN Configuration

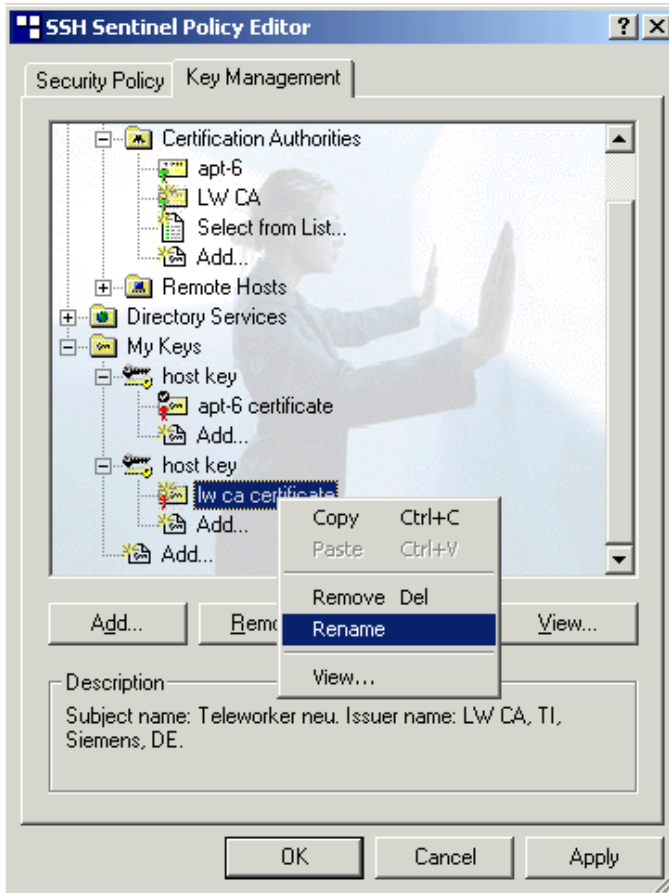
7. Import the peer certificate for the teleworker as follows:



The peer certificate is the certificate the VPN client uses to authenticate itself at the VPN server. The certificate must be formatted as a PKCS#12 file. Please note that the SSH client does not support certificates that use the "DSA" signature algorithm.

8. Because the PKCS#12 certificate also contains the private key, you must encrypt it with a password. When prompted, enter the password used for encrypting the PKCS#12 certificate.
9. Compare the fingerprint then displayed with the one you noted down earlier. Click "Yes" in the dialog showing the fingerprint if both fingerprints match.

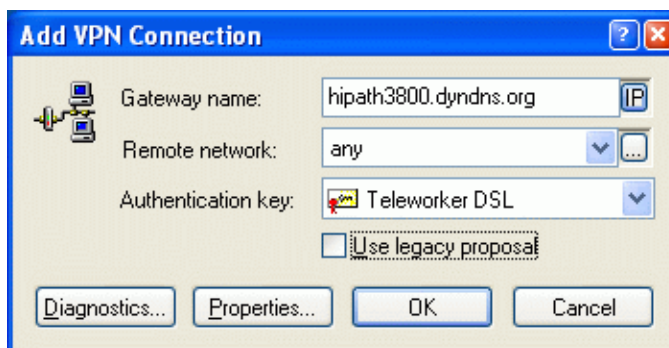
10. Rename the PKCS#12 certificate already imported as follows:



Renaming makes identification much easier at a later stage. All of the necessary certificates for tunnel configuration are now available. Please note that it is not possible/necessary to import the CRL in the SSH client.

11. Click "Apply" to save the data.
12. Now configure a new VPN tunnel under "VPN connections - Add Rule..." in the "Security Policy" tab.

The following dialog appears:



Practical Examples for HG 1500

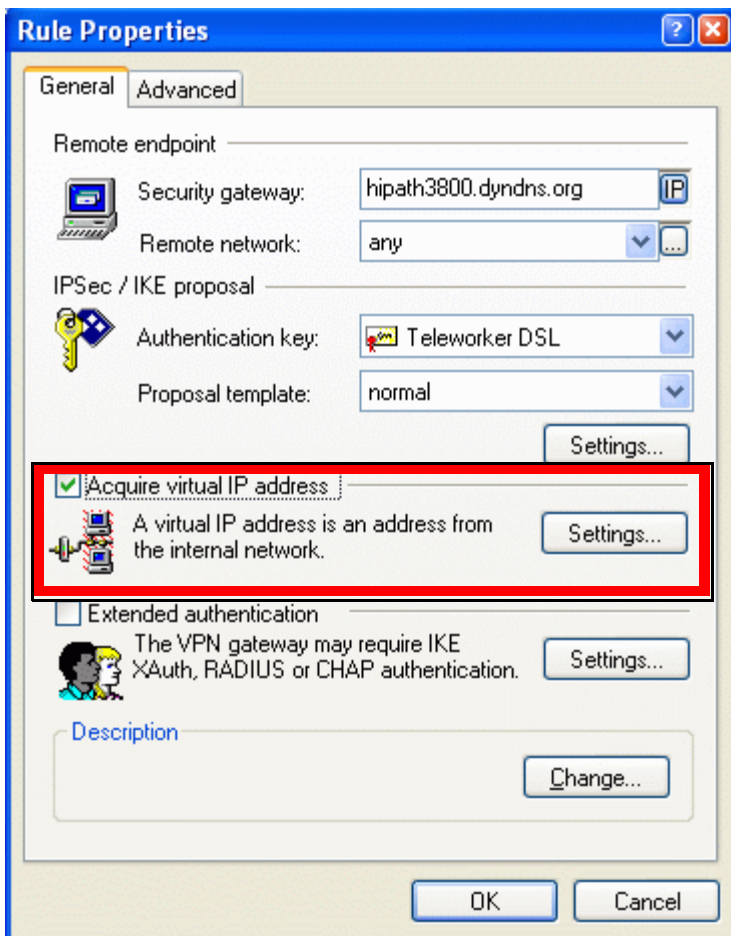
Setting up a VPN Configuration

Information on the fields:

- Under "Gateway IP address", specify the fixed public IP address or the DNS name of the VPN server (HG 1500). In our scenario enter the DNS name "hipath3800.dyndns.org" here. In the default the remote network "any" can be incorporated.
- Optional: Define the subnets that should be reached by the VPN tunnel under "Remote network".
- If the total IP traffic is routed through the tunnel (this is the standard case in the default since the IP traffic is monitored in the rules for the HG 1500), you can use the preconfigured network "any" (corresponds to 0.0.0.0). Note that a corresponding VPN rule must also be defined on the HG 1500 for any configured subnets. If a rule is not defined, the tunnel will not be configured.

13. In the "Authentication key" field, select the PKCS#12 certificate imported earlier.

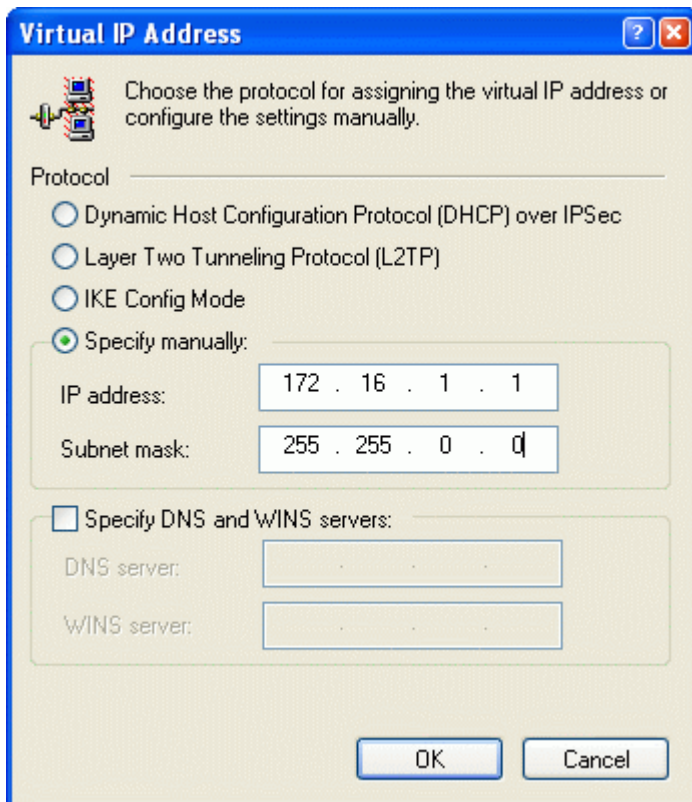
Click "Properties" to make further settings for the VPN client.



14. Activate "Acquire virtual IP address".

The appropriate VPN rules must be configured for the virtual IP address in the HG 1500. An encrypted connection from the virtual IP address to the remote network already configured must be permitted.

15. Click "Settings" to configure the virtual IP address. The following dialog appears:



16. Enter the address data as shown and confirm with "OK". Note that the VPN client's virtual IP address is located in a different subnet to the HG 1500 (VPN server) so that routing is possible.

You do not need to make any further settings on the VPN client for the VPN connection. Under "SA lifetimes" you can limit the validity of the negotiated key. This setting can and should be made on the HG 1500 during tunnel configuration, however. The default settings for "IPSec / IKE proposal" can also be retained. However, the use of AES encryption is recommended.

This concludes all activities with the SSH Sentinel Policy Editor.

Practical Examples for HG 1500

Setting up a VPN Configuration

17. Create the tunnel for the teleworker in the HG 1500 WBM:

"Explorers > Security > VPN > Tunnels > (right-click) Configured Tunnels > Add Tunnel".

Tunnel Name:	Teleworker
Local Tunnel Endpoint Type:	DNS Name
Local Tunnel Endpoint Address:	hipath3800.dyndns.org
Remote Tunnel Endpoint Type:	Host
Remote Tunnel Endpoint Address:	0.0.0.0
Suggested Encryption Algorithms:	AES and DES and 3DES
Suggested Hash Algorithms:	MD5 and SHA1
Session Key Handling:	Automatically, using IKE protocol
Suggested Lifetime of the Session Keys:	8 hours (default)
Suggested Lifetime of the Key Exchange Session:	10 minutes
Suggested Data Volume of the Session Keys:	unlimited (default)
Select the option "Key Exchange Data" and enter the key exchange parameter for this new tunnel:	
Session Key Handling:	Automatically, using IKE protocol
Suggested Diffie-Hellman Groups:	DH Group 2, DH Group 5
Activate 'Perfect Forward Secrecy':	Yes
VPN Peer Authentication Method:	Digital signatures
List of CA Certificates:	LWCA

Information on the fields:

- The tunnel is assigned the IP address 0.0.0.0 as endpoint address. This ensures that, irrespective of the teleworker's dynamic IP address, all teleworkers only use this particular tunnel.
- "Digital signatures" is used as the authentication procedure.

18. Define a rule to allow the teleworker to access the HG 1500 ("Teleworker Dial-In Rule"):
"Explorers > Security > VPN > Rules > (right-click) Configured Rules > Add Rule".

Configure the rule with the following data:

Priority:	64999
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address:	0.0.0.0
Destination Address Type:	Host
Destination Address IP Address:	0.0.0.0
Tunnel on Receive Side:	From teleworker
Tunnel on Transmit Side:	No Tunnel Assignment

Information on the fields:

- **Explanation:** This rule provides teleworkers with access during IKE negotiation (Phase1). If this rule were not available, the teleworker's connection request would be rejected immediately.
- **Priority:** The lowest possible priority is set.
- The **Source Address** should be configured at 0.0.0.0 because the IP address assigned to the teleworker by the ISP can be flexible.
- The **Destination Address** should also be 0.0.0.0 (default setting). Alternatively, the local destination network of the HG 1500 (192.168.1.0 for instance) can be configured for this.

A rule for the opposite direction is not needed in this case.

Practical Examples for HG 1500

Setting up a VPN Configuration

19. Define a rule for the teleworker's communication. The teleworker uses 172.16.1.1 / 16 as the "Virtual IP Address".

The destination address will be the subnet 192.168.1.0 / 24.

"Explorers > Security > VPN > Rules > (right-click) Configured Rules > Add Rule".

Configure the rule with the following data:

Priority:	200
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address: Subnet Address:	172.16.1.1
Destination Address Type:	Subnet
Destination Address IP Address: Subnet Address:	192.168.1.0
Destination Address Subnet Mask:	255.255.255.0
Tunnel on Receive Side:	From teleworker
Tunnel on Transmit Side:	No Tunnel Assignment

20. Now set up a counter rule for source address 192.168.1.0 for the teleworker's IP address: "Explorers > Security > VPN > Rules > Configured Rules > (right-click) selected rule > Add Rule for Opposite Direction".

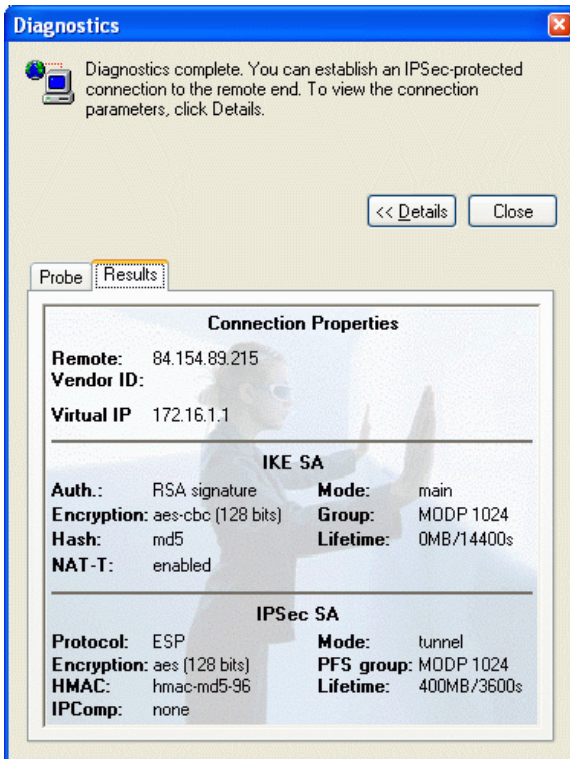
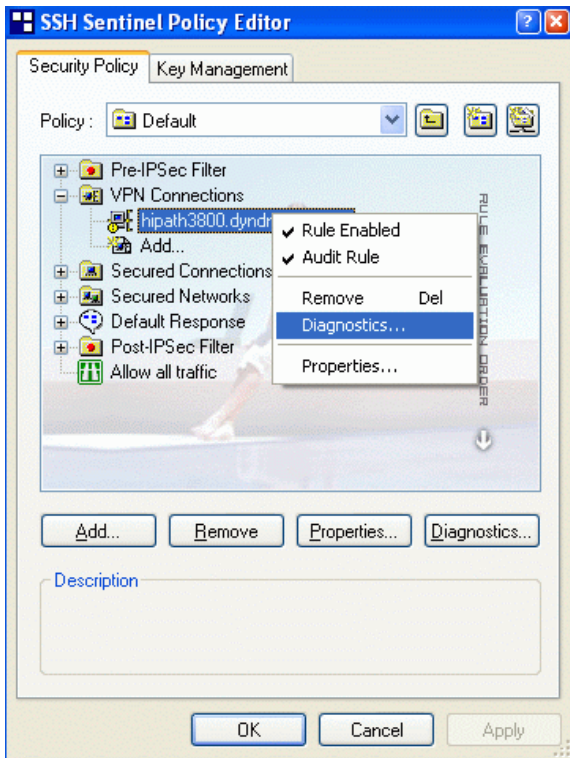
A rule with the following data is created automatically and simply needs to be accepted:

Priority:	200
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	yes
Enable Rule:	yes
Source Address Type:	Subnet
Source Address IP Address: Subnet Address:	192.168.1.0
Source Address Subnet Mask:	255.255.255.0
Destination Address Type:	Host
Destination Address IP Address:	172.16.1.1
Tunnel on Receive Side:	No Tunnel Assignment
Tunnel on Transmit Side:	From teleworker

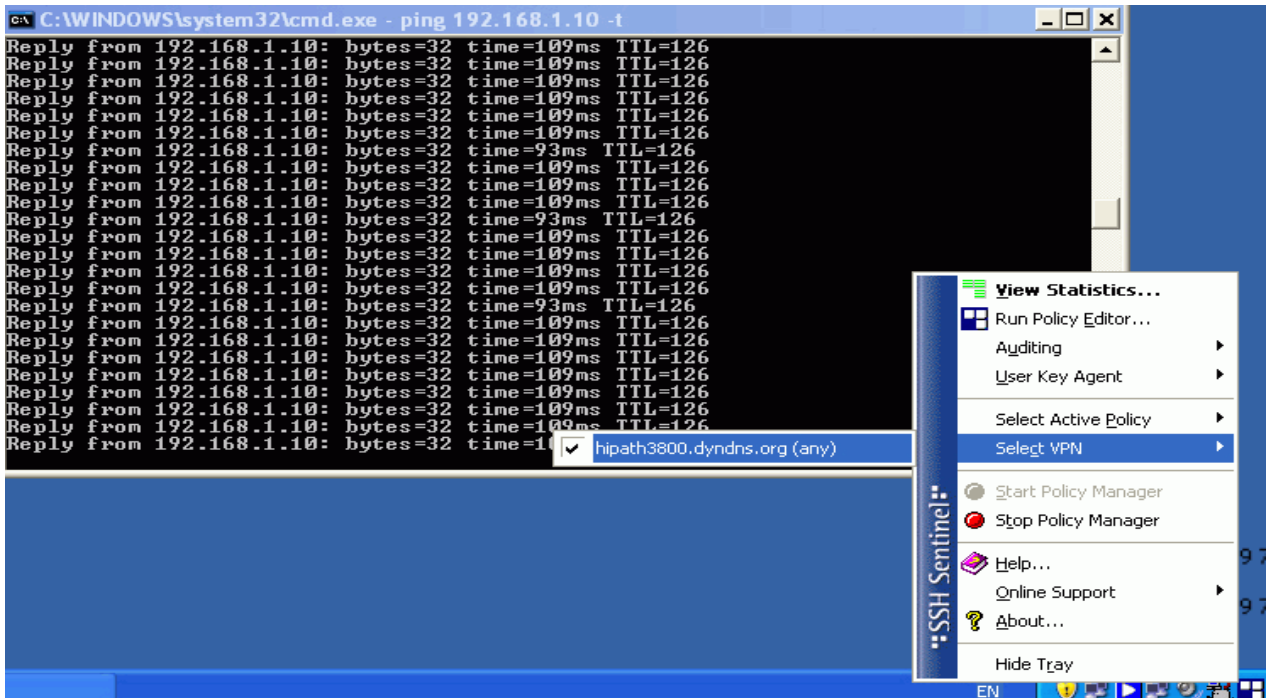
The SSH VPN client features a diagnostics function for checking the VPN connection. This indicates if IKE negotiation and tunnel configuration were successful.

Practical Examples for HG 1500

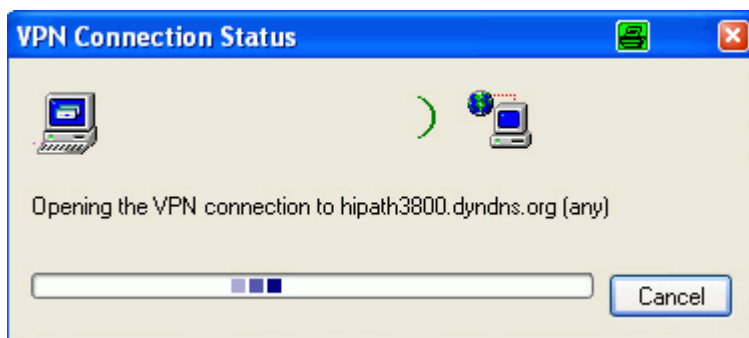
Setting up a VPN Configuration



21. Start the teleworker's VPN connection to his/her gateway manually. To do this, right-click the Sentinel icon on the Tray bar > Select VPN > and left-click the VPN connection:



Connection setup:



Once the connection has been successfully established you will receive a message to this effect (success!).

To check the routing function using the tunnel you have created, start a ping to an IP address on the remote side.

- To set up a VPN client (Teleworker 2 ISDN) on the HiPath 3500, repeat steps 2 - 16 while observing the modified configuration parameters.



What should be done if a teleworker encounters a DSL disconnect during a VPN connection to his/her gateway?

A Windows networking connection warning indicates connection loss in a separate window. Windows automatically attempts to reestablish the connection. Once the networking connection has been successfully reestablished, the teleworker must manually set up a VPN connection to the gateway. This is done by right-clicking the Sentinel icon on the Tray bar > Select VPN > and by left-clicking the required VPN connection.

Sentinel then establishes the VPN connection.

2.24.9 Connection Setup between Teleworkers

Additional VPN rules are required if the teleworker (currently connected with the HiPath 3800 system) wants to reach more networks. For example, to reach the host 172.20.20.1 / 16 (Teleworker 2 ISDN) you need to configure a rule with a counter rule that receives IP packets from the "From teleworker" tunnel (tunnel on the receive side) and forwards these to the "to HiPath 3500" tunnel (tunnel on transmit side).

- **Configuration of the HG 1500 on the HiPath 3800:**

Priority:	300
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address:	172.16.1.1
Destination Address Type:	Host
Destination Address IP Address:	172.20.20.1
Tunnel on Receive Side:	From teleworker
Tunnel on Transmit Side:	to HiPath 3500

1. Now configure the associated counter rule.

"Explorers > Security > VPN > Rules > Configured Rules > (right-click) selected rule > Add Rule for Opposite Direction".

In addition, you will need to incorporate a rule with a counter rule into the HG 1500 on the HiPath 3500 for communication between the teleworkers, which receives IP packets from the tunnel "to HiPath 3800" (tunnel on the receive side) and forwards them to the "From teleworker" tunnel.

Configuration of the HG 1500 on the HiPath 3500:

Priority:	300
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address:	172.16.1.1
Destination Address Type:	Host
Destination Address IP Address:	172.20.20.1
Tunnel on Receive Side:	to HiPath 3800
Tunnel on Transmit Side:	From teleworker

2. Now configure the associated counter rule.

To check the routing function using the configured tunnel, start a ping to the IP address on the remote side.

2.24.10 Teleworker 1 (DSL) Access to the Remote Station LAN

Additional VPN rules will be needed if you want to configure more teleworker networks. For example, for the subnet "192.168.2.0 / 24 (HiPath 3500 LAN), you need to configure a rule that receives IP packets from the "From teleworker" tunnel (tunnel on the receive side) and forwards them to the "HiPath 3500" tunnel (tunnel on transmit side).

1. Configure an additional VPN rule for each HiPath 3000 system for Teleworker 1 (DSL) access to the destination network 192.168.2.0 / 24.

HiPath 3800 Configuration:

Priority:	350
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address:	172.16.1.1
Destination Address Type:	Subnet

Practical Examples for HG 1500

Setting up a VPN Configuration

Destination Address IP Address: Subnet Ad- 192.168.2.0
dress
Subnet Mask: 255.255.255.0
Tunnel on Receive Side: From teleworker
Tunnel on Transmit Side: to HiPath 3500

2. Now configure the associated counter rule.

HiPath 3500 Configuration:

Priority: 350
Service: Any Service
Rule-Based Action: PASS
Encryption Required: Yes
Enable Rule: Yes
Source Address Type: Host
Source Address IP Address: 172.16.1.1
Destination Address Type: Subnet
Destination Address IP Address: Subnet Ad- 192.168.2.0
dress
Subnet Mask: 255.255.255.0
Tunnel on Receive Side: to HiPath 3800
Tunnel on Transmit Side: No Tunnel Assignment

To check the routing function using the configured tunnel, start a ping to an IP address on the remote side.

2.24.11 Internet Access for Teleworker 1 (DSL) via HiPath 3800

The VPN client that has just been configured does not permit Internet access. When the tunnel is successfully configured, all data packets are routed to the HG 1500. You will now need to configure another rule that will permit Teleworker 1 (DSL) to break out to the Internet:

Priority:	360
Service:	Any Service
Rule-Based Action:	PASS
Encryption Required:	Yes
Enable Rule:	Yes
Source Address Type:	Host
Source Address IP Address:	172.16.1.1
Destination Address Type:	Host
Destination Address IP Address:	0.0.0.0
Tunnel on Receive Side:	From teleworker
Tunnel on Transmit Side:	No Tunnel Assignment

A counter rule is not required.

To check the routing function using the tunnel you have created, start a ping to an IP address on the remote side.

2.24.12 Creation of Certificates for Multigateway Administration

Target Configuration

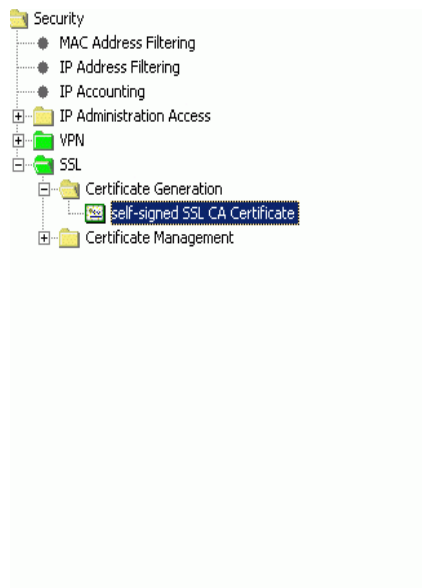
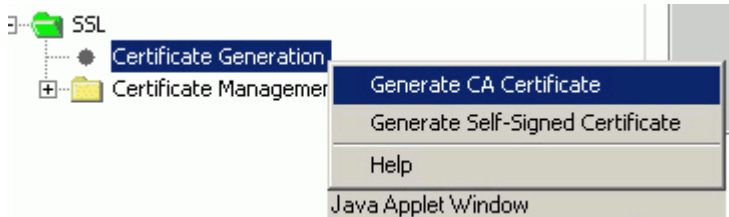
Configuration data from one HG 1500 should be transferred via a secure connection to other connected HG 1500 boards. For this purpose, each HG 1500 must be authenticated with a valid SSL server certificate.

PKCS#12 certificates for import into the HG 1500 are generated via the HG 1500 on the HiPath 3800. To do this you will need to configure a high-level certification authority (CA). In our example, this "virtual certification authority" should reside on the HG 1500 in the HiPath 3800.

Practical Examples for HG 1500

Setting up a VPN Configuration

1. Create a self-signed CA certificate in the HG 1500 on the HiPath 3800:
"Explorers > Security > SSL > (right-click) Certificate Generation > Generate CA Certificate".



Certificate Information

Certificate Name:	self-signed SSL CA Certificate
Certificate Type:	Self-Signed CA Certificate
Serial Number of Certificate:	1
Serial Number of Certificate (hex):	01
Type of Signature Algorithm:	md5RSA
Start Time of Validity Period (GMT):	Friday, 02/02/2007 00:00:00
End Time of Validity Period (GMT):	Thursday, 02/02/2017 00:00:00
CRL Distribution Point:	info: where is ssl-ca?

Issued by CA

Country (C):	DE
Organization (O):	Siemens Enterprise
Organization Unit (OU):	TI
Common Name (CN):	SSL-CA

Subject Name

Country (C):	DE
Organization (O):	Siemens Enterprise
Organization Unit (OU):	TI
Common Name (CN):	SSL-CA

Subject Alternative Name

--	-----

Public Key Encryption Data

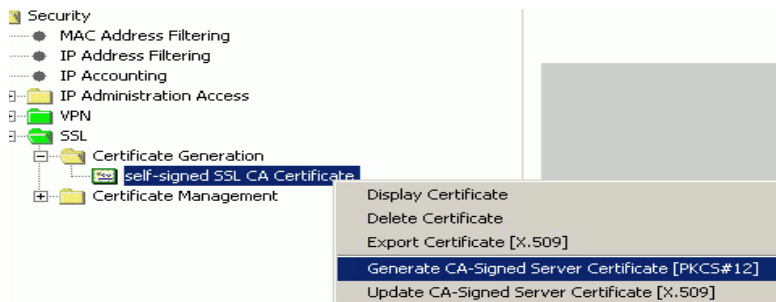
Public Key Length:	768
Public Key:	BA0E 9A79 48DE E5CA EAE7 3D2B D439 0407 4AF7 0245 C2AF A251 75A6 F7C9 670B 10D1 699C 7977
Fingerprint:	D14F 3B72 64BD 6784 AEEA 5FFF D59B 66F5 C81D 7AED

The CA certificate should have a validity period of at least 10 years. A CA certificate on the HG 1500 cannot be extended.

You can enter the URL of the originating certification authority as the CRL distribution point. This is `https://192.168.1.242` in our example. This only provides background information. For example, the generated certificate will contain information about who generated the certificate (in this example this is the HG 1500 on the HiPath 3800).

2. Use the self-signed CA certificate already created to generate a PKCS#12 CA-signed server certificate for the HG 1500 in HiPath 3800 and HiPath 3500 with the IP addresses 192.168.1.242 and 192.168.2.232:

"Explorers > Security > SSL > Certificate Generation > (right-click) selected certificate > Generate CA-Signed Server Certificate (PKCS#12)".



Practical Examples for HG 1500

Setting up a VPN Configuration

Generate SSL Server Certificate

Passphrase for encryption:	<input type="password" value="....."/>
Reenter Passphrase for encryption:	<input type="password" value="....."/>
Serial Number of Certificate:	<input type="text" value="2"/>
Type of Signature Algorithm:	md5RSA
Public Key Length:	<input type="text" value="768"/>

- Start Time of Validity Period (GMT) -

Day	Month	Year
<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="2007"/>
Hour	Min.	Sec.
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

- End Time of Validity Period (GMT) -

Day	Month	Year
<input type="text" value="2"/>	<input type="text" value="2"/>	<input type="text" value="2011"/>
Hour	Min.	Sec.
<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

- Subject Name -

Country (C):	<input type="text" value="DE"/>
Organization (O):	<input type="text" value="Siemens Enterprise"/>
Organization Unit (OU):	<input type="text" value="TI"/>
Common Name (CN):	<input type="text" value="192.168.1.242"/>

- Subject Alternative Name -

Distinguished Name Format Other Format

Subject Alternative Name:

CRL Distribution Point:

Use a sufficiently secure passphrase for encryption. After generation, you must save the certificate to a data medium (a USB stick for instance; after all the certificate needs to be transferred to the other HiPath somehow). To protect this "certificate transfer", the certificate is stored in encrypted format on the data medium.

3. Enter a unique serial number. The signature algorithm type is md5RSA and the length of the public key should be set to 768 bytes. The certificate validity period should be four years. Enter the IP address of the HG 1500 as the common name under Subject Name (in our example here 192.168.1.242 and 192.168.2.232).
4. Make a note of the fingerprint of the generated certificate and do not forget the passphrase for encryption.

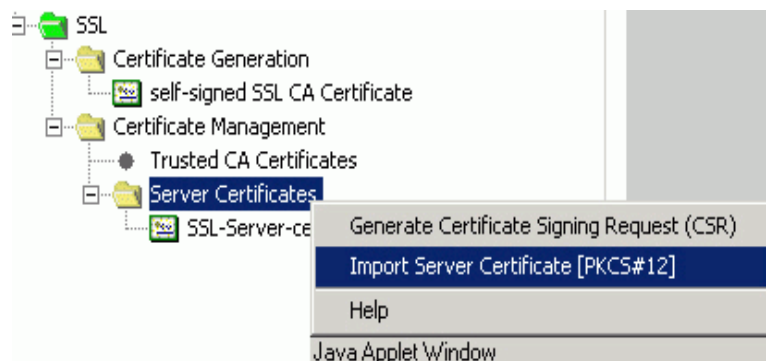


The local gateway cannot be selected for distribution.

You can now import the generated PKCS#12 certificate into the HG 1500 on the HiPath 3800 and HiPath 3500.

To do this you must also switch the HG 1500 to secure administration mode, in other words, configure SSL by first generating a certificate over V.24/CLI. If the board can then be administered over HTTPS, you can perform the following steps.

5. Import and activate the PKCS#12 certificates generated in the HG 1500 in the HiPath 3800 to the HG 1500 in the HiPath 3800 and 3500:
"Explorers > Security > SSL > Certificate Management > (right-click) Server Certificates > Import Server Certificate [PKCS#12]".



Use the passphrase for encryption you selected already. Always remember to compare the fingerprint.

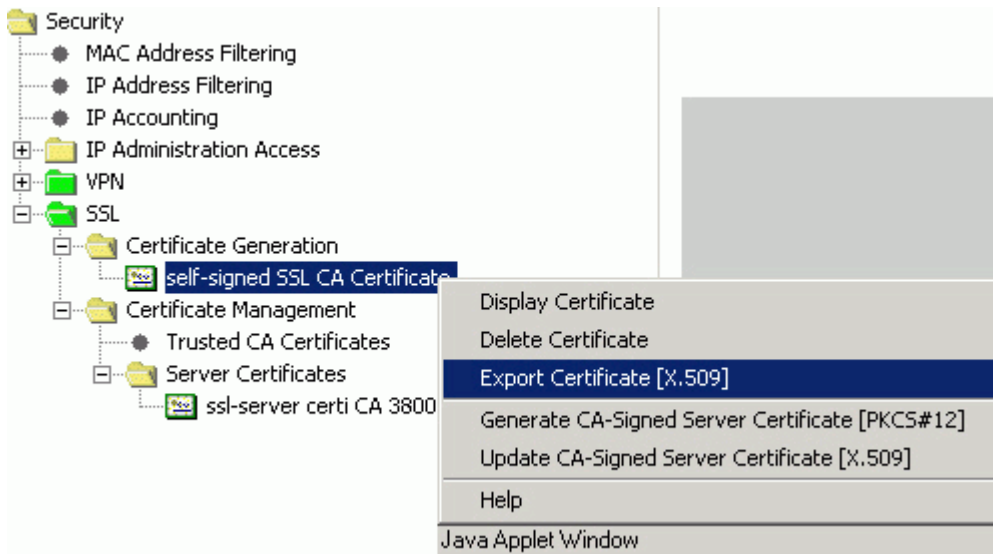
6. Delete the certificate that you generated with CLI on the HG 1500 in HiPath 3500 to start up SSL:
"Explorers > Security > SSL > Server Certificates > (right-click) certificate generated with CLI > Delete Certificate".
7. Delete the certificate that you generated earlier via WBM from the HG 1500 in the HiPath 3800:
"Explorers > Security > SSL > Server Certificates > (right-click) certificate generated with CLI > Delete Certificate".

Practical Examples for HG 1500

Setting up a VPN Configuration

Another certificate is required that describes the issuer of the SSL server certificates on the systems.

8. Generate this certificate by exporting the SSL CA X.509 certificate. In the example here, this can only be performed on the HG 1500 in HiPath 3800:
"Explorers > Security > SSL > Certificate Generation > (right-click) selected certificate > Export Certificate [X.509]".



9. Import the certificate exported in this way as a trusted CA certificate to all HG 1500 boards in the network:
"Explorers > Security > SSL > Certificate Management > (right-click) Trusted CA Certificates > Import Trusted CA Certificate [X.509]".

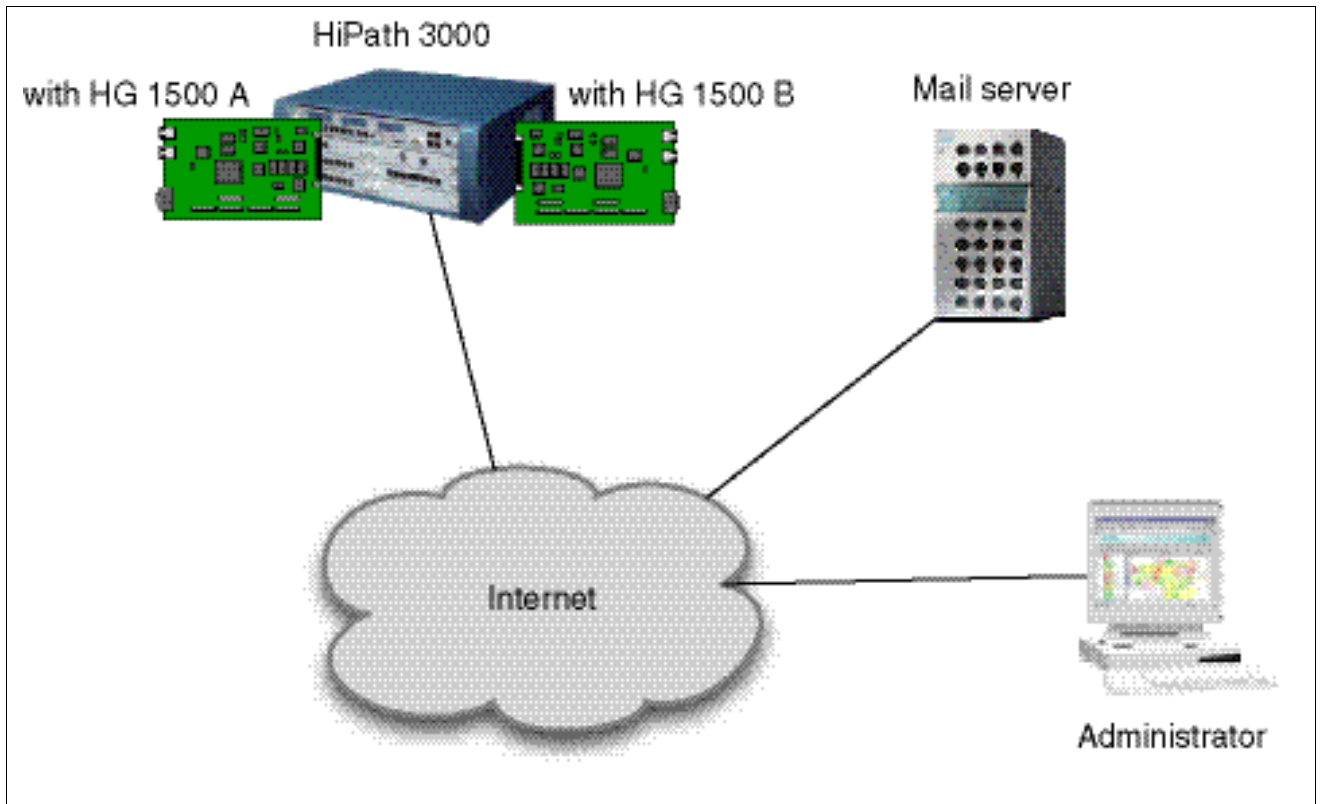


We recommend using descriptive meaningful names for exports/imports. This will help you to match the files created during an export with their purpose at a later date.

2.25 Setting up an E-Mail Connection

2.25.1 Target Configuration

An e-mail function enables notification to be sent to defined destination addresses when events occur. This function can be configured separately for each event.



Prerequisites

- A valid e-mail account must be set up on the destination mail server. The data of the e-mail server and the names of all e-mail addresses in use are known.

Restrictions

- No authentication methods are supported for SMTP. The e-mail server cannot therefore request any authentication.
- All e-mail addresses are stored on the same mail server. E-mails cannot be relayed.

2.25.2 WBM Settings

1. Specify the data for the destination mail server, the originator and the subject of the mail. Ensure that the board sending the e-mail is clearly identified in the "From" field. The subject should provide a clear indication of the triggering event.
2. Activate the "Send an E-mail" function for every event that is to be monitored via e-mail.
3. Save the settings.

2.26 SNMP with HG 1500

2.26.1 Target Configuration

The SNMP function of the HG 1500 should be enabled. PCs in the local network should be assigned read-only access to the SNMP traps using the password "hipath", and read and write access using the password "admin". However, only one PC (IP 1.150.1.10) should be granted read and write authorization.

The Advent MIB browser should be installed as the SNMP client.

The system name and location of the HG 1500 should be configured. The corresponding SNMP values "sysName" and "sysLocation" should then be checked using the default MIB file. The data for system name and location should then be edited using the MIB browser. An "Error Message" in the event of problems in the HG 1500 should also be enabled. The TrapWatcher program should be used to check that it is functioning correctly.

2.26.2 Configuration Steps

1. Activate the SNMP function of the HG 1500. Configure the password "hipath" for read-only access for the PCs in your local network, and the password "admin" for read and write access. Read and write authorization is only granted to the PC 1.150.1.10.

To do this, use WBM to configure a read community with the name "hipath" for each PC in the IP address range 1.150.1.x. Always assign "hipath" as the community name: WBM: "Maintenance > SNMP > Communities > Read Communities > (right-click) Add Read Community".

Configure a write community with the community name "admin" for the PC with the IP address 1.150.1.10.

WBM: "Maintenance > SNMP > Communities > Write Communities > (right-click) Add Write Community".

If you then display the configured communities, this should look as follows:

List of Communities

IP Address	Community	Type
1.150.1.10	admin	Write Community
1.150.1.10	hipath	Read Community
1.150.1.11	hipath	Read Community

2. Install the Advent MIB browser (\mib_browser\AdvN3201.EXE).

Practical Examples for HG 1500

SNMP with HG 1500

- Use the HG 1500 WBM to configure a contact address, system name and location for SNMP administration on the HG 1500:
WBM: "Explorers > Basic Settings > Gateway > (right-click) Edit Gateway Properties".

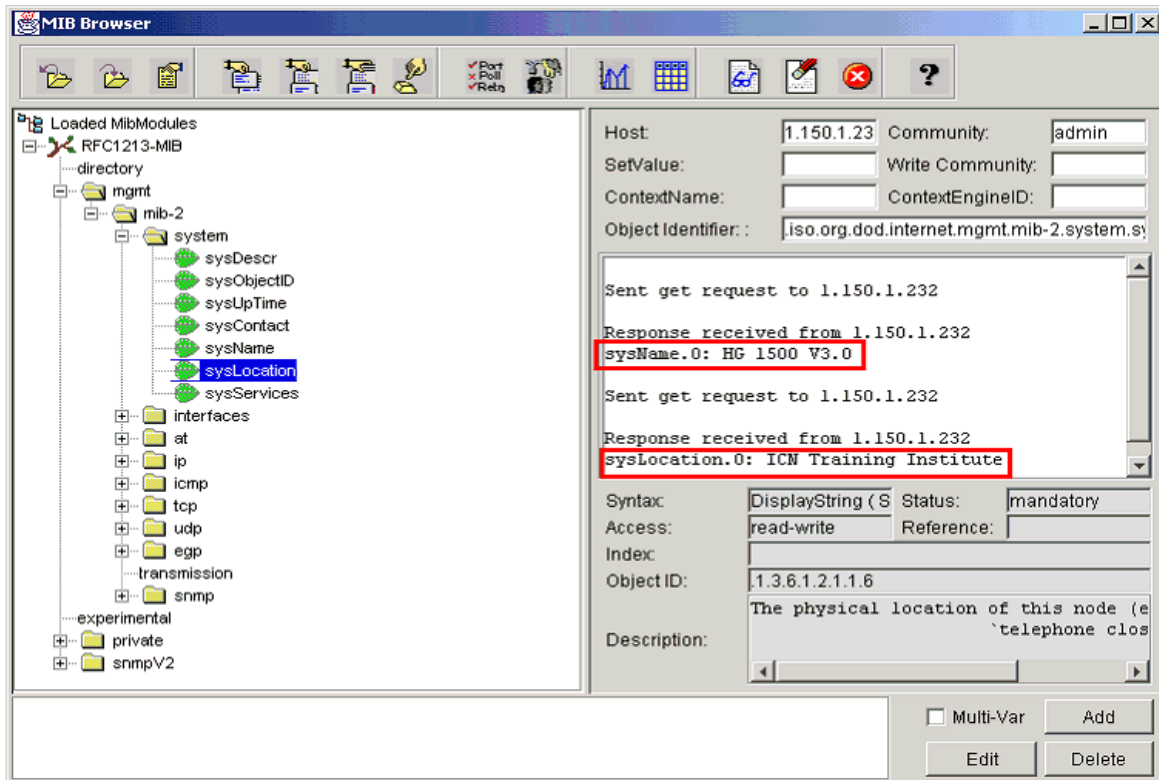
Once completed, the mask should look as follows:

Gateway Properties

General	
HG 1500 Slot Number:	0
System Name:	hg1500
Gateway Location:	
Contact Address:	
System Country Code:	49 (Germany)
Function Type:	Signaling and Media Gateway
Gateway IP Address:	192.168.1.146
Gateway Subnet Mask:	0.0.0.0

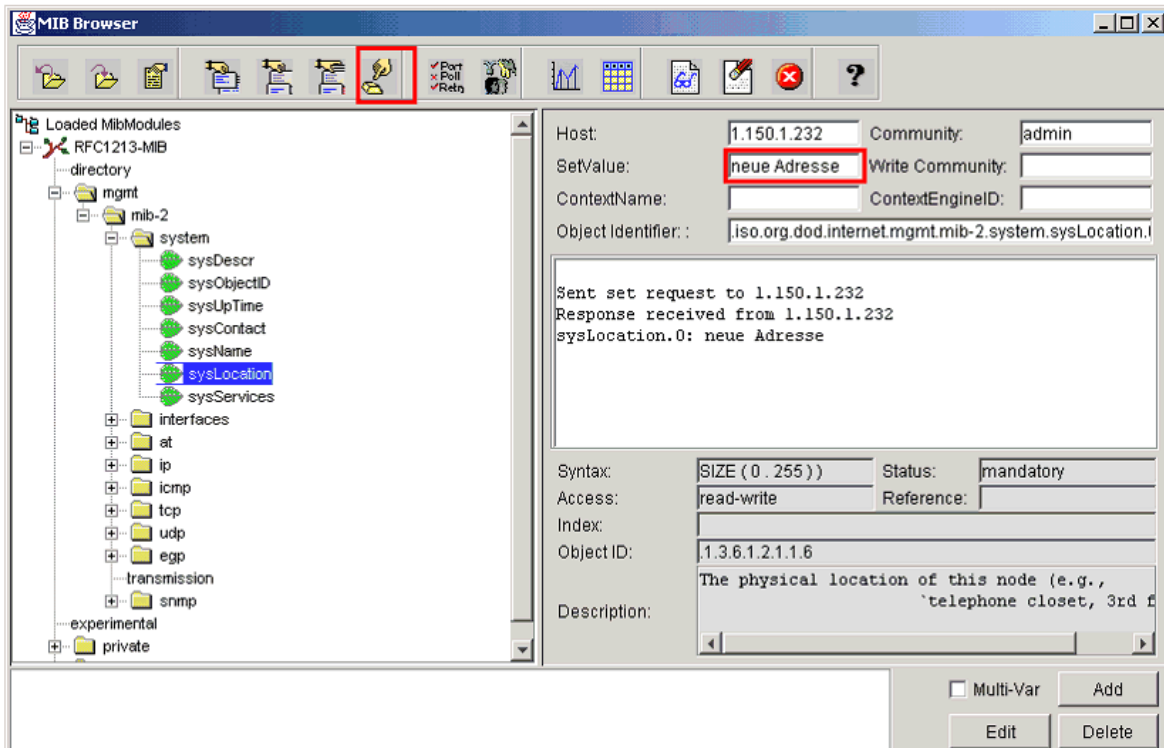
This data can now be requested using the SNMP protocol.

- Open the previously installed Advent MIB browser. Check whether the gateway properties can be viewed as shown in the following screenshot.



- Now edit the data for contact, system name, and location using the MIB browser. You will need SNMP write authorization for this purpose. In the sample configuration selected here, the data can only be edited via the PC with the IP address 1.150.1.10, which is a subscriber belonging to the write community "admin".

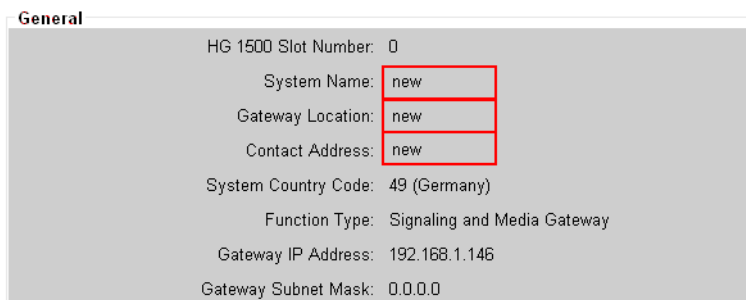
To edit the data in the MIB browser's Explorer view, select the entries "sysContact" (contact), "sysName" (system name), and "sysLocation" (location). You can edit the relevant field value in the "SetValue" field at the top right of the MIB Browser window.



The modified data is sent to the HG 1500 with a "Set" command when you click "Edit". Note that you must have write authorization ("admin" community) for this action.

- Now check WBM to see if the gateway properties have changed: WBM: "Explorers > Basic Settings > Gateway > (right-click) Display Gateway Properties".

Gateway Properties



Practical Examples for HG 1500

SNMP with HG 1500

7. An "Error Message" in the event of problems in the HG 1500 should now be enabled.

Use WBM to configure a trap community with the name "public" for the IP address range 1.150.1.10.

WBM: "Maintenance > SNMP > Communities > Trap Communities > (right-click) Add Trap Community".

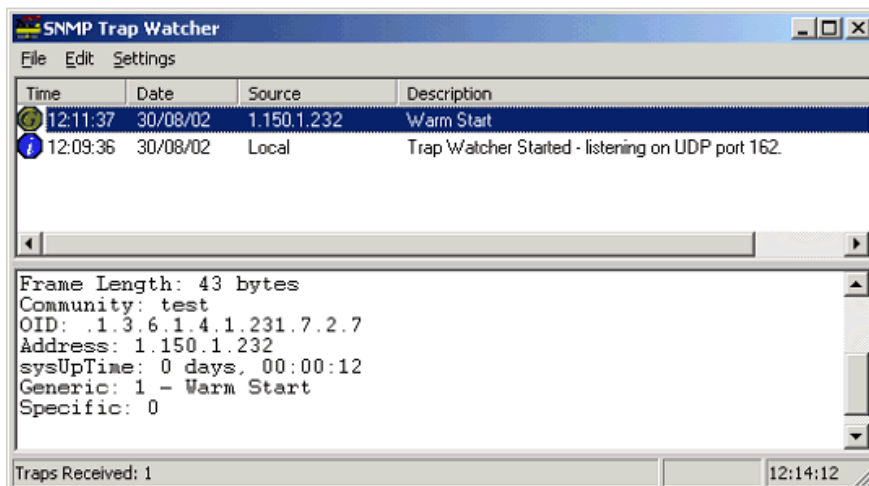
If you then display the trap community "public", it should look as follows:

Trap-Community

IP-Adresse: 1.150.1.10
Community: public

8. Activate the TrapWatcher (mib_browser\SNMPtrap.exe) on the administration PC.
9. Perform a restart of the HG 1500 via WBM (reset icon in lower window area).

Following the HG 1500 restart, the board generates a trap message to the entered PC. This should be displayed in the TrapWatcher as shown in the following screenshot:

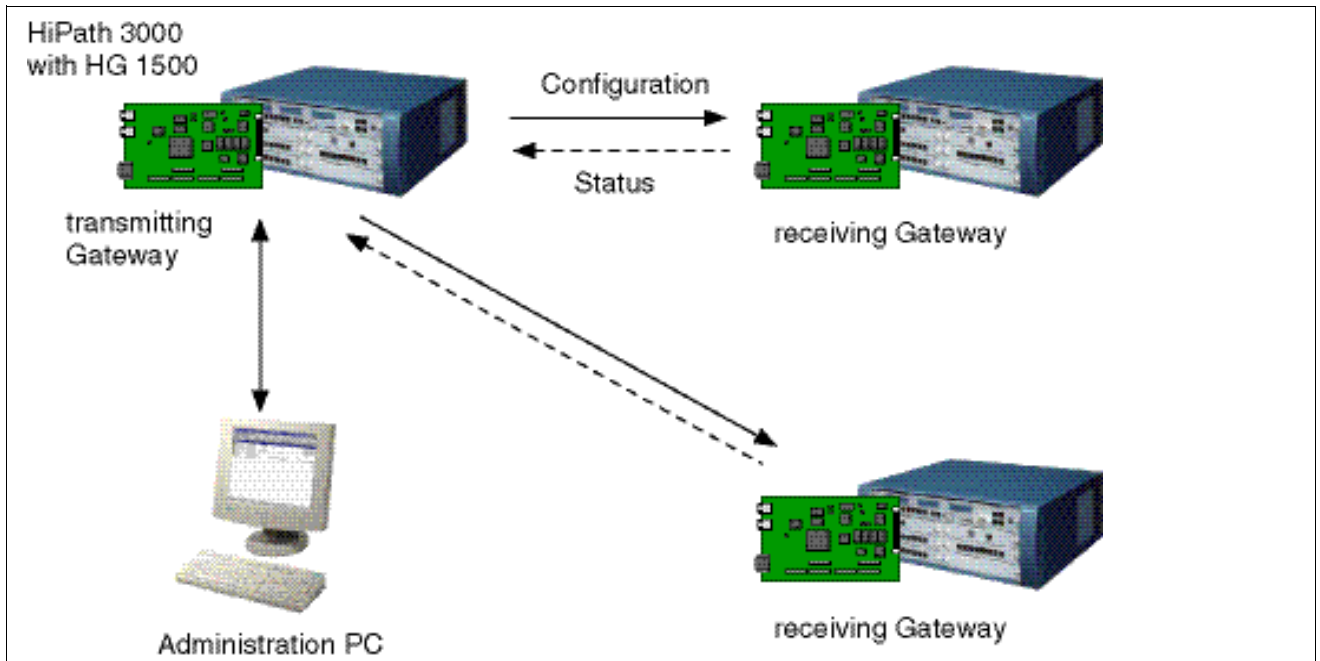


2.27 Multigateway Administration

2.27.1 Target Configuration

To simplify the configuration of multiple boards, you can use the "Multigateway Administration" function to distribute selected configuration tables to other gateways.

There is only ever one transmitting gateway and one or more receiving gateways.



Prerequisites

- The gateway whose configuration is to be distributed must have direct IP access to the receiving gateways.
- The administration PC must have direct IP access to the gateway whose configuration is to be distributed.
- All gateways must use the same WBM port (for example, 8085).
- The WBM port of the receiving gateways must be accessible for the transmitting gateway (external routers, hubs, firewalls and proxy servers must be transparent for this port).
- The WBM port of the transmitting gateway must be accessible for the administration PC (external routers, hubs, firewalls and proxy servers must be transparent for this port).
- You must be logged on to WBM with a login that is authorized for multi-gateway use.
- The login used must be available at all receiving gateways.

Practical Examples for HG 1500

Multigateway Administration

- You must use the same password to log on at any of the gateways involved.



The local gateway cannot be selected for distribution.

2.27.2 Configuration Steps

1. Ensure that the IP and MAC address filtering settings at the gateways permit connection to the transmitting or receiving gateway.

Ensure that the IP and MAC address filtering settings at the transmitting gateway permit connection to the administration PC.

To do this use the WBM Explorer "Security".

2. Ensure that the interfaces used are correctly configured:

Interface	Remark
LAN2 (Ethernet)	if a receiving gateway is connected via the second LAN interface
LAN2 (DSL)	if a receiving gateway is reached via PPP
HIP	if the HiPath gateways are connected via ISDN

3. Check that all the required gateways are included in the list of gateways for distribution.



The list of gateways to which configuration data should be distributed should not be too long. Otherwise, it will take quite a while for the WBM to be available again for other functions.

4. In the list of configuration tables, specify which tables are to be distributed.
5. Start the distribution routine and check the status of the processed jobs with the "Display List of Jobs" function.

3 Signaling & Payload Encryption (SPE) – Encryption

This chapter describes in detail how to configure signaling & payload encryption (SPE) for practical use. The SPE feature is provided in HiPath 3000/5000 from V7 R4 or later. This allows station-specific encryption of both signaling and payload data.



HG 1500 must have already been configured under Basic Settings. Please note that write access must be enabled before you can add, edit or delete configuration data in WBM. This is not explicitly indicated in the individual examples.

3.1 Overview

This document covers the topics listed in the table below.

Topic
SPE Configuration in a HiPath 3000/5000 from V7 R4 Environment, page 3-2
Generating SPE Certificates via the HG 1500 WBM, page 3-4
Setting Parameters for the SPE Security Configuration, page 3-11
Setting System Flags for SPE via HiPath 3000 Manager E, page 3-12
DLS - SPE Certificate Deployment, page 3-14
Automatic SPE Configuration via DLS, page 3-25
SPE Secure Trace, page 3-26

Signaling & Payload Encryption (SPE) – Encryption

SPE Configuration in a HiPath 3000/5000 from V7 R4 Environment

3.2 SPE Configuration in a HiPath 3000/5000 from V7 R4 Environment

3.2.1 Prerequisites for Configuration

The following prerequisites must be met before you can configure SPE at a HiPath 3000/5000 system.

Prerequisites

The following prerequisites must be met before you can activate SPE:

- All HiPath systems, IP gateways, and IP terminals (see [Section 3.2.1.1](#)) must support SPE (if necessary, upgrade to the relevant version).
- All HiPath systems, IP gateways, IP terminals, and the DLS must be synchronized (see [Section 3.2.1.2](#)); the time/time zone must be configured via SNTP/NTP.
- SPE certificates and a CA certificate must be deployed for all IP gateways (HG 1500, HG 3500 and HG 3575) in the systems.



If encryption has been activated on a HG 1500 board, the number of B channels configured must be 20% less than when encryption is deactivated.

The certificates are deployed to the IP gateways via DLS from the customer's Public Key Infrastructure (PKI).

- Once the SPE certificates have been configured and activated (in the IP gateways and IP terminals), the SPE feature must be configured in HiPath 3000 Manager E via system flags (see [Section 3.5](#)) and then activated by a system reset.

3.2.1.1 Telephones with SPE support

Signaling & Payload Encryption is only supported by HFA terminals.

The following HFA terminals support the encryption:

- optiPoint 410 (not optiPoint 410 entry, optiPoint 410 economy)
- optiPoint 420 (not optiPoint 420 economy)
- optiClient 130
- OpenStage CorNet IP (HFA)
 - 20 E, 20, 20 G
 - 40, 40 G
 - 60, 60 G
 - 80, 80 G

Analog fax machines or modems can be connected to the corporate LAN via the IP adapter, HiPath AP 98 1120. HiPath AP 1120 does not support encryption, but can still be operated in the company network.

3.2.1.2 Time Synchronization of all HiPath 3000/5000 Systems and IP Terminals

All HiPath 3000/5000 systems and IP terminals must operate with chronological synchronism and be synchronized by the NTP or SNTP server.

optiPoint 410/420 telephones also operate with the system time.

At present, OpenStage terminals only operate on the system time of the HiPath systems.

Signaling & Payload Encryption (SPE) – Encryption

Generating SPE Certificates via the HG 1500 WBM

3.3 Generating SPE Certificates via the HG 1500 WBM

You can start SPE certificate generation and deployment once all HiPath systems, IP gateways, and IP terminals have been upgraded to the necessary software version. The following examples show the simplest way to implement SPE in a HiPath 3000/5000 environment from V7 R4 or later.

3.3.1 Certificate Generation

This function is only available if SSL is enabled. You can generate CA certificates and self-signed server certificates. You can view, delete or export generated CA certificates using the Certificate Generation function. In addition, you can create or update server certificates using your own CA certificate.

WBM path:

Select: WBM > Explorers > Security > SSL > Certificate Generation.

Right-click Certificate Generation to display a menu containing the following entries:

- > "Generate CA Certificate"
- > "Generate Self-Signed Certificate"

Certificate Generation (folder):

If you have already generated CA certificates (see Section 3.3.2, "Generating the Root CA Certificate"), Certificate Generation is displayed in the tree structure as an expandable folder. In this case, double-click "Certificate Generation" in the tree structure to view CA certificates.

Right-click the individual CA certificates to display a menu containing the following entries:

- > "Display Certificate"
- > "Delete Certificate"
- > "Export Certificate [X.509]"
- > "Generate CA-Signed Server Certificate [PKCS#12]"
- > "Update CA-Signed Server Certificate [X.509]"

3.3.2 Generating the Root CA Certificate

A root CA certificate must first be created with `md5RSA` or `sha1RSA` as the signature algorithm type. A root certificate is the primary certificate in a PKI and is always a self-signed CA certificate. After you generate the root CA certificate (self-signed SSL-CA certificate), the certificate generated is checked.



The fingerprint and information about the private key of the root CA certificate and other certificates are stored in a file for subsequent archiving (refer to the customer's security guidelines).

WBM path:

1. Select: WBM > Explorers > Security > SSL > Certificate Generation > Generate Self-Signed Certificate.

The Generate self-signed SSL CA Certificate mask is displayed. You can edit the following fields:

- "Certificate Name:"
This field contains the certificate name. Enter the `root` CA certificate name in this field.
- "Serial Number of Certificate:"
Enter a serial number that you defined in this field (e.g., 1). The number must be a positive integer.



A serial number that is used once may not be used for another certificate as the serial number must be unique for every certificate that is created.

- "Type of Signature Algorithm:"
Select the signature algorithm to be used for this certificate (`md5RSA`). You can choose either `md5RSA` or `sha1RSA`.
- "Public Key Length:"
Select the key length used for this certificate (`1024`) as specified in the SPE Security Setup table under Explorers > Security > Signaling and Payload Encryption (SPE).
- "Start Time of Validity Period (GMT):"
Enter the start time for certificate validity in these fields. The time specified is interpreted as Greenwich Mean Time (GMT).
- "End Time of Validity Period (GMT):"
Enter the end time for certificate validity in these fields. The time specified is interpreted as Greenwich Mean Time (GMT).

Signaling & Payload Encryption (SPE) – Encryption

Generating SPE Certificates via the HG 1500 WBM

- "Subject Name:"
Specify the name of the subject who requested the certificate according to the conventions of the X.509 standard; for example, enter
 - DE for Germany in the "Country (C):" field
 - "Organization (O):" Siemens AG
 - "Organization Unit (OU):" Com Enterprise Systems
 - "Common Name (CN):" HiPath Gateway
 - "Subject Alternative Name:"
This optional information distinguishes between the "Distinguished Name Format" (such as, the data under "Subject Name") and "Other Format" (for example, the IP address entry). The input mask is dependent on the selected format.
 - "CRL Distribution Point:"
In this optional field, you can enter a URL to specify the location from which certificate revocation lists (CRL) are to be distributed.
2. Click "Generate Certificate".

3.3.3 Saving the Root CA Certificate

Save the root CA certificate.

1. Click "OK".
2. Click the diskette icon in the control area to save your changes permanently.

3.3.4 Displaying the Root CA Certificate

You can display and check the root CA certificate (self-signed SSL-CA certificate). This is only possible if you have already generated at least one CA certificate.

WBM path:

Select: WBM > Explorers > Security > SSL > Certificate Generation > Root CA > Display 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.

3.3.5 Generating a Server Certificate (Peer Certificate)

You must generate a peer certificate for every HG board when you finish generating the root CA certificate.

You can generate CA certificates and self-signed server certificates. This is only possible if you have already generated at least one CA certificate.

PKCS#12 files (PKCS#12 stands for "Personal Information Exchange Syntax Standard") save certificates with the private key. A PKCS#12 file therefore contains the necessary data for personal encryption and decryption.

WBM path:

1. Select: WBM > Explorers > Security > SSL > Certificate Generation > Root CA > Generate CA-Signed Server Certificate [PKCS#12].

The "Generate SSL Server Certificate" mask is displayed. You can edit the following fields:

- "Passphrase for encryption:"
Enter a password that you have defined (with at least seven characters) in this field. This password is requested if you want to import or view a PKCS#12 file. Take note of the public key length. The public key length must be identical in the SSL server certificate and the root CA certificate; a public key length of 1024 bits must be used (HG default).
- "Reenter Passphrase for encryption:"
In this field, repeat the password specified above.
- "Serial Number of Certificate:"
Enter a serial number that you defined in this field. The number must be a positive integer.



A serial number that is used once may not be used for another certificate as the serial number must be unique for every certificate that is created.

- "Subject Name:"
Specify the name of the subject who requested the certificate according to the conventions of the X.509 standard; for example, enter
 - DE for Germany in the "Country (C):" field
 - "Organization (O):" Siemens AG
 - "Organization Unit (OU):" Com Enterprise Systems
 - "Common Name (CN):" 1.150.88.232

Signaling & Payload Encryption (SPE) – Encryption

Generating SPE Certificates via the HG 1500 WBM

The IP address of the LAN1 interface ("1.150.88.232", for instance) should always be used as the "Common Name (CN)" for HG 1500. For security reasons, the passphrase for decryption should be made up of letters, digits, and special characters.

The other fields are the same as those available when generating an SSL server certificate (see Generating the Root CA Certificate).

2. Click "Generate Certificate".

3.3.6 Saving the SSL Server Certificate (Peer Certificate)

A window opens in the Web browser when you click "Generate Certificate" and lets you give the certificate file a name and save it in a location of your choice.

When prompted to save the "PKCS#12 certificate", make sure you enter a unique name for peer certificate generation, for instance, "Mch-Lab-H3500-IP-1-150-88-232-HG1500-EB5-Peer.p12".

The SSL server certificate must be imported later into the relevant HG board as an "SPE key certificate" once all certificates have been generated.

3.3.7 Exporting the Root CA Certificate as "X.509"

The root CA certificate must be exported as "X.509" if all peer certificates have been generated.

X.509 is a standard for certificates. The name and the digital signature of the person who issued the certificate are also saved in the certificate. X.509 is part of the X.500 directory service for world-wide, distributed, and open systems.

WBM path:

Select: WBM > Explorers > Security > SSL > Certificate Generation > Root CA > Export Certificate [X.509].

The Web browser displays a window that lets you give the file a name and save it in a location of your choice. The certificate name is used for the file name.

3.3.8 Importing the SSL Server Certificate [PKCS#12]

The SSL server certificate [PKCS#12] must be imported into all HG 1500s where SPE is active for SPE.

WBM path:

1. Select: WBM > Explorers > Security > SSL > Signaling and Payload Encryption (SPE) > SPE Certificate > Import SPE certificate plus private key (PEM or PKCS#12).

The "Load a SPE Key Certificate via HTTP" mask is displayed. You can edit the following fields:

- "Passphrase for decryption:"
In this field, enter the password which was used for creating the PKCS#12 file (for certificate generation).
- "File with certificate and private Key (PEM or PKCS#12 format):"
Specify the path and name of the file which contains the certificate data to be imported. Click "Browse" to open a window to search for the file.



An automatic reset is performed the first time you install a certificate when SPE is active.

2. 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. Appropriate measures should be taken.

3. Click "Import Certificate from File" if you are satisfied with the fingerprint check.

3.3.9 Checking the SSL Server Certificate

You can display and check the SSL server certificate.

WBM path:

Select: WBM > Explorers > Security > SSL > Signaling and Payload Encryption (SPE) > SPE Certificate > SPE Certificate.

The "Certificate Information" mask is displayed and can be checked.

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.

Signaling & Payload Encryption (SPE) – Encryption

Generating SPE Certificates via the HG 1500 WBM

3.3.10 Importing an Exported Root CA Certificate

The exported root CA certificate must now be imported into all HG 1500s.

WBM path:

1. Select: WBM > Explorers > Security > SSL > Signaling and Payload Encryption (SPE) > SPE CA Certificate(s) > Import trusted CA Certificate (PEM or Binary).

The "Load a SPE CA Certificate via HTTP" mask is displayed. You can edit the following fields:

- "File with certificate (PEM or binary):"
Enter the path and file name of the PEM or binary file you want to import. Click "Browse" to open a window to search for the file.
 - CRL Distribution Point (CDP) Protocol:
Select "LDAP" as the CDP.
A CDP is an optional certificate extension. An imported certificate is only checked against the CRLs for which the CDP was configured.
2. 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. Appropriate measures should be taken.

3. Click "Import Certificate from File" if you are satisfied with the fingerprint check.

3.4 Setting Parameters for the SPE Security Configuration

You can set parameters for the SPE security configuration.

WBM path:

1. Select: WBM > Explorers > Payload > Signaling & Payload Encryption (SPE) > Show Security Configuration.

The "SPE Security Setup" mask is displayed. This window contains for the following security settings for SPE (that is, for the encryption of signaling and payload data for communication between the gateway and the VoIP clients and between the two gateways):

- "Minimal length of RSA keys:" 1024.
 - "Certificate validation with CRL verification required:" No.
 - "Minimum Re-Keying interval [hours]:" 24.
 - "Subjectname check:" No.
 - "Salt Key Usage:" Yes.
 - "SRTP authentication required (SRTP: Secure Realtime Transport Protocol): Yes.
 - "SRTCP encryption required (SRTCP: Secure Realtime Transport Control Protocol): Yes.
 - "SRTP/SRTCP authentication tag length:" 80
2. Accept the default parameters.

3.5 Setting System Flags for SPE via HiPath 3000 Manager E

To be able to use the SPE feature, you must first set the appropriate SPE system flags and then activate them by resetting the system.



The SPE system flags can only be set via HiPath 3000 Manager E.

Setting system flags for SPE

The following system flags must be deactivated or activated:

- **"No security" flag**

1. Select: Systemview > Settings > Network > Gatekeeper > H.323/TS - Security.
2. Deactivate the "No security" flag.

The H.235 security protocol is not used if this flag is deactivated. No crypto tokens are sent by the IP clients.

- **"SPE Support" flag**

1. Select: Systemview > Settings > System parameters > Flags > Switches.
2. Activate the "SPE Support" flag.

If this flag is activated, the signaling and payload data and the authentication data are encrypted.

- **"Payload Security" flag**

1. Select: Stationview > Activated features > Payload Security.
2. Activate the "Payload Security" flag ("ON").

If this flag and the "SPE support" flag are activated, signaling and payload data is encrypted for the selected station(s).

- **"SPE Advisory Tone" flag**

1. Select: Systemview > Settings > System parameters > Flags > Switches.
2. Activate the "SPE Advisory Tone" flag.

If this flag is activated, subscribers are informed of encryption status changes by a beep. The call status ("Secure Call" or "Standard Call") is briefly indicated on the terminal at the start of the call (not for analog telephones).

3.6 Configuring an optiPoint 410/420 Telephone for SPE

You must configure the optiPoint 410/420 telephone via WBM and Manager E before you can use the SPE feature.

Configuration via WBM (HG 1500)

1. Select: Administration > Settings > System > Security settings.
The "Security settings" mask is displayed.
2. Set the "Transport mode" parameter to "TLS".
3. Click "Submit".

Configuration via Manager E

1. Select: Systemview > Settings > Network > IP Ports.
The "IP Ports" table contains all values for which the IP port can be modified.
2. Enter the values for the new IP ports in the Port no. column.



The "H323-TLS" parameter corresponds to the "H.225 TLS port" parameter in WBM.

The modified ports are activated the next time the application system is restarted.

3.6.1 Displaying Connection Information on an IP Phone's Screen

At the start of a secure SPE connection, the IP phone's display indicates the call status as "Secure Call" for approximately 5 seconds.

In the case of a "non-secure" connection, the display indicates the call status as "Standard Call" for approximately 5 seconds at the start of the call.

3.6.2 Configuring a Key for Secure Status Display

You can configure a key on the optiPoint 410/420 phone for secure status display (during a call) (see Section 1.4, "Programming and Labeling Keys"). You can press this key during a call to show the current secure status on the optiPoint 410/420 phone's display.

Signaling & Payload Encryption (SPE) – Encryption

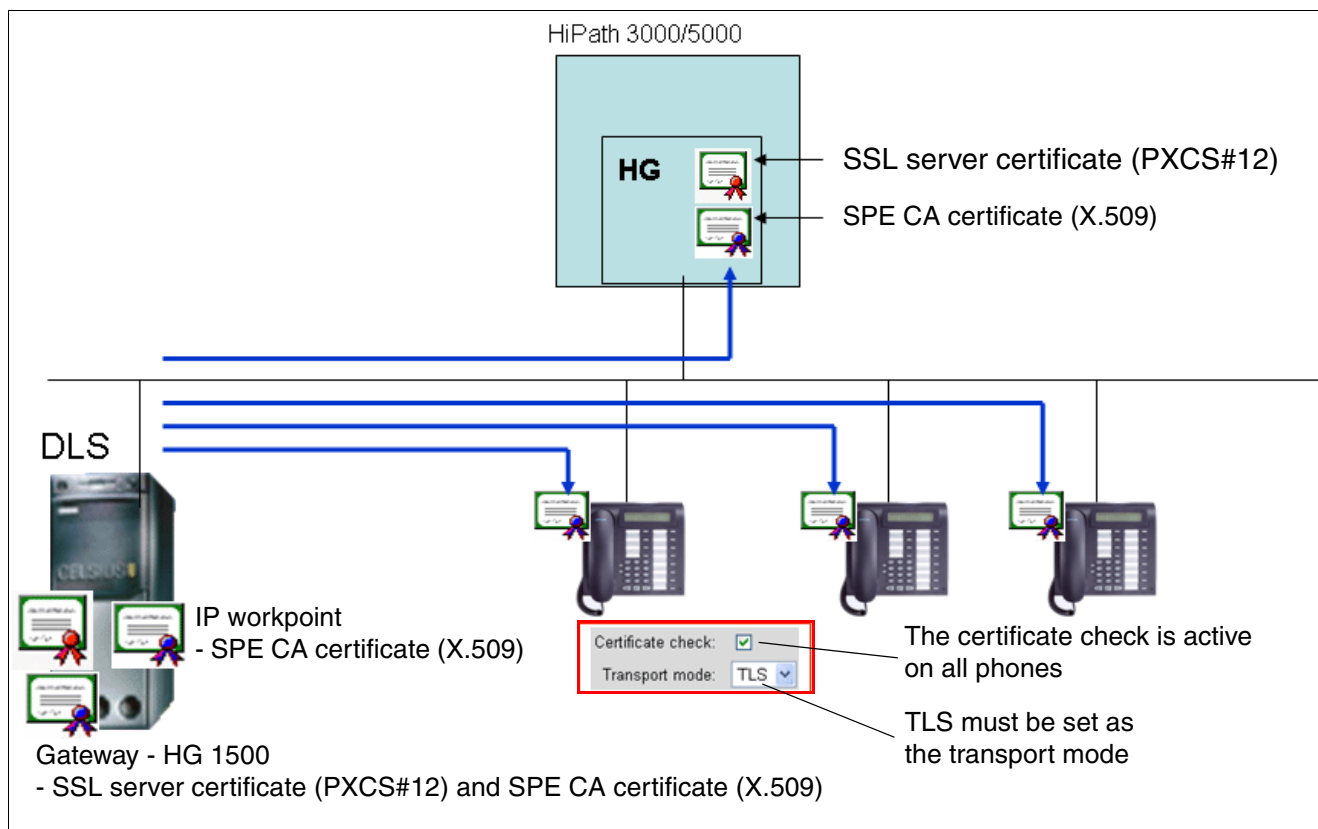
DLS - SPE Certificate Deployment

3.7 DLS - SPE Certificate Deployment

If you want greater security with a certificate check, you must integrate the DLS V2.0 R2 deployment service in the customer network. The SPE CA certificate needed for this must be imported into the DLS. The DLS then uses a secure connection to deploy the SPE CA certificate for encryption to all IP phones.

3.7.1 SPE with Certificate Check

You can use the DLS to load the certificates required for SPE to the gateways and IP phones. To do this, you must activate the certificate check and the TLS (Transport Layer Security) encryption protocol.



Activate the certificate check and set the TLS (Transport Layer Security) encryption protocol in the optiPoint410/420's WBM.

WBM path:

1. Select: WBM > Administration > Settings > System > Security settings.
The "Security settings" mask is displayed.
2. Activate the "Certificate check" flag.

3. Set the "Transport mode" parameter to "TLS".
4. Click "Submit".

3.7.2 Checking the HG 1500 Deployment and Licensing Client Configuration

Check the HG 1500 Deployment and Licensing Client configuration in the HG 1500's WBM.

WBM path:

Select: WBM > Explorers > Security > Deployment- and Licensing-Client (DLSC).



HG 1500 is only allowed to display the 0. DLSC client certificate and the 0. CA certificate.

Secure mode

"1. DLSC Client Certificates" and "1. CA Certificate" are only displayed in the HG 1500 if "Secure mode" has already been enabled in HG 1500 by means of HG 1500 – DLS communication and if the individual DLS certificates have been transferred.



"Secure mode" means that an HG 1500 only communicates with a DLS that has a valid DLSC client certificate.

Signaling & Payload Encryption (SPE) – Encryption

DLS - SPE Certificate Deployment

3.7.3 Displaying CA Certificates

You can display and check the 0. DLSC client certificate and the 0. CA certificate.

Example:

Displaying certificate information on the 0. CA certificate:

WBM path:

Select: WBM > Explorers > Security > Deployment- and Licensing-Client (DLSC) > DLSC CA-Certificates > 0. CA-Certificate.

The "Certificate Information" mask is displayed and can be checked.



The IP address of the DLS is not configured in the HG 1500 by default.

This mask displays general information about the certificate file, such as type (for example, self-signed CA certificate) and serial number, information about the start and end time of certificate validity, and encryption data.

3.7.4 Adding IP Gateways and IP Phones to the DLS

Before you can import and start to deploy SPE certificates or the automatic SPE configuration, you must add the IP gateways and IP phones to the DLS. To do this, you must start by adding the HG 1500 to the DLS as a virtual device.

3.7.5 Adding HG 1500 to the DLS as a Virtual Device

HG 1500 can be added to the DLS as a virtual device. The HG 1500 data can be read in automatically via the HG 1500 WBM - by entering the IP address of the DLS server in the "Edit DLS Client Basic Setup" mask - or manually via the DLS WBM.

3.7.5.1 Automatically Adding HG 1500 to the DLS

HG 1500 is automatically added as a virtual device via the HG 1500 WBM.

WBM path:

1. Select: WBM > Explorers > Security > Deployment- and Licensing-Client (DLSC).
The "Edit DLS Client Basic Setup" mask is displayed.
2. Enter the IP address of the DLS server in the "IP-Address of DLS Server:" mask.
3. Click "OK".
HG 1500 is automatically added to the DLS as a virtual device.
4. Click the diskette icon in the control area to save your changes permanently.

3.7.5.2 Manually Adding HG 1500 to the DLS

HG 1500 is manually added as a virtual device via the DLS WBM.

WBM path:

1. Select: WBM > Deployment Service > IP Devices > IP Device Administration > IP Device Configuration.
The "IP Device Configuration" mask is displayed.
2. Activate "Object" in the "Views:" field.
3. Select the "DLS Connection" tab.
4. Enter the IP address of the DLS server in the "DLS Server Address:" field.
5. Click "Scan".
HG 1500 is added to the DLS as a virtual device.

A DLSC certificate is transferred from the DLS to the HG 1500 and the HG 1500 is switched to secure mode. From this point on, only a DLS with a valid DLSC certificate can exchange data with the HG 1500.



If you attempt to communicate with the HG 1500 via another DLS, no data is exchanged because the other DLS is unable to authenticate itself.

Signaling & Payload Encryption (SPE) – Encryption

DLS - SPE Certificate Deployment

3.7.6 Displaying 1. CA and 1. DLSC Client Certificates

You can display and check the 1. CA and 1. DLSC client certificates.

- **1. CA certificate**

WBM path:

Select: WBM > Explorers > Security > Deployment- and Licensing-Client (DLSC) > DLSC CA-Certificates > 1. CA-Certificates.

- **1. DLSC client certificate**

WBM path:

Select: WBM > Explorers > Security > Deployment- and Licensing-Client (DLSC) > DLSC Client Certificate > 1. DLSC Client Certificates.

The "Certificate Information" mask is displayed for the relevant certificate and can be checked. This mask displays general information about the certificate file, such as type (for example, self-signed CA certificate) and serial number, information about the start and end time of certificate validity, and encryption data.

3.7.7 Correcting DLS - HG 1500 Errors

You can display the HG 1500 event log file in the event of problems between the DLS and HG 1500.

If you have to reinstall the DLS, you must export the DLS CA and DLSC client certificates before you perform the reinstallation (see Section 3.3.7, "Exporting the Root CA Certificate as "X.509"").

After you reinstall the DLS, you can reimport the DLS CA and DLSC client certificates needed in the customer network for HG 1500 communication (see Section 3.3.10, "Importing an Exported Root CA Certificate").



If the same IP address is reused for the reinstalled DLS, the HG 1500 automatically registers at the DLS.

If the DLS is unable to communicate with the HG 1500, for instance, after you reinstall the DLS, you can use the `reset dls bootstrapping` command in the HG 1500 CLI to delete the old "1." DLS certificates (such as "1. CA Certificate").

Commands via the HG 1500 CLI:

```
Please log in.
```

```
username: 31994
```

```
password: 31994
```

```
Welcome to the HG 1500 V7 SAPP HI-G15.74.000.S Command Line Interpreter.
```

```
vxTarget> get write access
```

```
OK
```

```
vxTarget> reset dls bootstrapping
```

```
OK
```

Signaling & Payload Encryption (SPE) – Encryption

DLS - SPE Certificate Deployment

3.7.8 Adding IP Phones to the DLS

IP phones are added to the DLS via the DLS WBM once you have added the IP gateways.

WBM path:

1. Select: WBM > Deployment Service > IP Devices > IP Device Interaction > Scan IP Devices

The "Scan IP Devices" mask is displayed.

2. Activate "Object" in the "Views:" field.
3. Select the "IP Ranges" tab.
4. Activate "Table" and enter the required data in the fields.
5. Select the "Configuration" tab.
6. Activate the "Send DSL Address" flag.
7. Enter the IP address of the DLS in the "DLS Address:" field.
8. Enter the DLS port number in the "DLS Port" field.
9. Click "Scan IP Devices".

The parameters set and the software version of the IP phones must be read out once the IP phones have been fully scanned.

3.7.9 Reading out Parameters and the Software Version of IP Phones

Read out the parameter and the software version of the IP phones via the DLS WBM.

WBM path:

1. Select: WBM > Deployment Service > IP Devices > IP Device Interaction > Read IP Devices Data.
2. The "Read IP Device Data" mask is displayed.
3. Activate "Table".
4. Select and mark all IP devices.
5. Click "Read".

The parameters and the software version of the IP phone are read out.

3.7.10 Updating IP Phones

Any necessary updates to IP phones must be performed via the DLS software.

WBM path:

1. Select: WBM > Deployment Service > Software Deployment > Workpoint Deployment.
The "Workpoint Deployment" mask is displayed.
2. Activate the table in the "Views:" field.
3. The "Select Deploy Workpoint-BLK Image" table is displayed.
4. Click the necessary software in the table.
5. Click "Deploy".



The current version is required as the NetBoot version for the IP phone. The NetBoot version (*.fli) can be upgraded via DLS.
The customer network must feature an FTP server.

3.7.11 Importing and Deploying SPE CA Certificates

The SPE certificates generated in the HG 1500 or in the customer's PKI infrastructure must be deployed to the IP gateways and IP phones. SPE certificates can only be deployed to the IP phones via the DLS.

3.7.11.1 Importing SPE CA Certificates for IP Gateways

Import the SPE CA certificates for IP gateways via the DLS WBM.

WBM path:

1. Select: WBM > Deployment Service > IP Devices > IP Gateway Configuration > Signaling and Payload Encryption (SPE).
The "Signaling and Payload Encryption (SPE)" mask is displayed.
2. Activate "Object" in the "Views:" field.
3. Select the "Settings" tab.
4. Enter 1024 as the public key length in the "Minimal Public Key Length for Certificates:" field.
The minimum public key length of the DLS must match the minimum public key length of the HG 1500 (1024 bits).

Signaling & Payload Encryption (SPE) – Encryption

DLS - SPE Certificate Deployment

5. Select the "SPE Certificate" tab.
6. Activate "SPE CA Certificates [0..15]" in the "Certificate Type" field.
7. Select the certificate in the "Filename:" field.
8. Click "Import Certificate".
9. Activate "SPE Certificate" in the "Certificate Type" field.
10. Select the HG 1500 server certificate in the "Filename:" field.
11. Enter the passphrase in the "Passphrase:" field.
The passphrase is a password made up of several words and containing up to 20 characters.
12. Click "Import Certificate".
13. Select the "SPE CA Certificates" tab.
14. Activate "Object".
15. Activate the certificates in the "Activate Certificate" table column.
16. Click "Save".



Make sure you read the notes or operating information on the DLS.

3.7.11.2 Importing SPE CA Certificates for IP Phones

Import the SPE CA certificates for the IP phones via the DLS WBM.

WBM path:

1. Select: WBM > Deployment Service > IP Devices > IP Phone Configuration > Signaling and Payload Encryption (SPE).

The "Signaling and Payload Encryption (SPE)" mask is displayed.

2. Activate "Object" in the "Views:" field.
3. Select the "SPE CA Certificates" tab.
4. Activate "Table".
5. Activate "SPE CA Certificates [0..1]" in the "Certificate Type" field.
6. Select the certificate in the "Filename:" field.
7. Click "Import Certificate for TLS Server (optiPoint)".



Select all required IP phones before you import the certificates, otherwise you must perform the import procedure for each individual IP phone.
Make sure you read the gray DLS note.

Signaling & Payload Encryption (SPE) – Encryption

DLS - SPE Certificate Deployment

3.7.12 Configuring optiClient 130

SPE is supported in optiClient 130 V5.1 and later. At present, optiClient 130 can only be configured for SPE via the DLS.

3.7.13 optiClient Attendant V8.0

optiClient Attendant V8.0 can only be connected via a terminal device as this is the only way to ensure that SPE does not impact the functionality of optiClient Attendant V8.0.

3.7.14 "Gateway not found!" Error Message

"Gateway not found!" appears on the display of the optiPoint 410/420 IP phone.

Causes:

- The optiPoint 410/420 cannot reach the HG 1500 via TCP/IP.
- "Security" TLS is activated on the optiPoint 410/420, but the IP ports for TLS are not configured in the HiPath 3000.
- "Security" TLS is activated on the optiPoint 410/420, but the SPE certificates are not available/imported into the HG 1500.
- TLS "unavailable" - SPE certificates are available in the HG 1500. The certificate check is activated in the IP phone, but a different SPE certificate is active in the HG 1500.

3.8 Automatic SPE Configuration via DLS

Automatic SPE configuration can be performed via DLS. To do this, all IP gateways must first be imported into the DLS. The DLS automatically recognizes and reads out all IP phones configured in the system. Automatic configuration can commence once all IP gateways and IP phones have been entered in DLS.

Proceed as follows to start automatic SPE configuration via DLS.

WBM path:

1. Select: WBM > Deployment Service > Administration > CDB Configuration > Automatic SPE Configuration.

The "Automatic SPE Configuration" mask is displayed.

2. Click "Create CA".
A new autoSPE credential is generated.
3. Click "Deploy CA".
The autoSPE credential is deployed to all IP gateways and IP phones.
4. Click "Activate".
The deployed credential is activated, that is, "generate and deploy" is active at every IP gateway for a CA-signed certificate. Following activation, only IP phones that accept the associated CA certificate can receive DLS requests.

Credential:

A credential is an instrument for confirming the identity of a system or user to another system. This credential is usually a user ID in conjunction with an authentication feature.

Credentials can be identity papers, certificates, passwords, keys or results of cryptographic methods or physical components for access authorization, such as smart cards or keys.

Signaling & Payload Encryption (SPE) – Encryption

SPE Secure Trace

3.9 SPE Secure Trace

SPE secure traces are used to detect defects in an SPE environment. SPE secure traces provide recordings of encrypted signaling and payload datastreams, for instance, from and to the gateway. Completed SPE secure trace recordings are sent to BackLevel Support. The recorded data can only be viewed by a developer with his or her private key.

3.9.1 SPE Secure Trace Certificate

This certificate is the prerequisite for activating or generating an SPE secure trace in the HG 1500 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 and must be imported into the HG 1500.

3.9.2 Importing the SPE Secure Trace Certificate

Import the SPE secure trace certificate into all HG 1500s now via the HG 1500 WBM.

WBM path:

1. Select: WBM > Explorers > Maintenance > Secure Trace > Import Secure Trace certificate (PEM or Binary).

The "Load the Secure Trace Certificate via HTTP" mask is displayed.

2. Enter the path and file name of the PEM or binary file you want to import in the "Certificate file (PEM or binary):" field.
3. Click "Browse" to open a window to search for the file.
4. 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. Appropriate measures should be taken.

5. Click "Import Certificate from File" if you are satisfied with the fingerprint check.

You can now create an SPE secure trace.

3.9.3 Displaying the SPE Secure Trace Certificate

You can display and check the SPE secure trace certificate via the HG 1500 WBM.

WBM path:

Select: WBM > Explorers > Maintenance > Secure Trace > Secure Trace Certificate.

The "Certificate Information" mask is displayed and can be checked. This mask displays general information about the certificate file, such as type (for example, CA-signed peer certificate) and serial number, information about the start and end time of certificate validity, and encryption data.

3.9.4 Starting the SPE Secure Trace

Prerequisites:

You can only start the SPE secure trace if the following prerequisites have been met:

- The "sniffer" (WireShark version 0.99.6, for instance) has been started.
- The HiPath plug-in for the "sniffer" has been connected and IP package recording is active.
- You received a public key from the developer and imported it into WBM.
- The secure trace activation passphrase has been entered in the WBM (passphrase: a password made up of a number of words and containing up to 20 characters).



Make sure you note the passphrase because an SPE secure trace is impossible without a passphrase. You cannot start a secure trace if you have forgotten your passphrase. You must bootstrap the HG 1500 before you can create a new passphrase.

Signaling & Payload Encryption (SPE) – Encryption

SPE Secure Trace

3.9.4.1 Editing the SPE Secure Trace Passphrase

You can change the secure trace passphrase via the HG 1500 WBM.

WBM path:

1. Select: WBM > Explorers > Maintenance > Secure Trace > Change Secure Trace Activation Passphrase.

The "Change Secure Trace Activation Passphrase" mask is displayed.

2. Fill out the input fields "Current Passphrase", "New Passphrase", and "Confirm New Passphrase".
3. Click "OK".
4. Click the diskette icon in the control area to permanently save changes.

3.9.4.2 Activating the SPE Secure Trace

If the SPE secure trace is started in the HG 1500, a secure trace beacon for TSL is sent for every terminal device (IP gateway and IP terminal). This enables you to decrypt the data later with the private key generated for Development.

Activate the SPE secure trace via the HG 1500 WBM.

WBM path:

1. Select: WBM > Explorers > Maintenance > Secure Trace > Start Secure Trace.

The "Start Secure Trace" mask is displayed.

2. Enter the passphrase in the "Secure Trace Activation Passphrase:" field.
The passphrase is a password made up of several words and containing up to 20 characters.
3. Enter the trace duration (in minutes) in the field "Duration of Secure Trace (Mins.):".
4. Activate all protocols.
5. Click "Start Secure Trace".

The secure trace is generated.

4 Networking Scenarios for HiPath 3000/5000 V8

This chapter describes scenarios with typical, practical configurations. The application scenarios are displayed and the configuration steps are described. In the practical examples, Manager E and WBM are used for configuration.

4.1 Overview

This document covers the topics listed in the table below.

Topic
Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP, page 4-2
Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2, page 4-10
Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-NQ Trunks, page 4-18
Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Breakout to the ITSP, page 4-25
Networking HiPath 3000 V9 with HiPath 3000 V9 via IP, page 4-27
Networking HiPath 3000 V9 with HiPath 3000 V9 via TDM, page 4-34
Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164, page 4-38
Networking HiPath 3000 V8 with HiPath 4000 V4 via IP, page 4-44
Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2, page 4-48
Networking HiPath 3000 V9 with HiPath 4000 V4 via TDM, page 4-57
Networking HiPath 3000 V8 and HiPath 4000 V4 with E.164, page 4-60
Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2, page 4-63
Networking HiPath 3000 V9 with External Systems via ISO-QSIG or ECMA-QSIG, page 4-122
Information on Configuring Networking Routes, page 4-125
Information on the Rerouting Parameter and Path Optimization Flag, page 4-127
Least Cost Routing (LCR) for E.164, page 4-128

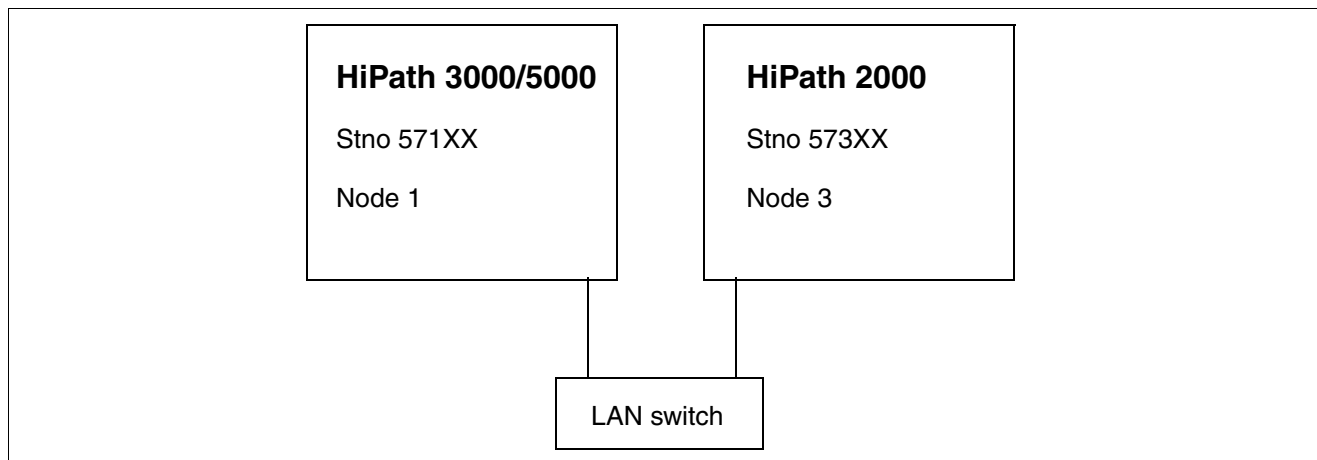
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP

4.2 Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP

4.2.1 Target Configuration

The target configuration involves establishing a CorNet-IP connection from HiPath 3000/5000 to HiPath 2000 V2 / HiPath OpenOffice EE.V9



4.2.2 Configuring HiPath 3000/5000

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > IP Trunks".
3. Select the gatekeeper board slot.
4. Enable gateway resources.
5. Add the required number of IP trunking lines.
6. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under "Routes", the last possible route should be selected (clicked).
3. Enter the route name (e.g., LAN).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" and "No. and type, outgoing" for the selected route (LAN).
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number, e.g., 1 (corresponds to the node number).
3. Click Apply.

Configure system parameters

1. Select "System parameters > Flags > Node number", enter the node number (for example, 57199), and check if "Path optimization" is set.
2. Click Apply.

Configure LCR

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area "LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 2000 / HiPath OpenOffice EE station numbers (e.g., -573XX).
3. Assign a route table to the station number (e.g., route table 1).
4. Select the IP trunking route (the last possible trunk group) for the route table.
5. Assign a dial rule to the IP trunking route (e.g., dial rule 1).
6. Select "Corporate network" as the network provider's method for dial rule 1 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Click Apply.

Licensing...

1. Select "Licensing... > HXG > HG 1500 B-channel".
2. License the number of IP trunking lines configured.
3. Click Apply.
4. Transfer the CDB to HiPath 3000 (delta mode possible).

4.2.3 Configuring the HG 1500 in HiPath 3000/5000

Setup is performed via WBM.

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 3).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HiPath 2000 / HiPath OpenOffice EE.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG.
11. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 2000 / HiPath OpenOffice EE (e.g. 573). with this input all numbers from 57300 to 57399 are routed to HiPath 2000 / HiPath OpenOffice EE.
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG with the reset icon to activate the trunking line.

4.2.4 Configuring HiPath 2000 / HiPath OpenOffice EE

Setup is performed via WBM.

Add trunks

1. Start WBM.
2. Select "Expert Mode" and confirm with "OK".
3. Select "Explorers > Trunks/Routing > Trunks > LAN: Slot 2 > Port 3 CorNet-IP".
4. Right-click "Add Trunk".
5. Enter the required number of IP trunking lines.
6. Click Apply.

Configure routes

1. Select "Lines/Networking > Route > Last Possible Route".
2. Right-click "Last Possible Route".
3. Enter the route name (e.g., LAN).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If seizure codes are set, delete them.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters > Trk Grp 8".
2. Right-click "Trk Grp 8 > Change Routing Parameters".
3. Select "PABX" under "Route type", "Direct inward dialing" under "Callnumber typ" and "Internal" under "No. and type, outgoing" for "Trk Grp 8" (currently only possible via Manager E).
4. Click Apply.

Configure QSIG features

1. Select "Explorers > Lines / networking... > QSIG features".
2. Right-click "QSIG-Feature" and select "QSIG-Feature change".
3. Select "Own system data > System number" and enter the system number (for example, 3; corresponds to the node number).
4. Click Apply.

Configuring system flags

1. Select "Explorers > Basic Settings > System > System Flags".
2. Right-click "System Flags" and select "Edit System Flags".
3. Enter the node number (currently only possible in Manager E) and check if path optimization is set.
4. Click Apply.

Configure LCR

1. Select "Explorers > Routing > LCR".
2. Right-click "Edit LCR flags".
3. Select "Activate LCR".
4. If necessary, activate "Digit-by-digit" under "Digit transmission".
5. Click Apply.
6. Configure the dial plan.
7. Select "Explorers > Routing > LCR > Dial Plan".
8. Right-click "Edit Dial Plan".
9. Enter the HiPath 3000 station numbers (e.g., -571XX) under "Dialed digits".
10. Assign a free route table to the station number (e.g., 12).
11. Click Apply.

Configuring the route table

1. Select "Explorers > Routing > LCR > Routing table".
2. Right-click the selected route table (e.g., 12) and click "Change Routing table".
3. Enter the "Trk Grp 8" for the IP trunking lines under Index 1 and select a free dial rule (e.g., outdial rule 4).
4. Click Apply.

Configuring the outdial rule

1. Select "Explorers > Routing > LCR > Dialrule".
2. Right-click the selected dial rule (e.g., dial rule 4) and click "Change Dialrule".
3. Assign a rule name, enter "E1A" as the dial rule format; select "Corporate network" as the network provider's method for the dial rule and "Unknown" as the type.
4. Click Apply.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via CorNet IP

Add node

1. Select "Explorers > Voice Gateway > PBX > Nodes".
2. Right-click "Add PBX Node".
3. Enter the node number (e.g., 1).
4. Click Apply.
5. Right-click the added node number and select "Edit IP Addresses".
6. HXG board 1: Enter the IP address of HG 1500 in HiPath 3000.
7. Click Apply.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing" (if the Routing folder does not appear, exit the window by clicking Maintenance, for example, and return to "Explorers > Voice Gateway > PBX > Routing". This refreshes Java; the page is now correctly displayed).
2. Right-click "Add Station Number".
3. Enter the station number(s) in the Station number field for the HiPath 3000 node number (e.g., 571). This entry routes all station numbers in the range 57100 - 57199 to HiPath 3000.
4. Click Apply.
5. Select "Explorers > Basic Settings > License Management > License File".
6. Select and load the associated license file.
7. Click the diskette icon.
8. Click the reset icon.

Note on node monitoring



The same node monitoring settings (TCP or ICMP) must be used for all nodes belonging to the network. In the case of HiPath 3000 and HiPath 2000 / HiPath OpenOffice EE networks, the use of TCP is preferable.

4.2.5 Using Signaling & Payload Encryption

Signaling & Payload Encryption is supported as of HiPath 3000/5000 R4 and HiPath 2000 V2 R4 / HiPath OpenOffice EE. It allows station-specific encryption of both signaling and payload data (see Chapter 3, "Signaling & Payload Encryption (SPE) – Encryption").

The system-wide flag for SPE support must be activated for all systems belonging to the network.

"Payload Security" must be activated to allow a station to use SPE. In addition, one of the following IP workpoints must be available:

- OpenStage CorNet IP (HFA)
 - 20 E, 20, 20 G
 - 40, 40 G
 - 60, 60 G
 - 80, 80 G
- optiPoint 410 (not optiPoint 410 entry, optiPoint 410 economy)
- optiPoint 420 (not optiPoint 420 economy)

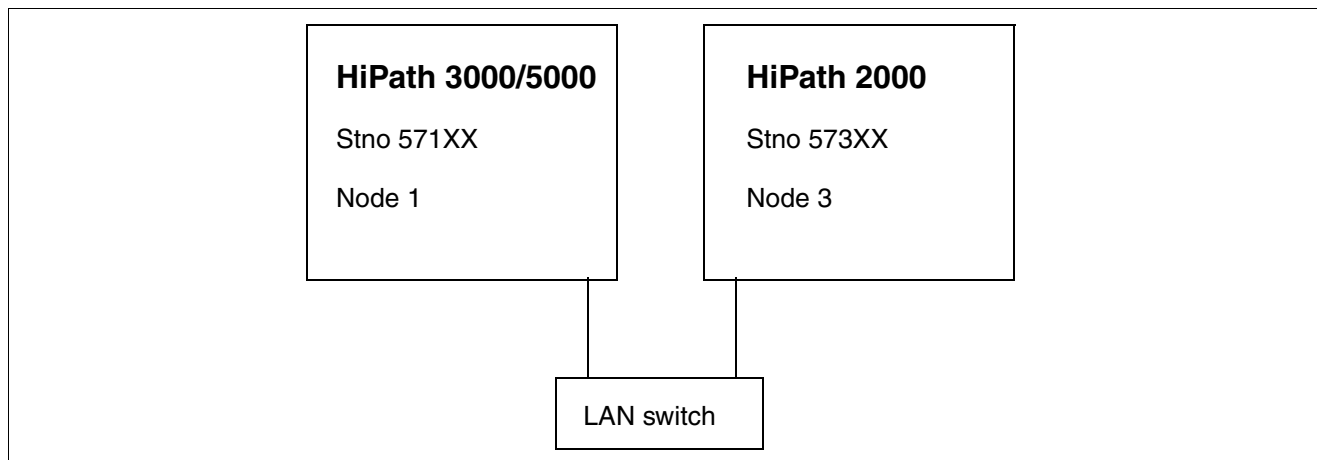
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2

4.3 Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2

4.3.1 Target Configuration

The target configuration involves establishing a SIP-Q connection from HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE.



4.3.2 Prerequisites

- HiPath 3000 as of V7 R4
- HiPath 2000 as of V2 R4 / HiPath OpenOffice EE

4.3.3 Configuring HiPath 3000/5000

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > IP Trunks".
3. Select the gatekeeper board slot.
4. Enable gateway resources.
5. Add the required number of IP trunking lines.
6. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under "Routes", the last possible route should be selected (clicked).
3. Enter the route name (e. g., SIP-Q).
4. Enter the 2nd trunk code (e. g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" and "No. and type, outgoing" for the selected route (SIP-Q).
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number, e. g., 1 (corresponds to the node number).
3. Click Apply.

Configure system parameters

1. Select "System parameters > Flags > Node number", enter the node number (for example, 57199), and check if "Path optimization" is set.
2. Click Apply.

Configure LCR

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area " LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 2000 / HiPath OpenOffice EE station numbers (e.g., -573XX).
3. Assign a route table to the station number (e.g., route table 1).
4. Select the SIP-Q route (the last possible trunk group) for the route table.
5. Assign a dial rule to the SIP-Q route (e.g., dial rule 1).
6. Select "Corporate network" as the network provider's method for dial rule 1 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Click Apply.

Licensing...

1. Select "Licensing... > HXG > HG 1500 B-channel".
2. License the number of SIP-Q lines configured.
3. Click Apply.
4. Transfer the CDB to HiPath 3000 (delta mode possible).

4.3.4 Configuring the HG 1500 in HiPath 3000/5000

Setup is performed via WBM.

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 3).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HiPath 2000 / HiPath OpenOffice EE.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG.
11. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 2000 / HiPath OpenOffice EE (e.g. 573). with this input all numbers from 57300 to 57399 are routed to HiPath 2000 / HiPath OpenOffice EE.
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG with the reset icon to activate the trunking line.

4.3.5 Configuration of HiPath 2000 / HiPath OpenOffice EE

Setup is performed via WBM.

Add trunks

1. Start WBM.
2. Select "Expert Mode" and confirm with "OK".
3. Select "Explorers > Trunks/Routing > Trunks > LAN: Slot 2 > Port 3 CorNet-IP".
4. Right-click "Add Trunk".
5. Enter the required number of SIP-Q lines.
6. Click Apply.

Configure routes

1. Select "Lines/Networking > Route > Last Possible Route".
2. Right-click "Last Possible Route".
3. Enter the route name (e.g., SIP-Q).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If seizure codes are set, delete them.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters > Trk Grp 8 (SIP-Q)".
2. Right-click "Trk Grp 8 (SIP-Q) > Change Routing Parameters".
3. Select "PABX" under "Route type", "Direct inward dialing" under "Callnumber typ" and "Internal" under "No. and type, outgoing" for "Trk Grp 8 (SIP-Q)" (currently only possible via Manager E).
4. Click Apply.

Configure QSIG features

1. Select "Explorers > Lines / networking... > QSIG features".
2. Right-click "QSIG-Feature" and select "QSIG-Feature change".
3. Select "Own system data > System number" and enter the system number (for example, 3; corresponds to the node number).
4. Click Apply.

Configuring system flags

1. Select "Explorers > Basic Settings > System > System Flags".
2. Right-click "System Flags" and select "Edit System Flags".
3. Enter the node number (currently only possible in Manager E) and check if path optimization is set.
4. Click Apply.

Configure LCR

1. Select "Explorers > Routing > LCR".
2. Right-click "Edit LCR flags".
3. Select "Activate LCR".
4. If necessary, activate "Digit-by-digit" under "Digit transmission".
5. Click Apply.
6. Configure the dial plan.
7. Select "Explorers > Routing > LCR > Dial Plan".
8. Right-click "Edit Dial Plan".
9. Enter the HiPath 3000 station numbers (e.g., -571XX) under "Dialed digits".
10. Assign a free route table to the station number (e.g., 12).
11. Click Apply.

Configuring the route table

1. Select "Explorers > Routing > LCR > Routing table".
2. Right-click the selected route table (e.g., 12) and click "Change Routing table".
3. Enter the "Trk Grp 8 (SIP-Q)" under Index 1 and select a free dial rule (e.g., dial rule 4).
4. Click Apply.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000/5000 V9 to HiPath 2000 V2 / HiPath OpenOffice EE via SIP-Q V2

Configuring the outdial rule

1. Select "Explorers > Routing > LCR > Dialrule".
2. Right-click the selected dial rule (e.g., dial rule 4) and click "Change Dialrule".
3. Assign a rule name, enter "E1A" as the dial rule format; select "Corporate network" as the network provider's method for the dial rule and "Unknown" as the type.
4. Click Apply.

Add node

1. Select "Explorers > Voice Gateway > PBX > Nodes".
2. Right-click "Add PBX Node".
3. Enter the node number (e.g., 1).
4. Click Apply.
5. Right-click the added node number and select "Edit IP Addresses".
6. Select "SIP-Q" as the LAN trunking protocol.
7. HXG board 1: Enter the IP address of HG 1500 in HiPath 3000.
8. Click Apply.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing" (if the Routing folder does not appear, exit the window by clicking Maintenance, for example, and return to "Explorers > Voice Gateway > PBX > Routing". This refreshes Java; the page is now correctly displayed).
2. Right-click "Add Station Number".
3. Enter the station number(s) in the Station number field for the HiPath 3000 node number (e.g., 571). This entry routes all station numbers in the range 57100 - 57199 to HiPath 3000.
4. Click Apply.
5. Select "Explorers > Basic Settings > License Management > License File".
6. Select and load the associated license file.
7. Click the diskette icon.
8. Click the reset icon.

Note on node monitoring



The same node monitoring settings (TCP or ICMP) must be used for all nodes belonging to the network. In the case of HiPath 3000 and HiPath 2000 / HiPath OpenOffice EE networks, the use of TCP is preferable.

4.3.6 Using Signaling & Payload Encryption

Signaling & Payload Encryption is supported in HiPath 3000/5000 R4 and later. It allows station-specific encryption of both signaling and payload data (see Chapter 3, "Signaling & Payload Encryption (SPE) – Encryption").

The system-wide flag for SPE support must be activated for all systems belonging to the network.

"Payload Security" must be activated to allow a station to use SPE. In addition, one of the following IP workpoints must be available:

- OpenStage CorNet IP (HFA)
 - 20 E, 20, 20 G
 - 40, 40 G
 - 60, 60 G
 - 80, 80 G
- optiPoint 410 (not optiPoint 410 entry, optiPoint 410 economy)
- optiPoint 420 (not optiPoint 420 economy)

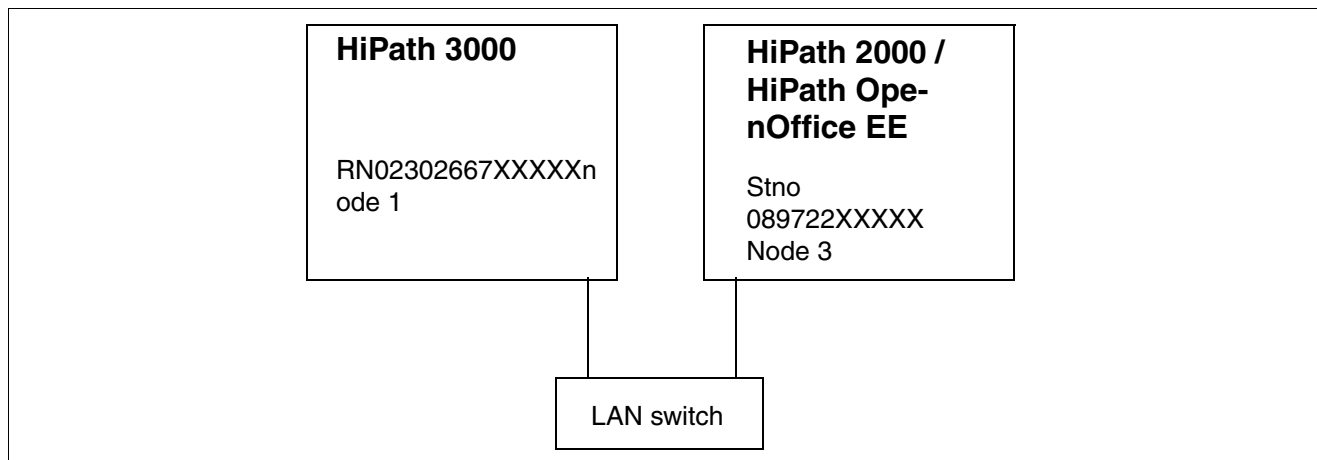
Networking Scenarios for HiPath 3000/5000 V8

Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-

4.4 Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-NQ Trunks

4.4.1 Target Configuration

The target configuration involves establishing a network between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with two CorNet-NQ trunks.



4.4.2 Configuring the HiPath 3000/5000, HiPath 2000 / HiPath OpenOffice EE and HG 1500

For information on configuring HiPath 3000/5000, HG 1500 and HiPath 2000 / HiPath OpenOffice EE, see [Section 4.2](#). Internet telephony is configured with various ITSPs and works (see [Section 2.8](#) and [Section 2.10](#) HiPath 2000 / HiPath OpenOffice EE Setup Wizard).

4.4.3 Configuring the HiPath 3000/5000, HiPath 2000 / HiPath OpenOffice EE and HG 1500 for E.164

The following examples describe the additional configuration of HiPath 3000/5000, HiPath 2000 / HiPath OpenOffice EE, and HG 1500 for E.164.

4.4.4 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "System parameters > Flags > E.164 numbering scheme".
3. Activate "System parameters > Display > outreach call number transparent" (if the chargeable feature is active on a remote CO connection and you want to use breakout there; displays and caller lists relevant).
4. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "Add direction prefix incoming", "Add direction prefix outgoing for the last possible route".
3. Select "Country code" under "No. and type, outgoing".
4. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under "Routes", the last possible route should be selected (clicked).
3. Enter the country code (e.g., 49) under "PABX number-incoming > Country code".
4. Enter the local area code (e.g., 2302) under "PABX number-incoming > Local area code".
5. Enter the PABX number (e.g., 667) under "PABX number-incoming > PABX number".
6. Activate the flag "Location number current" (if the system has a CO connection and the entries for the trunk group are the same as the last trunk group, the "Location number current" flag is set for the CO connection's trunk group).
7. Delete the routing prefix.
8. Enter a CO code > 2nd trunk code (e.g., 0).
9. Click Apply.

Networking Scenarios for HiPath 3000/5000 V8

Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 2000 / HiPath OpenOffice EE Node3 station number (e.g., 0C0-89-Z).
3. Assign a route table to the station number (e.g., route table 3).
4. Select the IP trunking route (the last possible trunk group) for the route table.
5. Assign a dial rule to the IP trunking route (e.g., dial rule 3).
6. Select "Corporate network" as the network provider's method for dial rule 3 in the Dial rule wizard.
7. Enter "D49E3A" as the dial rule format.
8. Select "Country code" under "Type of Number (TON)".
9. Enter the HiPath 2000 / HiPath OpenOffice EE Node3 station number (e.g., 0C00-49-89-Z).
10. Assign a route table to the station number (e.g., route table 4).
11. Select the IP trunking route (the last possible trunk group) for the route table.
12. Assign a dial rule to the IP trunking route (e.g., dial rule 4).
13. Select "Corporate network" as the network provider's method for dial rule 4 in the Dial rule wizard.
14. Enter "E3A" as the dial rule format.
15. Select "Country code" under "Type of Number (TON)" (if Node1 is in the same location as Node3, another LCR entry is needed, for example, 0C722-Z with D4989E2A and "Country code" as the TON).
16. Click Apply.
17. Transfer the CDB to HiPath 3000 (delta mode possible).

4.4.5 Configuring the HG 1500 in HiPath 3000 Node1

Setup is performed via WBM.

Add node

1. Start WBM
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 3).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HG 1500 in HiPath 2000 / HiPath OpenOffice EE Node3.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG 1500.
11. If necessary, configure a static route for Node3.
12. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 2000 / HiPath OpenOffice EE Node3 (e.g., 49 or 4989).
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG 1500 with the reset icon to activate the trunking line.

4.4.6 Configuring HiPath 2000 / HiPath OpenOffice EE Node3

Setup is performed via WBM.

Configure routes

1. Start WBM.
1. Select "Explorers > Lines/Networking > Route > Last Possible Route".
2. Right-click "Last Possible Route".
3. Delete the seizure code.
4. Enter the CO code (2nd trunk code, e.g., 0).
5. Enter the country code (e.g., 49) under "PABX number-incoming > Country code".
6. Enter the local area code (e.g., 89) under "PABX number-incoming > Local area code".
7. Enter the PABX number (e.g., 722) under "PABX number-incoming > PABX number".
8. Activate the flag "Location number current" (if the system has a CO connection and the entries for the trunk group are the same as the last trunk group, the "Location number current" flag is set for the CO connection's trunk group).
9. Click Apply.

Configure routing parameters

1. Select "Explorers > Trunks/Routing > Routing Parameter".
2. Right-click "Trk Grp 8" and select "Change Routing Parameters".
3. Select "Add direction prefix incoming", "Add direction prefix outgoing for the last possible route".
4. Select "Country code" under "No. and type, outgoing".
5. Click Apply.

Configure LCR

1. Select "Explorers > Routing > LCR".
2. Right-click "Edit Dial Plan".
3. Enter the HiPath 3000 Node1 station numbers (e.g., 0C0-2302-Z) under "Dialed digits".
4. Assign a free route table to the station number (e.g., 13).

5. Enter the HiPath 3000 Node1 station numbers (e.g., 0C00-49-2302-Z) under "Dialed digits".
6. Assign a free route table to the station number (e.g., 14).
7. Click Apply.

Configuring the route table

1. Select "Explorers > Routing > LCR > Routing table".
2. Right-click the selected route table (e.g., 13) and click "Change Routing table".
3. Enter the "Trk Grp 8" for the IP trunking lines under Index 1 and select a free outdial rule (e.g., outdial rule 5).
4. Click Apply.
5. Right-click the selected route table (e.g., 14) and click "Change Routing table".
6. Enter the "Trk Grp 8" for the IP trunking lines under Index 1 and select a free outdial rule (e.g., outdial rule 6).
7. Click Apply.

Configuring the outdial rule

1. Select "Explorers > Routing > LCR > Dialrule".
2. Right-click the selected dial rule (e.g., dial rule 5) and click "Change Dialrule".
3. Assign a rule name, enter "D49E3A" as the dial rule format; select "Corporate network" as the network provider's method for the dial rule and "Country code" as the type.
4. Click Apply.
5. Right-click the selected dial rule (e.g., dial rule 6) and click "Change Dialrule".
6. Assign a rule name, enter "E3A" as the dial rule format; select "Corporate network" as the network provider's method for the dial rule and "Country code" as the type.
7. Click Apply.

Add node

1. Select "Explorers > Voice Gateway > PBX > Nodes".
2. Right-click "Add PBX Node".
3. Enter the node number (e.g., 1).
4. Click Apply.

Networking Scenarios for HiPath 3000/5000 V8

Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Two CorNet-

5. Right-click the added node number and select "Edit IP Addresses".
6. HXG board 1: Enter the IP address of HG 1500 in HiPath 3000.
7. Click Apply.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing" (if the Routing folder does not appear, exit the window by clicking Maintenance, for example, and return to "Explorers > Voice Gateway > PBX > Routing". This refreshes Java; the page is now correctly displayed).
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 3000 (e.g., 49 or 492302).
4. Click Apply.
5. Select "Explorers > Basic Settings > System".
6. Right-click "Edit System Flags".
7. Activate "E.164 numbering scheme".
8. Click Apply.
9. Right-click "Display and edit display".
10. Activate "outreach call number transparent" (if the chargeable feature is active on a remote CO connection and you want to use breakout there; displays and caller lists relevant).
11. Click Apply.

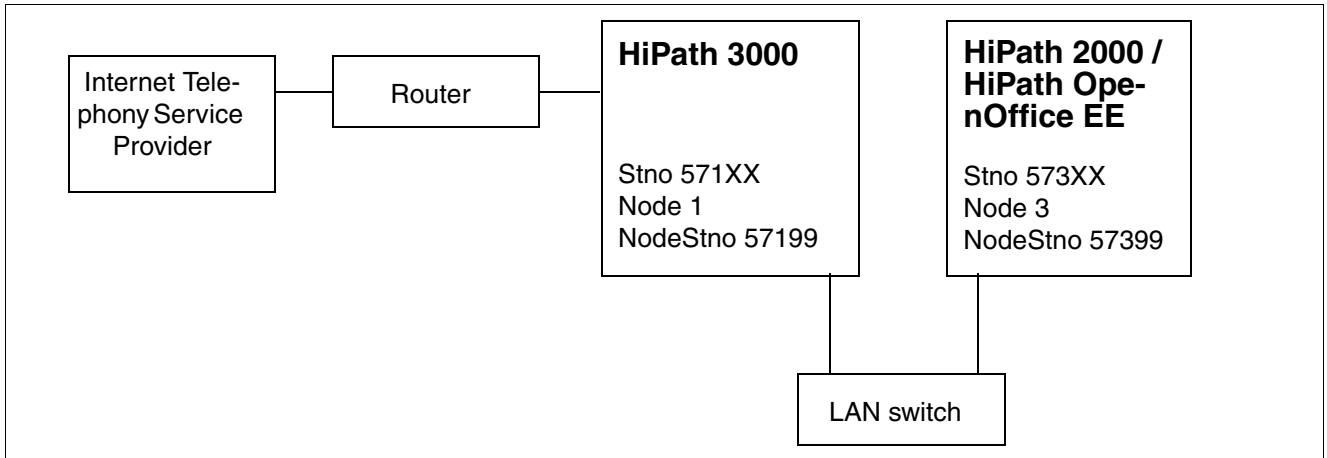
Licensing...

1. Select "Explorers > Basic Settings > License Management > License File".
2. Select and load the associated license file.
3. Click the diskette icon.
4. Click the reset icon.

4.5 Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Breakout to the ITSP

4.5.1 Target Configuration

The target configuration involves establishing a network between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with breakout to the ITSP.



Prerequisites

- ITSP (Internet Telephony Service Provider) is configured at HiPath 3000 Node1 and is ready for operation.
- The route to the Internet Telephony Service Provider provider is seized with code 85.
- Networking is configured between HiPath 3000 and HiPath 2000 / HiPath OpenOffice EE as described in [Section 4.2](#) and [Section 4.4](#).

4.5.2 Configuration for "Breakout" from HiPath 2000 / HiPath OpenOffice EE via HiPath 3000 to ITSP

The following example describes the additional configuration needed for breakout from HiPath 2000 / HiPath OpenOffice EE via HiPath 3000 to the ITSP.

Networking Scenarios for HiPath 3000/5000 V8

Networking Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000 with Breakout to

4.5.3 Configuring the HiPath 2000 / HiPath OpenOffice EE Node3

Setup is performed via WBM.

Configure LCR

1. Start WBM.
2. Select "Expert Mode" and confirm with "OK".
3. Select "Explorers > Routing > LCR".
4. Right-click "Edit Dial Plan".
5. Enter the station numbers for dialing the ITSP of HiPath 3000 Node1 under "Dialed digits" (e.g., 85CZ).
6. Assign a free route table to the station number (e.g., 15).
7. Click Apply.

Configuring the route table

1. Select "Explorers > Routing > LCR > Routing table".
2. Right-click the selected route table (e.g., 15) and click "Change Routing table".
3. Enter the "Trk Grp 8" for the IP trunking lines under Index 1 and select a free outdial rule (e.g., outdial rule 7).
4. Click Apply.

Configuring the outdial rule

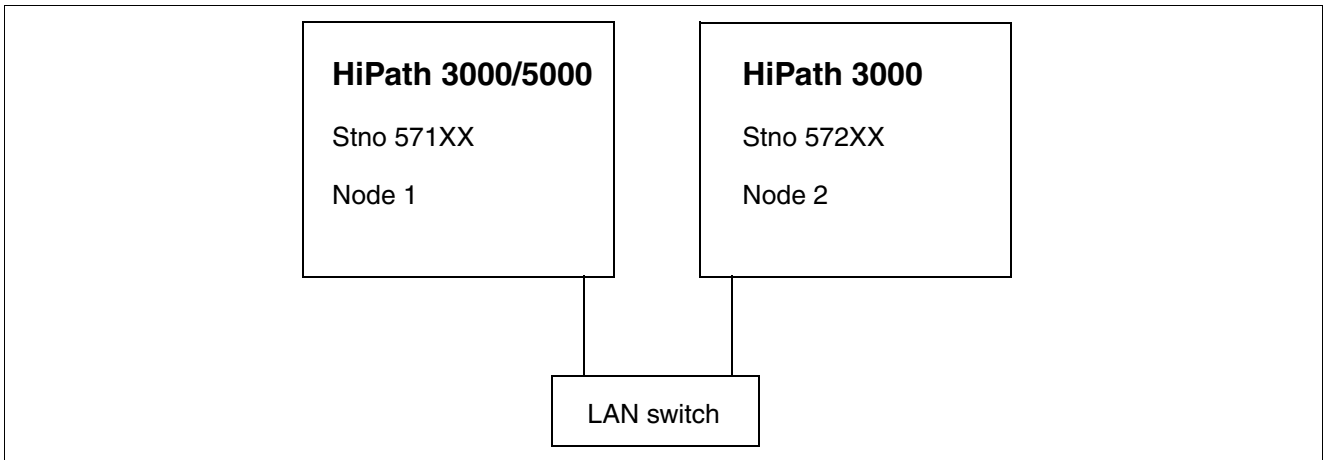
1. Select "Explorers > Routing > LCR > Dialrule".
2. Right-click the selected outdial rule (e.g., outdial rule 7) and click "Change Dialrule".
3. Assign a rule name, enter "D57199E1A" as the dial rule format; select "Corporate network" as the network provider's method for the dial rule and "Unknown" as the type.
4. Click Apply.
5. Click the diskette icon.

No further configuration is needed for HiPath 3000 Node1 and HG 1500.

4.6 Networking HiPath 3000 V9 with HiPath 3000 V9 via IP

4.6.1 Target Configuration

The target configuration involves establishing an IP trunking connection in a HiPath 3000 V9 with a HiPath 3000 V9.



4.6.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Adding IP trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > IP Trunks".
3. Select the gatekeeper board slot.
4. Enable gateway resources.
5. Add the number of trunking lines.
6. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the last possible Trk Grp.
3. Enter the route name (e.g., LAN).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 via IP

5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" under "Route type" and "Internal" under "No. and type, outgoing" for the selected Trk Grp (LAN).
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number, e.g., 1 (corresponds to the node number).
3. Click Apply.

Configure system parameters

1. Select "System parameters > Flags > Node number", enter the node number (for example, 57199), and check if "Path optimization" is set.
2. Click Apply.

Configure LCR

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area "LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node2 station numbers (e.g., -572XX).
3. Assign a route table to the station number (e.g., route table 2).
4. Select the IP trunking route (the last possible trunk group) for the route table.

5. Assign a dial rule to the IP trunking route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Click Apply.

Licensing...

1. Select "Licensing... > HXG > HG 1500 B-channel".
2. License the number of IP trunking lines configured.
3. Click Apply.
4. Transfer the CDB to HiPath 3000 (delta mode possible).

4.6.3 Configuring the HG 1500 in HiPath 3000 Node1

Setup is performed via WBM.

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 2).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HG 1500 in HiPath 3000 Node2.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG.
11. Once HG 1500 is ready for operation, quit and restart WBM.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 via IP

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the HiPath 3000 Node2 number (e.g., 572). This entry routes all station numbers in the range 57200 - 57299 to HiPath 3000 Node2.
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG 1500 with the reset icon to activate the trunking line.

4.6.4 Configuring HiPath 3000 Node2

4.6.4.1 Setup is performed via Manager E.

Adding IP trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > IP Trunks".
3. Select the gatekeeper board slot.
4. Enable gateway resources.
5. Add the number of trunking lines.
6. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the last possible Trk Grp.
3. Enter the route name (e.g., LAN).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" under "Route type" and "Internal" under "No. and type, outgoing" for the selected Trk Grp (LAN).
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number, e.g., 2 (corresponds to the node number).
3. Click Apply.

Configure system parameters

1. Select "System parameters > Flags > Node number", enter the node number (for example, 57299), and check if "Path optimization" is set.
2. Click Apply.

Configure LCR

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area "LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node1 station numbers (e.g., -571XX).
3. Assign a route table to the station number (e.g., route table 2).
4. Select the IP trunking route (the last possible trunk group) for the route table.
5. Assign a dial rule to the IP trunking route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 via IP

7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Click Apply.

Licensing...

1. Select "Licensing... > HXG > HG 1500 B-channel".
2. License the number of IP trunking lines configured.
3. Click Apply.
4. Transfer the CDB to HiPath 3000 (delta mode possible).

4.6.4.2 Configuration via WBM

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 1).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HG 1500 in HiPath 3000 Node1.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG.
11. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the HiPath 3000 Node1 number (e.g., 571). This entry routes all station numbers in the range 57100 - 57199 to HiPath 3000 Node1.
4. Click Apply.

5. Click the diskette icon.
6. You may have to reset the HG with the reset icon to activate the trunking line.



Alive monitoring over TCP or ICMP must be identical on both nodes and TCP must have precedence in HiPath 3000 and HiPath 3000 networks.

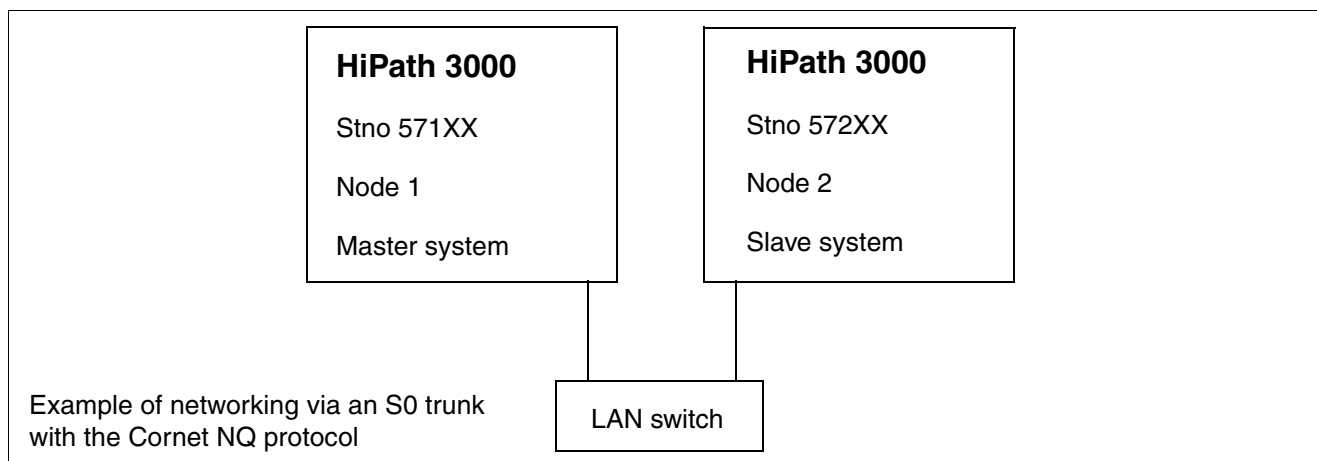
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 via TDM

4.7 Networking HiPath 3000 V9 with HiPath 3000 V9 via TDM

4.7.1 Target Configuration

The target configuration involves establishing a network in a HiPath 3000 V9 with a HiPath 3000 V9 via TDM.



4.7.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > Trunks".
3. Double-click the parameter field once in the row containing the required STLS or STMD trunk.
4. Select the protocol in the pop-up window under "ISDN flags > Protocol: Description" (S0: Cornet-NQ Master Direct CR=2 CHI=S2 (standard)); the protocol applies at all times to the port; in other words, there are always two trunks assigned to an S0 port.
5. Click Apply.
6. Click Close.
7. Select a free route in the row containing the required STLS or STMD trunk (e.g., Trk Grp 2).
8. Assign the same route (e.g., Trk Grp 2) to the second trunk associated with the S0 port.
9. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the selected route (e.g., Trk Grp 2).
3. Enter the route name (e.g., Tie).
4. Enter the 2nd trunk code (e.g., 0); for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" under "Route type" for the trunk group selected.
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number (e.g., 1).
3. Click Apply.

Configure LCR

1. Select "Least cost routing > Codes and flags".
2. Select "Activate LCR".
3. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node2 station numbers (e.g., -572XX).
3. Assign a route table to the station number (e.g., route table 2).
4. Select the chosen route (e.g., Trk Grp 2 or Tie) for the route table.
5. Assign a dial rule to the route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 via TDM

7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Enter "E1A" as the dial rule format.
10. Click Apply.
11. Transfer the CDB to HiPath 3000 (delta mode possible).

4.7.3 Configuring HiPath 3000 Node2

Setup is performed via Manager E.

Adding IP trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > Trunks".
3. Double-click the parameter field once in the row containing the required STLS or STMD trunk.
4. Select the protocol in the pop-up window under "ISDN flags > Protocol: Description" (S0: CorNet-NQ Slave CR=2 CHI=S2 (standard)); the protocol applies at all times to the port; in other words, there are always two trunks assigned to an S0 port.
5. Click Apply.
6. Click Close.
7. Select a free route in the row containing the required STLS or STMD trunk (e.g., Trk Grp 2).
8. Assign the same route (e.g., Trk Grp 2) to the second trunk associated with the S0 port.
9. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the selected route (e.g., Trk Grp 2).
3. Enter the route name (e.g., Tie).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

Select "Lines/networking > Routing parameters".

1. Select "PABX" under "Route type" for the trunk group selected.
2. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number (e.g., 2).
3. Click Apply.

Configure LCR

1. Select "Least cost routing > Codes and flags".
2. Select "Activate LCR".
3. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node2 station numbers (e.g., -571XX).
3. Assign a route table to the station number (e.g., route table 2).
4. Select the chosen route (e.g., Trk Grp 2 or Tie) for the route table.
5. Assign a dial rule to the route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Select "Unknown" as the type of number (TON).
9. Enter "E1A" as the dial rule format.
10. Click Apply.
11. Transfer the CDB to HiPath 3000 (delta mode possible).

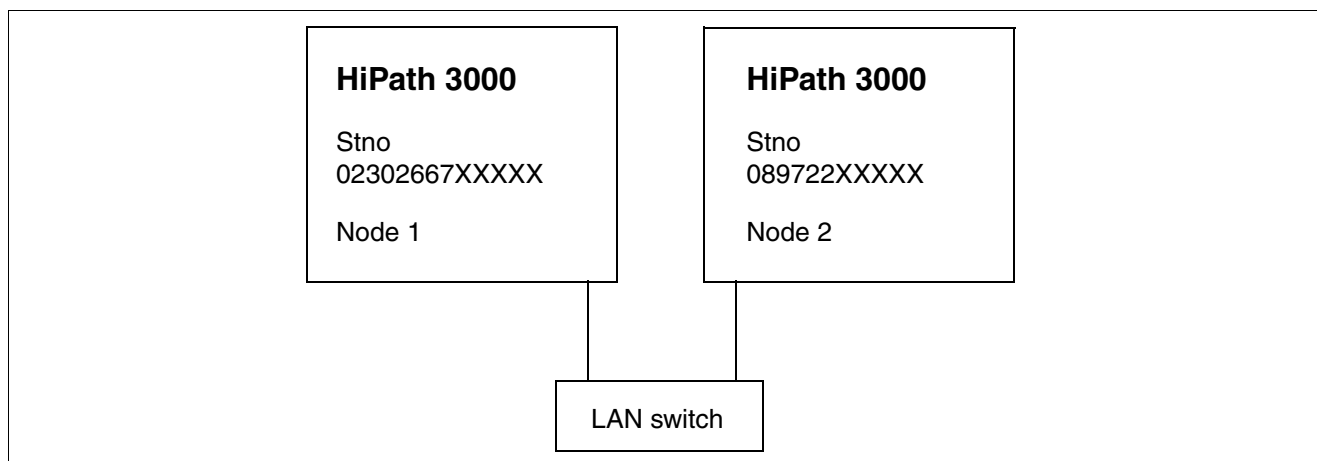
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164

4.8 Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164

4.8.1 Target Configuration

The target configuration involves establishing a network in a HiPath 3000V9 to a HiPath 3000V9 with E.164.



Prerequisites

Networking is configured between HiPath 3000 and HiPath 3000 as described in [Section 4.6](#) and [Section 4.7](#).

Note: If HiPath 3000 is connected to a point to multipoint, destination phone number detection no longer works when using E.164. Therefore, HiPath 3000 must be connected to a point to point and the "PABX number" input field in Manager E completed –as described below.

4.8.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "System parameters > Flags > E.164 numbering scheme".
3. Activate "System parameters > Display > outreach call number transparent" (if the chargeable feature is active on a remote CO connection and you want to use breakout there; displays and caller lists relevant).
4. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "Country code" under "No. and type, outgoing".
3. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under "Routes", the last possible route should be selected (clicked).
3. Enter the country code (e.g., 49) under "PABX number-incoming > Country code".
4. Enter the local area code (e.g., 2302) under "PABX number-incoming > Local area code".
5. Enter the PABX number (e.g., 667) under "PABX number-incoming > PABX number".
6. Activate the flag "Location number current".
7. Delete the routing prefix.
8. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node2 station number (e.g., 0C0-89722-Z).
3. Assign a route table to the station number (e.g., route table 3).
4. Select the IP trunking route (the last possible trunk group) for the route table.
5. Assign a dial rule to the IP trunking route (e.g., dial rule 3).
6. Select "Corporate network" as the network provider's method for dial rule 3 in the Dial rule wizard.
7. Enter "D49E3A" as the dial rule format.
8. Select "Country code" under "Type of Number (TON)".
9. Enter the HiPath 3000 Node2 station number (e.g., 0C00-49-89722-Z).
10. Assign a route table to the station number (e.g., route table 4).
11. Select the IP trunking route (the last possible trunk group) for the route table.
12. Assign a dial rule to the IP trunking route (e.g., dial rule 4).

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164

13. Select "Corporate network" as the network provider's method for dial rule 4 in the Dial rule wizard.
14. Enter "E3A" as the dial rule format.
15. Select "Country code" under "Type of Number (TON)" (if Node1 is in the same location as Node2, another LCR entry is needed, for example, 0C722-Z with D4989E2A and "Country code" as the TON).
16. Click Apply.
17. Transfer the CDB to HiPath 3000 (delta mode possible).

4.8.3 Configuring the HG 1500 in HiPath 3000 Node1

Setup is performed via WBM.

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 2).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HG 1500 in HiPath 3000 Node2.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG 1500.
11. If necessary, configure a static route for Node2 or enter the default router.
12. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 3000 Node2 (e.g., 4989722).
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG 1500 with the reset icon to activate the trunking line.

4.8.4 Configuring HiPath 3000 Node2

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "System parameters > Flags > E.164 numbering scheme".
3. Activate "System parameters > Display > outreach call number transparent" (if the chargeable feature is active on a remote CO connection and you want to use breakout there; displays and caller lists relevant).
4. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "Country code" under "No. and type, outgoing".
3. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under "Routes", the last possible route should be selected (clicked).
3. Enter the country code (e.g., 49) under "PABX number-incoming > Country code".
4. Enter the local area code (e.g., 89) under "PABX number-incoming > Local area code".
5. Enter the PABX number (e.g., 722) under "PABX number-incoming > PABX number".
6. Activate the flag "Location number current".

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 3000 V9 using E.164

7. Delete the routing prefix.
8. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 3000 Node1 station number (e.g., 0C0-2302667-Z).
3. Assign a route table to the station number (e.g., route table 3).
4. Select the IP trunking route (the last possible trunk group) for the route table.
5. Assign a dial rule to the IP trunking route (e.g., dial rule 3).
6. Select "Corporate network" as the network provider's method for dial rule 3 in the Dial rule wizard.
7. Enter "D49E3A" as the dial rule format.
8. Select "Country code" under "Type of Number (TON)".
9. Enter the HiPath 3000 Node1 station number (e.g., 0C00-49-2302667-Z).
10. Assign a route table to the station number (e.g., route table 4).
11. Select the IP trunking route (the last possible trunk group) for the route table.
12. Assign a dial rule to the IP trunking route (e.g., dial rule 4).
13. Select "Corporate network" as the network provider's method for dial rule 4 in the Dial rule wizard.
14. Enter "E3A" as the dial rule format.
15. Select "Country code" under "Type of Number (TON)" (if Node2 is in the same location as Node1, another LCR entry is needed, for example, 0C667-Z with D492302E2A and "Country code" as the TON).
16. Click Apply.
17. Transfer the CDB to HiPath 3000 (delta mode possible).

4.8.5 Configuring the HG 1500 in HiPath 3000 Node2

Setup is performed via WBM.

Add node

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "Add PBX Node".
4. Enter the node number (e.g., 2).
5. Click Apply.
6. Right-click the added node number and select "Edit IP Addresses".
7. HXG gatekeeper board 1: Enter the IP address of HG 1500 in HiPath 3000 Node2.
8. Click Apply.
9. Click the diskette icon.
10. Use the reset icon to reset the HG 1500.
11. If necessary, configure a static route for Node1.
12. Once HG 1500 is ready for operation, quit and restart WBM.

Configuring routing

1. Select "Explorers – Voice Gateway – PBX – Routing".
2. Right-click "Add Station Number".
3. Enter the station number(s) for the node number of HiPath 3000 Node2 (e.g., 492302667).
4. Click Apply.
5. Click the diskette icon.
6. You may have to reset the HG 1500 with the reset icon to activate the trunking line.



SIP phones always have to register at an E.164 network with their E.164 station number.
The default setting "System check" is maintained in the sections "Called Party Number" and "All others" under "Lines/networking > Routes > Special".

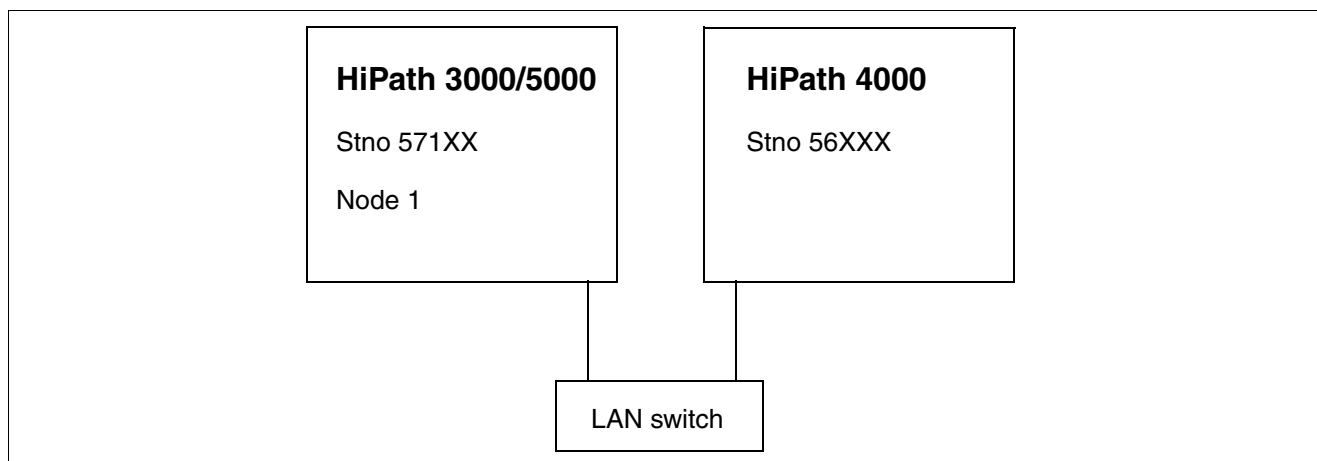
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V4 via IP

4.9 Networking HiPath 3000 V8 with HiPath 4000 V4 via IP

4.9.1 Target Configuration

The target configuration involves establishing an IP trunking connection to a HiPath 3000 V8 in a HiPath 4000 V4.



4.9.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Adding IP trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > IP Trunks".
3. Select the gatekeeper board slot.
4. Enable gateway resources.
5. Add the number of Ext. H323 trunks needed.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Click "Trk Grp11".
3. Select "Internal" under "No. and type, outgoing".
4. Select "PABX" under "Route type".
5. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Click "Trk Grp11".
3. Enter the route name (e.g., HiPath 4000).
4. Enter the country code (e.g., 49) under "PABX number-incoming > Country code".
5. Enter the local area code (e.g., 2302) under "PABX number-incoming > Local area code".
6. Enter the PABX number (e.g., 9878) under "PABX number-incoming > PABX number".
7. If necessary, activate the flag "Location number current".
8. Delete the routing prefix.
9. Enter a CO code > 2nd trunk code (e.g., 0).
10. Click Apply.

Configure special networking

1. Select "Lines/networking > Special".
2. Click "Trk Grp11".
3. Activate the "Always Use DSP" switch.
4. Click Apply.

Enter the IP address of HiPath 4000

1. Select "Network > Ext. H323".
2. Activate a connection with the external H.323 target.
3. Select the HP 4000 environment.
4. Enter the IP address of STMI in HiPath 4000.
5. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 4000 station numbers (e.g., -56XXX).
3. Assign a route table to the station number (e.g., route table 5).
4. Select route 11 in the Ext. H323 route for the route table.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V4 via IP

5. Assign a dial rule to route 11 (e.g., dial rule 5).
6. Select "Corporate network" as the network provider's method for dial rule 5 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Click Apply.
9. If necessary, clarify DMC settings with HiPath 4000 under "System parameters/Flags/Direct Media Connection" or "Early DMC" or "No DMC".
10. Transfer the CDB to HiPath 3000 (delta mode possible).

4.9.3 Configuring the HG 1500 in HiPath 3000 Node1

Setup is performed via WBM.

Configuring IP networking data

1. Start WBM
2. Select "Explorers – Voice Gateway – PBX".
3. Right-click "IP Networking Data" and select "Edit".
4. Select Alive Monitoring via Ping (ICMP).
5. Click Apply.

Add node

1. Select "Explorers > Voice Gateway > PBX > Nodes".
2. Right-click "Add PBX Node".
3. Enter the node number (e.g., 4).
4. Click Apply.
5. Right-click the added node number and select "Edit IP Addresses".
6. HXG gatekeeper board 1: Enter the IP address of STMI in HiPath 4000.
7. Click Apply.
8. Click the diskette icon.
9. Use the reset icon to reset the HG.

Note

A number entry for the path to HiPath 4000 is not needed under "Explorers\Voice Gateway\PBX\Routing".

If you want to use a non-standard setting (for the audio codes, for instance) with the Ext. H323 connection to HiPath 4000, you must configure a node that references the IP address of the HiPath 4000 under Voice Gateway in the HG 1500. A routing entry is not necessary here.

The required settings can then be made via this node. Alive monitoring from the HiPath 3000 to the HiPath 4000 is generally only possible with a "ping"; this is also set with the node entry.

When using the DB Feature Server in the scenario described above, this node must be entered as an "external HiPath 5000RSM/Allserve domain". The node entry is then automatically created on all HGs. A number entry in the Call No. field is not needed for this.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2

4.10 Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2

Overview

This section describes how to configure a SIP-Q network between HiPath 3000 V8 and HiPath 4000 V5. This requires specific settings to be made at the HiPath 3000 V8 using Manager E and in the WBM of the HG 1500.

Prerequisites

- HiPath 3000 as of V8
- HiPath 4000 as of V5

4.10.1 HiPath 3000 V8 Configuration

4.10.1.1 Settings in Manager E on HiPath 3000

Start Manager E.

Network... -> Ext. SIP

1. In the system view, select **Network... -> Ext. SIP**. The window "Ext. SIP" is displayed.
2. Select the check box "Operate with external SIP-Registrar". Selection fields, entry fields and selection options in the "Gateway" and "Security" window areas are enabled.
3. In the window "Ext. SIP", make the following settings:
 - Environment: **HiPath 4000**
 - Trunking mode: **SIP-Q**
 - Call Number: Enter the alias number of the HiPath 4000 endpoint.
 - Registration expiry: The value may not be less than 300 seconds.
 - IP address: Enter the IP address of the SIP Signaling Manager (SIPSM) for HiPath 4000.
 - Port: **5060**
 - Perform registration: select the check box.
 - Security: is optional.
4. Click **Apply**. Your changes are saved.

Lines/networking -> IP Trunks

1. In the system view, select **Lines/networking -> IP Trunks**. The window "IP Trunks" is displayed.
2. Enter the required number of "Ext. SIP" lines. To do so, make the following settings:
 - Gatekeeper HG1500: **Slot 5**
 - Access gateway resources: select the check box.
 - Number: **10** and **Ext. SIP**.Click **Add**. In the "Trunks" table, the following, for example, is then shown in a line: **Trk 21, Code: 7821, Type: Ext. SIP, Route: Trk Grp10**.
3. Click **Apply**. Your changes are saved.

Lines/networking -> Routes

1. In the system view, select **Lines/networking -> Routes**. The window "Routes" is displayed.
2. Select the route "Trk Grp 10". The settings for this route are displayed.
3. For "Trk Grp 10", make the following settings:
 - Route Name/Name: **H4KSIP**
 - CO code/2nd trunk code: **0**
 - PABX number-incoming: Enter the location number in the E.164 format for the country code, local area code and system number.
 - Overflow route: **None**
4. Click **Apply**. Your changes are saved.

Lines/networking -> Routing parameters

1. In the system view, select **Lines/networking -> Routing parameters**. The window "Routing parameters" is displayed.
2. Select the route "H4kSIP" or "Trk Grp 10". The settings for this route are displayed.
3. For "H4kSIP" or "Trk Grp 10", make the following settings:
 - Route type: **PABX**
 - No. and type, outgoing: **Country code**
 - Route optimize active: **No**
4. Click **Apply**. Your changes are saved.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2

Least cost routing

Basic settings:

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area " LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.
4. Go to "Settings > Lines/networking" and select the tab **Routes**.
5. Under "Digit transmission" area select "en-bloc sending".
6. Click the **Apply** button.

Least cost routing to the CO (ISDN):

The screenshot displays the configuration interface for Least Cost Routing (LCR) to the CO (ISDN). The interface is divided into several sections:

- Codes and flags**: Includes tabs for "Codes and flags", "Classes of service", "Dial plan", and "LCR - schedule". A "Digit analysis wizard" button is present.
- Table 1**: A table with columns "Name", "Dialed digits", and "Route table". The first row shows "CO", "0CZ", and "1".
- Route table**: A dropdown menu set to "1".
- Dial rule wizard**: A button to launch the wizard.
- Table 2**: A table with columns "Route", "Dial rule", and "min.". The first row shows "CO", "rule 1", and "15".

The **Dial rule wizard** dialog box is open, showing the following configuration:

- Edited dial rule: Dial rule 1
- Network provider's method of: Main network supplier
- Access code: (empty)
- Pause (max. 12 secs.): (empty)
- Authorization code: (empty)
- Dial rule format: A
- min. COS: 15
- Schedule: -
- Warning: None
- Type of Number (TON): Unknown

Buttons for "Help", "OK", and "Cancel" are at the bottom of the dialog.

1. In the system view, select **Least cost routing** -> **Dial plan**. The window "Dial plan" is displayed.
2. In the upper table, set the route to the CO. The table then shows, for example: Name: **co**, Dialed digits: **0cz**, Route table: **1**.
3. In the "Route table" selection field, check that route table 1 is selected (defined in the previous step). If not, select it.
4. Select the route **co** in the lower table in the column "Route".
5. In the "Dial rule" column, define the dial rule, select it, and click on **Dial rule wizard**. The Dial rule wizard is displayed.
6. In the Dial rule wizard, you can make the following settings:
 - Edited dial rule: **co**
 - Network provider's method of: **Main network provider**
 - Dial rule format: **A**
 - min. COS.: e.g. **15**
 - Schedule: e.g. **-**
 - Warning: e.g. **None**
 - Type of Number (TON): **Unknown**
7. Click **OK**. The Dial rule wizard is closed.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2

Least cost routing to HiPath 4000:

The first line should be routed to HiPath 4000. As an option, a second line can be configured for least cost routing via the CO. The second line bridges the gap in the case of LAN failure. During a LAN failure, calls are routed via the local CO to another HiPath 4000 gateway. All dial rules to HiPath 8000 must be configured using the international E.164 station number format.

The screenshot displays the configuration interface for dial plan settings. At the top, there are tabs for 'Codes and flags', 'Classes of service', 'Dial plan', and 'LCR - schedule'. Below these is a 'Digit analysis wizard' button. A table lists dial plan entries:

	Name	Dialed digits	Route table
1	Hp8k internal	-13XXX	5

Below this is a 'Route table' dropdown set to '5' and a 'Dial rule wizard' button. A second table shows route configurations:

	Route	Dial rule	min.
1	Hp8k	Dial rule 5	15
2	CO	Dial rule 7	15

Red circles highlight 'Dial rule 5' and 'Dial rule 7' in the second table. Red arrows point from these circles to two 'Dial rule wizard' dialog boxes. The left dialog box is titled 'Line for LAN failure, rerouted via CO' and shows settings for 'rerouting CO'. The right dialog box is titled 'Direct line to HiPath 8000' and shows settings for 'E.164 intern'.

Dial rule wizard (Left):

- Edited dial rule: rerouting CO
- Network provider's method of: Main network supplier
- Access code:
- Pause (max. 12 secs.):
- Authorization code:
- Dial rule format: D030400E2A
- min. COS: 15
- Schedule: .
- Warning: None
- Type of Number (TON): Unknown

Dial rule wizard (Right):

- Edited dial rule: E.164 intern
- Network provider's method of: Corporate network
- Access code:
- Pause (max. 12 secs.):
- Authorization code:
- Dial rule format: D496951E2A
- min. COS: 15
- Schedule: .
- Warning: None
- Type of Number (TON): Country code

1. In the system view, select **Least cost routing** -> **Dial plan**. The window "Dial plan" is displayed.
2. In the upper table, set the route to HiPath 4000. The table then shows, for example: Name: **H4k internal1**, Dialed digits: **-13XXX**, Route table: **5**.
3. In the "Route table" selection field, check that route table 1 is selected (defined in the previous step). If not, select it.
4. Select the route **H4k** in the lower table in the column "Route".

5. In the "Dial rule" column, define the dial rule, select it, and click on **Dial rule wizard**. The Dial rule wizard is displayed.
6. Make the following settings in the Dial rule wizard for the direct line to HiPath 8000:
 - Edited dial rule: **E.164 internal**
 - Network provider's method of: **Corporate network**
 - Dial rule format: e.g. **D496951E2A**
 - min. COS.: e.g. **15**
 - Schedule: e.g. -
 - Warning: e.g. **none**
 - Type of Number (TON): **Country code**
7. Select the route **CO** in the lower table in the column "Route".
8. In the "Dial rule" column, define the dial rule, select it, and click on **Dial rule wizard**. The Dial rule wizard is displayed.
9. Make the following settings in the Dial rule wizard for the line to be used for rerouting to the CO during LAN failure:
 - Edited dial rule: **rerouting CO**
 - Network provider's method of: **Main network provider**
 - Dial rule format: e.g. **D030400E2A**
 - min. COS.: e.g. **15**
 - Schedule: e.g. -
 - Warning: e.g. **none**
 - Type of Number (TON): **Unknown**
10. Click **OK**. The Dial rule wizard is closed.

System parameters -> Flags

1. In the system view, select **System parameters -> Flags**. The window "Flags" is displayed.
2. Make the following settings:
 - Table "Switches" -> E.164 numbering scheme: select the check box.
 - Area "Transit permission" -> External traffic transit: select the check box (for rerouting via CO to another HiPath 8000 gateway in the case of LAN failure).
3. Click **Apply**. Your changes are saved.

4.10.1.2 Settings in the HG 1500 WBM

Deactivating the "T.38 Fax"

1. Start WBM.
2. Select **Explorers -> Voice Gateway -> Codec Parameters**.
3. Right-click "Edit Codec Parameters". The "Codec Parameters" mask is displayed.
4. T.38 Fax: clear the check box.
5. Click **Apply**.
6. Click the diskette icon. Your changes are saved.
7. Click the reset icon. HG 1500 is reset.
8. Once HG 1500 is ready for operation, quit and restart WBM.

Resetting SIP parameters

1. Start WBM.
2. Select **Explorers -> Voice Gateway -> SIP Parameters**.
3. Right-click "Edit SIP Parameters". The "SIP Parameters" mask is displayed.
4. Reset the SIP parameters to the default values. These are:
 - SIP Transport Protocol
 - SIP via TCP: Yes
 - SIP via UDP: Yes
 - SIP via TLS: Yes
 - SIP session timer
 - RFC 4028 support: Yes
 - Session-Expires (sec): 1800
 - Minimal-SE (sec): 90
 - Provider calls
 - Maximum number of call possible via the provider: 0
5. Click **Apply**.
6. Click the diskette icon. Your changes are saved.
7. Click the reset icon. HG 1500 is reset.
8. Once HG 1500 is ready for operation, quit and restart WBM.

Adding PBX nodes

1. Start WBM.
2. Select **Explorers -> Voice Gateway -> PBX -> Nodes**.
3. Add PBX nodes:
 1. Right-click "Add PBX Node". The menu "Add PBX Node" is displayed.
 2. Enter the node number.
 3. Click **Apply**.
4. Click the diskette icon. Your changes are saved.
5. Click the reset icon. HG 1500 is reset.
6. Once HG 1500 is ready for operation, quit and restart WBM.

Editing IP addresses for the newly-added PBX node

1. Start WBM.
2. Select **Explorers -> Voice Gateway -> PBX -> Nodes -> <node number>**.
3. Edit IP addresses:
 1. Right-click "Edit IP Addresses". The menu "PBX Node / IP Addresses" is displayed.
 2. Make the following settings:
 - LAN trunking protocol: **SIP-Q**
 - HXG Gatekeeper Board 1 IP Address: Enter the IP address of the SIP Signaling Manager (SIPSM) for HiPath 8000.
 - Alive Monitoring: clear the check box
 - Security Level of Node Encryption: **traditional**
 3. Click **Apply**.
4. Click the diskette icon. Your changes are saved.
5. Click the reset icon. HG 1500 is reset.
6. Once HG 1500 is ready for operation, quit and restart WBM.

Adding route station numbers

Station numbers do not have to be configured in WBM under **Explorers -> Voice Gateway -> PBX -> Routing** for HiPath 4000.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2

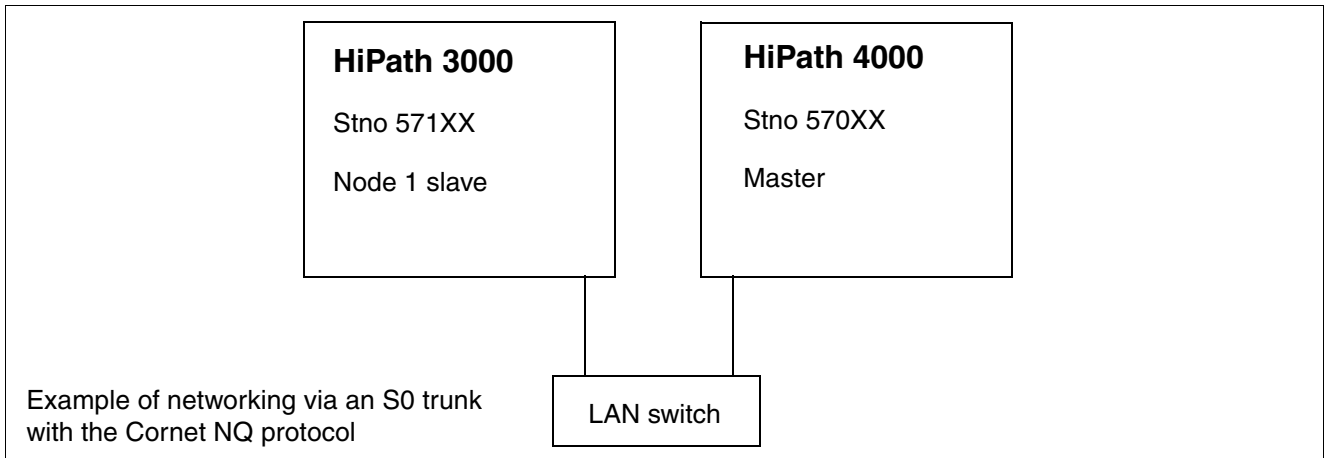
4.10.2 HiPath 4000 V5 Configuration

The configuration of the HiPath 4000 is described in detail in the "SIP Connectivity" chapter of the Service Manual for HiPath 4000 V5, Volume 4 - IP Solutions. The commands for configuring a HiPath 4000 for SIP-Q can be found in the "SIP-Q Trunking" section.

4.11 Networking HiPath 3000 V9 with HiPath 4000 V4 via TDM

4.11.1 Target Configuration

The target configuration involves establishing a network in a HiPath 3000 V8 to a HiPath 4000 V4 via TDM.



4.11.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > Trunks".
3. Double-click the parameter field once in the row containing the required STLS or STMD trunk.
4. Select the protocol in the pop-up window under "ISDN flags > Protocol: Description" (S0: CorNet-NQ Slave CR=2 CHI=S2 (standard)); the protocol applies at all times to the port; in other words, there are always two trunks assigned to an S0 port.
5. Click Apply.
6. Click Close.
7. Select a free route in the row containing the required STLS or STMD trunk (e.g., Trk Grp 2).
8. Assign the same route (e.g., Trk Grp 2) to the second trunk associated with the S0 port.
9. Click Apply.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with HiPath 4000 V4 via TDM

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the selected route (e.g., Trk Grp 2).
3. Enter the route name (e.g., HiPath 4000).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Select "PABX" under "Route type" for the trunk group selected.
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number (e.g., 1).
3. Click Apply.

Configure LCR

1. Select "Least cost routing > Codes and flags".
2. Select "Activate LCR".
3. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 4000 station numbers (e.g., -570XX).
3. Assign a route table to the station number (e.g., route table 2).
4. Select the chosen route (e.g., Trk Grp 2) for the route table.
5. Assign a dial rule to the route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.
7. Enter "E1A" as the dial rule format.
8. Click Apply.
9. Transfer the CDB to HiPath 3000 (delta mode possible).



Important: For an ISDN direct interconnection between HiPath 3000 and HiPath 4000, if the camp-on functionality shall be set (e.g. if an incoming call from HiPath 4000 to a HiPath 3000 busy subscriber occurs) then the following Manager E configuration must be applied:
Set under the S₀ trunks that refer to the HiPath 4000 Ext. SIP Trunks -> **Param** column (double-click) -> **General flags** tab -> **Circuit flags** section: check the **Call prio./immed. tone call wait.** flag.

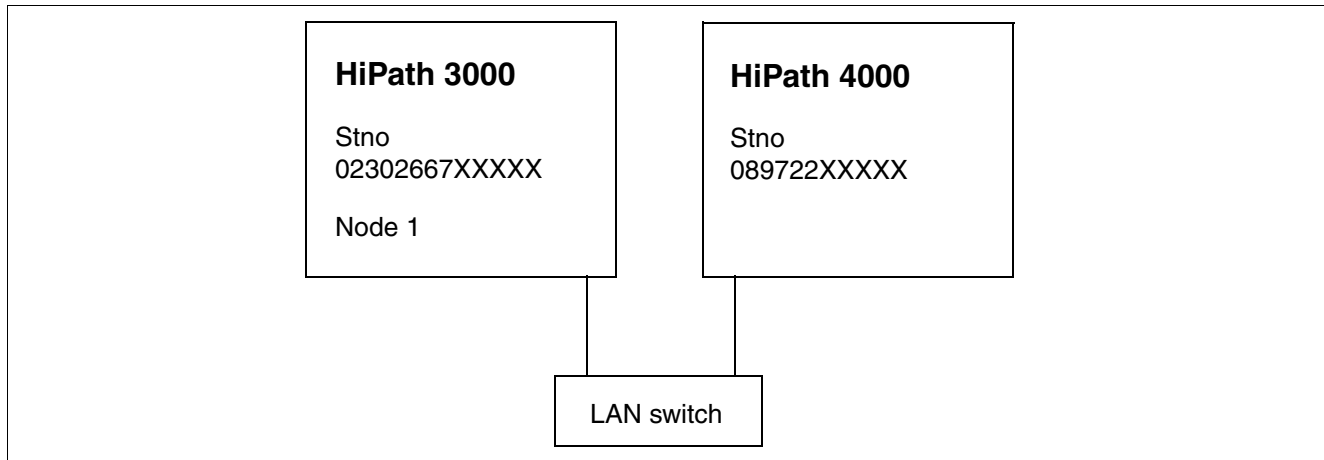
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 and HiPath 4000 V4 with E.164

4.12 Networking HiPath 3000 V8 and HiPath 4000 V4 with E.164

4.12.1 Target Configuration

The target configuration involves establishing a network in a HiPath 3000 V8 to a HiPath 4000 V4 with E.164.



Prerequisites

Networking is configured between HiPath 3000 and HiPath 4000 as described in [Section 4.9](#) and [Section 4.11](#).

4.12.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "System parameters > Flags > E.164 numbering scheme".
3. Activate "System parameters > Display > outreach call number transparent" (if the chargeable feature is active on a remote CO connection and you want to use breakout there; displays and caller lists relevant).
4. Click Apply.

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Click "Trk Grp11".
3. Select "Country code" under "No. and type, outgoing".
4. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the HiPath 4000 station numbers (e.g., 0C0-89722-Z).
3. Assign a route table to the station number (e.g., route table 6).
4. Select route 11 in the Ext. H323 route for the route table.
5. Assign a dial rule to route 11 (e.g., dial rule 6).
6. Select "Corporate network" as the network provider's method for dial rule 6 in the Dial rule wizard.
7. Enter "D49E3A" as the dial rule format.
8. Select "Country code" under "Type of Number (TON)".
9. Enter the HiPath 4000 station numbers (e.g., 0C00-49-89722-Z).
10. Assign a route table to the station number (e.g., route table 7).
11. Select route 11 in the Ext. H323 route for the route table.
12. Assign a dial rule to route 11 (e.g., 7).
13. Select "Corporate network" as the network provider's method for dial rule 7 in the Dial rule wizard.
14. Enter "E3A" as the dial rule format.
15. Select "Country code" under "Type of Number (TON)" (if Node1 is in the same location as HiPath 4000, another LCR entry is needed, for example, 0C722-Z with D4989E2A and "Country code" as the TON).
16. Click Apply.
17. Transfer the CDB to HiPath 3000 (delta mode possible).

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V8 and HiPath 4000 V4 with E.164

Note

If you want to use a non-standard setting (for the audio codes, for instance) with the Ext. H323 connection to HiPath 4000, you must configure a node that references the IP address of the HiPath 4000 under Voice Gateway in the HG 1500. A routing entry is not necessary here.

The required settings can then be made via this node. Alive monitoring from the HiPath 3000 to the HiPath 4000 is generally only possible with a "ping"; this is also set with the node entry.

When using the DB Feature Server in the scenario described above, this node must be entered as an "external HiPath 5000RSM/Allserve domain". The node entry is then automatically created on all HGs. A number entry in the Call No. field is not needed for this.

Special features of the HiPath 5000 RSM network

Calls between the nodes in the RSM network are only set up with speed-dialing numbers (the called party is "Unknown"). This is necessary because in future only extensions will be loaded to the HG 1500 routing table (CAR table).

For correct number display, only enter the location number for all RSM nodes (HiPath 3000 and HiPath 2000 / HiPath OpenOffice EE) under "Lines/networking > E.164 Table". None of the other E.164 nodes (HiPath 4000) are entered in this table.

4.13 Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

Overview

This section describes the configuration of the SIP-Q networking between HiPath 3000 and OpenScape Voice. This requires HiPath 3000 settings in the Manager E and in the WBM of the HG 1500. OpenScape Voice settings are made in the Common Management Portal and in StartCli. The Common Management Portal is also used for OpenScape Branch.

Requirements

- HiPath 3000, V8 MR5 and later
- OpenScape Voice, V5 R0 and later

Contents

This section describes the following topics:

- Section 4.13.1, "Networking Limitations"
- Section 4.13.2, "Configuration of HiPath 3000"
- Section 4.13.3, "Configuring OpenScape Voice"
- Section 4.13.4, "Configuring OpenScape Branch"

4.13.1 Networking Limitations

The following restrictions have to be applied:

- The connection of analog trunks to HiPath 3000 gateways is not released (Exception: Brazil, due to dual-sided “Silent Reversal” support in Brazilian exchanges).
- Networking of HiPath 3000 gateways to one another or with systems other than OpenScape Voice is not supported. HiPath 5000 Real-Time Services Manager RSM is not supported. Networking of HiPath 3000 gateways to OpenScape Office must use a star structure.
- Path replacement via SIP-Q V2 is not supported for TDM workpoints which are connected to a HiPath 3000 gateway.
- To avoid poor voice quality for transit connections, avoiding the use of the G.729 voice codec is recommended. The use of G.729 voice compression could degrade voice quality (especially when HiPath 3000 HFA telephones are connected to OpenScape Voice). The use of the G.711 codec is recommended.

Transit trunk connections can stem from features such as Conference, Call Forwarding, and Transfer as path replacement is not supported.

- There is no cross-system support of features such as call pick groups, group calls and hunt groups between OpenScape Voice and HiPath 3000 gateways. The groups must only contain OpenScape Voice, or only HiPath 3000 stations. The sole exception is the “One Number Service” of OpenScape Office.
- Encryption (SPE) is not supported between OpenScape Voice and HiPath 3000 gateways.
- The TDM workpoints and trunk lines connected to a HiPath 3000 gateway cannot be integrated into OpenScape Voice applications and cannot use these. Dialing from OpenScape Voice applications over HiPath 3000 gateways will be supported from HiPath 3000 V8 MR5 onward.
- Only networking with an E.164 numbering plan will be supported.

4.13.2 Configuration of HiPath 3000

Contents

This section describes the following topics:

- Section 4.13.2.1, "Settings in the Manager E of HiPath 3000"
- Section 4.13.2.2, "Settings in the WBM of the HG 1500"

4.13.2.1 Settings in the Manager E of HiPath 3000

Procedure

1. Start the Manager E.
2. Work through the following sections in sequence.

Contents

Make the following settings in the Manager E of HiPath 3000:

- Section 4.13.2.1.1, "Lines/networking -> IP Trunks"
- Section 4.13.2.1.2, "Lines/networking -> Routes (route to CO)"
- Section 4.13.2.1.3, "Lines/networks -> Routes (route to OpenScape Voice)"
- Section 4.13.2.1.4, "Lines/networking -> Routing parameters"
- Section 4.13.2.1.5, "Network -> Ext. SIP"
- Section 4.13.2.1.6, "Network -> Gatekeeper"
- Section 4.13.2.1.7, "Least Cost Routing"
- Section 4.13.2.1.8, "System parameters -> Flags"
- Section 4.13.2.1.9, "Flag: Transit allowed via Hook-on"
- Section 4.13.2.1.10, "Phone Payload Security"

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.1.1 Lines/networking -> IP Trunks

Add IP trunks of the "Ext. SIP" type. Proceed as follows:

1. Select **Systemview** -> **Settings** -> **Lines/networking** -> **IP Trunks**. The "IP Trunks" window is displayed.
2. Make the following settings under "Selection":
 - Gatekeeper HG1500: e.g. **s1ot 5**
 - Access gateway resources: Activate the checkbox.
3. Make the following settings under "Number":
 - e.g. **10**
 - **Ext . SIP**

Click **Add**. Ten IP trunks of the "Ext.SIP" type are inserted in the "Trunks" table. Each row then contains the following information, for example:

Trunk: **Line 21**, Code: **7821**, Type: **Ext . SIP**, Route: **Hp8k**.

(Hp8k = OpenScape Voice).

4. Click **Apply**. The changes are stored.

4.13.2.1.2 Lines/networking -> Routes (route to CO)

Set up a route to the CO. Proceed as follows:

1. Select **Systemview** -> **Settings** -> **Lines/networking** -> **Routes**. The "Routes" window is displayed.
2. Select the "Trk Grp. 1" route (route to CO). The settings of this route are displayed.
3. Make the following settings for "Trk Grp. 1":
 - Route Name/Name: **co**
 - PABX number-incoming: For the "Country code", "Local area code" and "PABX number", enter the location number in the E.164 format, e.g. **49, 69, 5113**.
 - Location number: Activate the checkbox.
4. Click **Apply**. The changes are stored.

4.13.2.1.3 Lines/networks -> Routes (route to OpenScape Voice)

Set up a route to OpenScape Voice (= Hp8k). Proceed as follows:

1. Select **Systemview -> Settings -> Lines/networking -> Routes**. The "Routes" window is displayed.
2. Select the "Trk Grp. 10" route (route for OpenScape Voice). The settings of this route are displayed.
3. Make the following settings for "Trk Grp. 10":
 - Route Name/Name: **Hp8k**
 - Second CO code: **0** as the second CO code.
 - PABX number-incoming: For "Country code", "Local area code" and "PABX number", enter the location number in the E.164 format. This number is usually the same number as in the route to the CO (see previous section); thus, for example, **49, 69, 5113**.
 - Digit transmission: **en-block sending**
 - Always use DSP: Activate the checkbox.
4. Click **Apply**. The changes are stored.

4.13.2.1.4 Lines/networking -> Routing parameters

The routing parameters must be set up for the route to OpenScape Voice "Hp8k" that was configured in the previous section. Proceed as follows:

1. Select **Systemview -> Settings -> Lines/networking -> Routing parameters**. The "Routing parameters" window is displayed.
2. Select the "Hp8k" route. The settings of this route are displayed.
3. Make the following settings for the "Hp8k" route:
 - Route type: **PABX**
 - No. and type, outgoing: **Country code**
 - Rerouting active: **No**
4. Click **Apply**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.1.5 Network -> Ext. SIP

Set up the parameters for the external SIP registrar. Proceed as follows:

1. Select **Systemview** -> **Settings** -> **Network** -> **Ext. SIP**. The "Ext. SIP" window is displayed.
2. Activate the "Operate with external SIP-Registrar" checkbox. Selection fields, entry fields and selection options in the "Gateway" and "Security" window areas are enabled.
3. Make the following settings in the "Gateway" window area:

Environment:	HiPath 8000
Trunking mode:	SIP-Q
Call Number:	Alias number of the OpenScape Voice end point, e.g. 13310 .
Registration expiry:	At least 300 .
IP address:	Select one of the following sections as required for the system: <ul style="list-style-type: none">• "Settings for »TLS Not Activated« (TCP trunking to OpenScape Voice)"• "Settings for »TLS Activated« (TLS trunking to OpenScape Voice)"• "Settings for »Branch Solution with OpenScape Branch«"
Port:	
TLS:	
Alternate RG IP address:	
Perform registration:	Activate the checkbox.
Security:	Optional.

4. Make the following settings in the "Security" window area:
 - a) If digest authentication is needed for OpenScape Voice: Activate the "Authentication Required" option. The entry fields are activated.
 - b) Complete the entry fields:
 - SIP User ID: e.g. **hipath3000br13**
 - Password: Enter the password.
 - Confirm password: Re-enter the password to confirm.
 - Realm: Enter the range for which the authentication should apply, for example, **sol**.
5. Click **Apply**. The changes are stored.

Settings for »TLS Not Activated« (TCP trunking to OpenScape Voice)

Set the following items:

- IP address: Enter the IP address of the SIP Signaling Manager [sipsm1 (for node 1) or sipsm2 (for node 2)] of OpenScape Voice, e.g. **10.22.14.24**.
- Port: **5060**
- TLS: Deactivate the checkbox.
- Alternate RG IP address: Enter a fallback IP address, i.e. the IP address of sipsm2 for node 2 or the IP address of sipsm1 for node 1.

Return to step 3.

Settings for »TLS Activated« (TLS trunking to OpenScape Voice)

Set the following items:

- IP address: Enter the IP address of the SIP Signaling Manager [sipsm3 (for node 1) or sipsm4 (for node 2)] of OpenScape Voice, e.g. **10.22.14.26**.
- Port: **5061**
- TLS: Activate the checkbox.
- Alternate RG IP address: Enter a fallback IP address, i.e. the IP address of sipsm4 for node 2 or the IP address of sipsm3 for node 1.

Return to step 3.

Settings for »Branch Solution with OpenScape Branch«

Set the following items:

- IP address: Enter the IP address of the OpenScape Branch proxy server, e.g. **10.22.113.10**.
- Port: **5060**
- TLS: Deactivate the checkbox.
- Alternate RG IP address: As an alternate IP address, enter the IP address of sipsm1 for TCP or the IP address of sipsm3 for TLS.

Return to step 3.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.1.6 Network -> Gatekeeper

Enter the NTP server address. Proceed as follows:

1. Select **Systemview** -> **Settings** -> **Network** -> **Gatekeeper**. The "Gatekeeper" window is displayed.
2. In the "SNTP Server" area, make the following settings:
 - IP address: Enter the IP address of the NTP servers, e.g. **10.21.255.7**.



Important: For TLS connections, the same time must be set for all components. This is achieved by all components using the same NTP server.

3. Click **Apply**. The changes are stored.

4.13.2.1.7 Least Cost Routing

The first route should lead to the **CO**. As an option, a second route can be configured for least cost routing to OpenScape Voice (**Hp8k**). This route is only used to bridge trunk failures. During a trunk failure, calls are routed to OpenScape Voice (with a transition to another OpenScape Voice gateway).

This section describes the following topics:

- Basic Settings
- First Route: Least Cost Routing to CO
- Second Route: Least Cost Routing to OpenScape Voice

Basic Settings

Proceed as follows:

1. Select **Systemview -> Settings -> Least Cost Routing -> Flags and COS**. The "Flags and COS" window is displayed.
2. Make the following settings:
 - Activate LCR: Activate the checkbox.
 - In the "Class of service" table, assign COS 14 to all phone numbers.
3. Click **Apply**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

First Route: Least Cost Routing to CO

[Overview](#)

Here you are given an overview of the settings to be made in this section. This is followed by a detailed description of the procedure.

Dialed digits

The upper table shows which LCR rule, e.g. **Hp8k local**, is to be applied for which dialed digits, e.g. **0CZ**.

	Name	Dialed digits	Route table	Acc. code	COS	Emergency number
1	Hp8k local	0CZ	1	no	yes	no
2	Hp8k nat	0C0-Z	2	no	yes	no
3	Hp8k int	0C00-Z	3	no	yes	no

Route tables

A route table must be created for each LCR rule defined above.

1. For Local Calls:

- LCR rule, dialed digits and route table to be used: **Hp8k local, 0CZ, 1**
- Route table **1**:

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 city	14	-	Display + tone

2. For National Calls:

- LCR rule, dialed digits and route table to be used: **Hp8k nat, 0C0-Z, 2**
- Route table **2**:

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 nat.	14	-	Display + tone

3. For International Calls:

- LCR rule, dialed digits and route table to be used: **Hp8k int., 0C00-Z, 3**
- Route table **3**:

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 int.	14	-	Display + tone

Dial rule table

The dial rules listed in the above route tables are defined as follows:

	Rule name	Rule format	Procedure	TON
1	E.164 city	D4969E2A	Corporate Network	Country code
2	E.164 nat.	D49E3A	Corporate Network	Country code
3	E.164 int.	E3A	Corporate Network	Country code
4	CO	A	Main network provider	Unknown



Important: All dial rules for OpenScape Voice must be configured in the international E.164 phone number format.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

[For Local Calls](#)

Proceed as follows:

1. Select **Systemview** -> **Least cost routing** -> **Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, set the route to the CO. The table then shows, for example: Name: **Hp8k1oca1**, Dialed digits: **0CZ**, Route table: **1**.
3. In the "Route table" selection field, check that route table 1 is selected (defined in the previous step). If not, select it.
4. **Route to CO:**
 - a) In the "Route" column in the lower table, select the **CO** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **CO**
 - Network provider's method of: **Main network provider**
 - Dial rule format: **A**
 - min. COS.: e.g. **14**
 - Schedule: e.g. **-**
 - Warning: e.g. **None**
 - Type of number (TON): **Unknown**
 - d) Click **OK**. The dial rule wizard is closed. The dial rule is entered in the lower table.
5. **Route to OpenScape Voice:**
 - a) In the "Route" column of the lower table, select the **Hp8k** route (directly under the route to CO).
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:



Important: All dial rules to OpenScape Voice must be configured in the international E.164 phone number format.

- Edited dial rule: **E.164 city**
- Network provider's method of: **Corporate Network**

- Dial rule format: e.g. **D4969E2A**
- min. COS.: e.g. **14**
- Schedule: e.g. -
- Warning: e.g. **Display + tone**
- Type of Number (TON): **Country code**

d) Click **OK**. The dial rule wizard is closed. The dial rule is entered in the lower table.

6. Click **Apply**. The changes are stored.

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
1	Hp8k local	0CZ	1

Route table 1 1

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 city	14	-	Display + tone

To CO:

Dial rule wizard

Edited dial rule	CO
Network provider's method of	Main network supplier
....	
Dial rule format	A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Unknown

To OpenScape Voice:

Dial rule wizard

Edited dial rule	E.164 city
Network provider's method of	Corporate network
....	
Dial rule format	D4969E2A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Country code

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

[For National Calls](#)

Proceed as follows:

1. Select **Systemview** -> **Least cost routing** -> **Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, set the route to the CO. The table then shows, for example:
Name: **Hp8k nat**, Dialed digits: **0C0-z**, Route table: **2**.
3. In the "Route table" selection field, check that route table 2 is selected (defined in the previous step). If not, select it.
4. **Route to CO:**
 - a) In the "Route" column in the lower table, select the **CO** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **CO**
 - Network provider's method of: **Main network supplier**
 - Dial rule format: **A**
 - min. COS.: e.g. **14**
 - Schedule: e.g. -
 - Warning: e.g. **None**
 - Type of number (TON): **Unknown**
 - d) Click **OK**. The dial rule wizard is closed.
5. **Route to OpenScape Voice:**
 - a) In the "Route" column of the lower table, select the **Hp8k** route (directly under the route to CO).
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:



Important: All dial rules to OpenScape Voice must be configured in the international E.164 phone number format.

- Edited dial rule: **E.164 nat.**

- Network provider's method of: **Corporate network**
- Dial rule format: e.g. **D49E3A**
- min. COS.: e.g. **14**
- Schedule: e.g. **-**
- Warning: e.g. **Display + tone**
- Type of Number (TON): **Country code**

d) Click **OK**. The dial rule wizard is closed.

6. Click **Apply**. The changes are stored.

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
2	Hp8k nat	0C0-Z	2

Route table 2

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 nat.	14	-	Display + tone

To CO:

Dial rule wizard

Edited dial rule	CO
Network provider's method of	Main network supplier
....	
Dial rule format	A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Unknown

To OpenScope Voice:

Dial rule wizard

Edited dial rule	E.164 nat.
Network provider's method of	Corporate network
....	
Dial rule format	D49E3A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Country code

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

[For International Calls](#)

Proceed as follows:

1. Select **Systemview** -> **Least cost routing** -> **Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, set the route to the CO. The table then shows, for example:
Name: **Hp8k int**, Dialed digits: **0C00-z**, Route table: **3**.
3. In the "Route table" selection field, check that route table 3 is selected (defined in the previous step). If not, select it.
4. **Route to CO:**
 - a) In the "Route" column in the lower table, select the **CO** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **CO**
 - Network provider's method of: **Main network supplier**
 - Dial rule format: **A**
 - min. COS.: e.g. **14**
 - Schedule: e.g. **-**
 - Warning: e.g. **None**
 - Type of number (TON): **Unknown**
 - d) Click **OK**. The dial rule wizard is closed.
5. **Route to OpenScape Voice:**
 - a) In the "Route" column of the lower table, select the **Hp8k** route (directly under the route to CO).
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:



Important: All dial rules to OpenScape Voice must be configured in the international E.164 phone number format.

- Edited dial rule: **E.164 int.**

- Network provider's method of: **Corporate network**
- Dial rule format: e.g. **E3A**
- min. COS.: e.g. **14**
- Schedule: e.g. -
- Warning: e.g. **Display + tone**
- Type of Number (TON): **Country code**

d) Click **OK**. The dial rule wizard is closed.

6. Click **Apply**. The changes are stored.

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
3	Hp8k int	0C00-Z	3

Route table 3

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	14	-	None
2	Hp8k	E.164 int.	14	-	Display + tone

To CO:

Dial rule wizard

Edited dial rule	CO
Network provider's method of	Main network supplier
....	
Dial rule format	A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Unknown

To OpenScope Voice:

Dial rule wizard

Edited dial rule	E.164 int.
Network provider procedure	Corporate network
....	
Dial rule format	E3A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Country code

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

Second Route: Least Cost Routing to OpenScape Voice

Overview

Here you are given an overview of the settings to be made in this section. This is followed by a detailed description of the procedure.

Dialed digits

The upper table shows which LCR rule, e.g. **int. 10x**, is to be applied for which dialed digits, e.g. **-10x**.

	Name	Dialed digits	Route table	Acc. code	COS	Emergency number
4	int. 10x	-10X	5	no	yes	no
5	HQ30	-30XXX	17	no	yes	no
6	HQ10	0C0-3040030XXX	8	no	yes	no

Route tables:

A route table must be created for each LCR rule defined above.

1. Dialing a Short Phone Number Within the Same Location in OpenScape Voice:

- LCR rule, dialed digits and route table to be used: **int. 10x, -10x, 5**
- Route table **5**:

	Route	Dial rule	min. COS	Schedule	Warning
1	Hp8k	E.164 internal	14	-	None
2	CO	Rerouting HQ30	14	-	Display + tone

2. Dialing a Short Phone Number of All Other Locations of OpenScape Voice:

- LCR rule, dialed digits and route table to be used: **HQ30, -30xxx, 17**
- Route table **17**:

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	Rerouting HQ30	15	-	None
2	Hp8k	HQ30	14	-	None
3	CO	Rerouting HQ30	14	-	Display + tone

Three routes must be set up to avoid loops.

3. E.164 Routing to All Other Phone Numbers in OpenScape Voice:

- LCR rule, dialed digits and route table to be used: **HQ10**, **0CO-3040030XXX**, **8**
- Route table **8**:

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	15	-	None
2	Hp8k	E.164 nat.	14	-	None
3	CO	CO	14	-	Display + tone

Three routes are required to avoid loops.

Dial rule table:

The dial rules listed in the above route tables are defined as follows:

	Rule name	Rule format	Procedure	TON
1	CO	A	Main network supplier	Unknown
2	E.164 nat.	D49E3A	Corporate Network	Country code
3	E.164 internal	D49695113A	Corporate Network	Country code
4	HQ30	D4930400E2A	Corporate Network	Country code
5	Rerouting HQ30	D030400E2A	Main network supplier	Unknown



Important: All dial rules for OpenScape Voice must be configured in the international E.164 phone number format.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

[Dialing a Short Phone Number Within the Same Location in OpenScape Voice](#)



Important: If HiPath 3000 and OpenScape Voice stations have the same CO number, the phone number must be searched for locally in HiPath 3000 and in OpenScape Voice. The settings in this section take this situation into account.

Routes that need to be set up:

- The first route goes "To OpenScape Voice".
- Optionally, the second route can be set up "For LAN failure – Reroute via CO". This second route is used to bridge LAN failures. During LAN failure, calls must be conducted through the local CO to another gateway of OpenScape Voice.

Procedure:

Proceed as follows:

1. Select **Systemview** -> **Least cost routing** -> **Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, define the route to OpenScape Voice. The table then shows, for example: Name: **int. 10x**, Dialed digits: **-10x**, Route table: **5**.
3. In the "Route table" selection field, check that route table 5 is selected (defined in the previous step). If not, select it.
4. **First route "To OpenScape Voice":**
 - a) In the "Route" column in the lower table, select the **Hp8k** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **E.164 internal**
 - Network provider's method of: **Corporate network**
 - Dial rule format: **D49695113A**
 - min. COS: **14**
 - Schedule: **-**
 - Warning: **None**
 - Type of Number (TON): **Country code**
 - d) Click **OK**. The dial rule wizard is closed.

5. **Second route "For LAN failure – Reroute via CO":**

- a) In the "Route" column in the lower table, select the **CO** route.
- b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
- c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **Rerouting HQ30**
 - Network provider's method of: **Main network provider**
 - Dial rule format: **D030400E2A**. The phone number of another gateway is used to reach the OpenScape Voice network.
 - min. COS: **14**
 - Schedule: **-**
 - Warning: **Display + tone**
 - Type of number (TON): **Unknown**
- d) Click **OK**. The dial rule wizard is closed.

6. Click **Apply**. The changes are stored.

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
4	int. 10x	-10X	5

Route table 5

	Route	Dial rule	min. COS	Schedule	Warning
1	Hp8k	E.164 internal	14	-	None
2	CO	Rerouting HQ30	14	-	Display + tone

To OpenScape Voice:
Dial rule wizard

Edited dial rule	E.164 internal
Network provider's method of	Corporate Network
....	
Dial rule format	D49695113A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Country code

For LAN failure – Reroute via CO:
Dial rule wizard

Edited dial rule	Rerouting HQ30
Network provider procedure	Main network supplier
....	
Dial rule format	D030400E2A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Unknown

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

[Dialing a Short Phone Number of All Other Locations of OpenScape Voice](#)

Routes that need to be set up:

- The first route "From OpenScape Voice via HiPath 3000 to CO" is only intended for calls from OpenScape Voice via HiPath 3000 to the CO. This direction is used if OpenScape Voice is not available and OpenScape Branch redirects the call via HiPath 3000. The "min. COS" (minimum class of service) value must be set to 15 so that only trunks and no stations can use this route.
- The second route "From HiPath 3000 to OpenScape Voice" is used for calls from HiPath 3000 to OpenScape Voice. The "min. COS" (minimum class of service) value must be set to 14 so that HiPath 3000 telephones can use this route.
- The third route "For LAN failure – Reroute via CO" is used if the LAN on the route to OpenScape Voice/OpenScape Branch fails. During LAN failure, calls must be conducted through the local CO to another gateway of OpenScape Voice.

Procedure:

Proceed as follows to set up the routes:

1. Select **Systemview** -> **Least cost routing** -> **Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, define which route table is to be used for which dialed digits. The table then shows, for example: Name: **HQ30**, Dialed digits: **-30xxx**, Route table: **17**.
3. In the "Route table" selection field, check that the route table **17** was selected automatically (defined in the previous step). If not, select it.
4. **First route "From OpenScape Voice via HiPath 3000 to CO":**
 - a) In the "Route" column in the lower table, select the **CO** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **Rerouting HQ30**
 - Network provider's method of: **Main network provider**
 - Dial rule format: **D030400E2A**
 - min. COS: **15**
 - Schedule: **-**
 - Warning: **None**
 - Type of number (TON): **Unknown**

d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.

5. **Second route "From HiPath 3000 to OpenScape Voice":**

a) In the "Route" column in the lower table, select the **Hp8k** route.

b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.

c) Make the following settings in the dial rule wizard:

- Edited dial rule: **HQ30**
- Network provider's method of: **Corporate Network**
- Dial rule format: e.g. **D4930400E2A**
- min. COS: **14**
- Schedule: -
- Warning: **None**
- Type of Number (TON): **Country code**

d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.

6. **Third route "For LAN failure – Reroute via CO":**

a) In the "Route" column in the lower table, select the **CO** route.

b) In the "Dial rule" column, select the **Rerouting HQ30** dial rule for the selected route and then click **Dial rule wizard**. The dial rule wizard is displayed.

c) Make the following settings in the dial rule wizard:

- Edited dial rule: **Rerouting HQ30**
- Network provider's method of: **Main network supplier**
- Dial rule format, e.g. **D030400E2A**
- min. COS: **14**
- Schedule: -
- Warning: **Display + tone**
- Type of number (TON): **Unknown**

d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.

7. Click **Apply**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
5	HQ30	-30XXX	17

Route table 17

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	Rerouting HQ30	15	-	None
2	Hp8k	HQ30	14	-	None
3	CO	Rerouting HQ30	14	-	Display + tone

From OpenScape Voice via HiPath 3000 to CO:

Dial rule wizard

Edited dial rule	Rerouting HQ30
Network provider's method of	Main network supplier
....	
Dial rule format	D030400E2A
min. COS	15
Schedule	-
Warning	None
Type of Number (TON)	Unknown

From HiPath 3000 to OpenScape Voice:

Dial rule wizard

Edited dial rule	HQ30
Network provider's method of	Corporate network
....	
Dial rule format	D4930400E2A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Country code

For LAN failure – Reroute via CO:

Dial rule wizard

Edited dial rule	Rerouting HQ30
Network provider's method of	Main network supplier
....	
Dial rule format	D030400E2A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Unknown

[E.164 Routing to All Other Phone Numbers in OpenScape Voice](#)



Important: All phone numbers in the OpenScape Voice network must be set up for least cost routing. The phone numbers can be found in the OpenScape Voice Assistant under **Global Translation and Routing -> Directory Number -> Office Codes**.

Routes that need to be set up:

- The first route "From OpenScape Voice via HiPath 3000 to CO" is only intended for calls from OpenScape Voice via HiPath 3000 to the CO. This route is used when another node is in restricted operation (WAN failure) and OpenScape Voice routes the call via HiPath 3000. The "min. COS" (minimum class of service) value must be set to 15 so that only trunks and no stations can use this route.
- The second route "From HiPath 3000 to OpenScape Voice" is used for calls from HiPath 3000 to OpenScape Voice. The "min. COS" (minimum class of service) value must be set to 14 so that HiPath 3000 telephones can use this route.
- The third route "For LAN failure – Reroute via CO" is used if the LAN on the route to OpenScape Voice/OpenScape Branch fails. During LAN failure, calls must be conducted through the local CO to another gateway of OpenScape Voice.

Procedure:

Proceed as follows to set up the routes:

1. Select **Systemview -> Least cost routing -> Dial plan**. The "Dial plan" window is displayed.
2. In the upper table, define which route table is to be used for which dialed digits. The table then shows, for example: Name: **HQ10**, Dialed digits: **0C0-3040030xxx**, Route table: **8**.
3. In the "Route table" selection field, check that route table **8** was selected automatically (defined in the previous step). If not, select it.
4. **First route "From OpenScape Voice via HiPath 3000 to CO":**
 - a) In the "Route" column in the lower table, select the **co** route.
 - b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
 - c) Make the following settings in the dial rule wizard:
 - Edited dial rule: **co**
 - Network provider's method of: **Main network supplier**
 - Dial rule format: **A**
 - min. COS: **15**

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

- Schedule: -
 - Warning: **None**
 - Type of number (TON): **Unknown**
- d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.
5. **Second route "From HiPath 3000 to OpenScape Voice":**
- a) In the "Route" column in the lower table, select the **Hp8k** route.
- b) In the "Dial rule" column, define the dial rule for the selected route, highlight it and then click **Dial rule wizard**. The dial rule wizard is displayed.
- c) Make the following settings in the dial rule wizard:
- Edited dial rule: **E.164 nat.**
 - Network provider's method of: **Corporate Network**
 - Dial rule format: e.g. **D49E3A**
 - min. COS: **14**
 - Schedule: -
 - Warning: **None**
 - Type of Number (TON): **Country code**
- d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.
6. **Third route "For LAN failure – Reroute via CO":**
- a) In the "Route" column in the lower table, select the **CO** route.
- b) In the "Dial rule" column, select the **CO** dial rule for the selected route and then click **Dial rule wizard**. The dial rule wizard is displayed.
- c) Make the following settings in the dial rule wizard:
- Edited dial rule: **CO**
 - Network provider's method of: **Main network supplier**
 - Dial rule format: **A**
 - min. COS: **14**
 - Schedule: -
 - Warning: **Display + tone**
 - Type of number (TON): **Unknown**

d) Click **OK**. The dial rule wizard is closed and the changes are adopted in the route table.

7. Click **Apply**. The changes are stored.

Result (Manager E tables and entry windows):

Dial plan

	Name	Dialed digits	Route table
6	HQ10	0C0-3040030XXX	8

Route table 8

	Route	Dial rule	min. COS	Schedule	Warning
1	CO	CO	15	-	None
2	Hp8k	E.164 nat.	14	-	None
3	CO	CO	14	-	Display + tone

From OpenScape Voice via HiPath 3000 to CO:

Dial rule wizard

Edited dial rule	CO
Network provider's method of	Main network supplier
....	
Dial rule format	A
min. COS	15
Schedule	-
Warning	None
Type of Number (TON)	Unknown

From HiPath 3000 to OpenScape Voice:

Dial rule wizard

Edited dial rule	E.164 nat.
Network provider's method of	Corporate network
....	
Dial rule format	D49E3A
min. COS	14
Schedule	-
Warning	None
Type of Number (TON)	Country code

For LAN failure – Reroute via CO:

Dial rule wizard

Edited dial rule	CO
Network provider's method of	Main network supplier
....	
Dial rule format	A
min. COS	14
Schedule	-
Warning	Display + tone
Type of Number (TON)	Unknown

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.1.8 System parameters -> Flags

Proceed as follows:

1. Select **Systemview** -> **System parameters** -> **Flags**. The "Flags" window is displayed.
2. Make the following settings in the "Switch" table:
 - Path optimization: Deactivate the checkbox.
 - E.164 numbering scheme: Activate the checkbox.
 - If a HiPath 4000 is contained in the network:
 - Direct Media Connection (DMC): Activate the checkbox.
 - HiPath 4000 networking: Early DMC: Activate the checkbox.
 - If TLS is used:
 - SPE support: Activate the checkbox.
 - SPE advisory tone: Activate the checkbox.
3. Make the following settings in the "Transit permission" area:
 - External traffic transit: Activate the checkbox.
If the LAN fails, this setting enables forwarding via the CO to another OpenScape Voice gateway.
4. Click **Apply**. The changes are stored.

4.13.2.1.9 Flag: Transit allowed via Hook-on

Overview

For certain internal stations, the following can be defined by activating the "Transit allowed via Hook-on" flag:

- An internal station can, by hanging up, transfer an external call to another external station.
- If an internal station is participating in a conference as the conference leader and hangs up, the other participants can continue the conference.

This setting also applies in restricted operating mode (in the case of WAN failure).

Procedure

Proceed as follows to activate the flag:

1. Select **Stationview** -> **Flags**. The "Station flags" tab applicable to a specific internal station is displayed.
2. In the "Station selection" area, select the internal station you wish to make settings for. The "Station flags" tab applicable to the selected internal station is displayed.
3. "Transit allowed via Hook-on": Activate the checkbox.
4. Click **Apply**. The changes are stored.

4.13.2.1.10 Phone Payload Security

Overview

If TLS is used, the "Payload Security" setting is must be activated for all phones on HiPath 3000.

Procedure

Proceed as follows to activate the flag:

1. Select **Stationview** -> **Activated features**. The "Activated features" tab applicable to a specific internal station is displayed.
2. In the "Station selection" area, select the internal station you wish to make settings for. The "Activated features" tab applicable to the selected internal station is displayed..
3. In the "Payload Security" area, activate the "ON" option.
4. Click **Apply**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.2 Settings in the WBM of the HG 1500

Contents

This section describes the following topics:

- Section 4.13.2.2.1, "Setting the Codec Parameters (T.38 fax, frame size)"
- Section 4.13.2.2.2, "Resetting SIP Parameters"
- Section 4.13.2.2.3, "Adding and Configuring PBX Nodes"
- Section 4.13.2.2.4, "Importing the Certificate for TLS"

4.13.2.2.1 Setting the Codec Parameters (T.38 fax, frame size)

Overview

T.38 fax:

- T.38 fax is not supported in HiPath 3000 V8 MR4 and earlier versions and must be deactivated.
- T.38 fax is supported in HiPath 3000 V8 MR5 and later versions and must be activated.

Frame size:

HiPath Cordless IP and OpenScape Mobile Connect support only a frame size of 20 ms for codec G.711. If the network contains either of these products, the frame size must be set to 20 ms in the WBM of the HG 1500.

Procedure

Proceed as follows to set the codec parameters:

1. Start WBM for HG 1500 (in the Manager E: **Systemview** -> **HG 1500 / Xpress@LAN**).
2. Select the following menu items: **Explorers** -> **Voice Gateway** -> **Codec parameters**.
3. Select **Codec parameters** (right mouse button) -> **Edit codec parameters**. The "Codec Parameters" menu is displayed.
4. Make the settings:
 - G.711 A-law: Select the frame size 20 ms.
 - G.711 μ -law: Select the frame size 20 ms.
 - T.38 fax:
 - HiPath 3000 V8 MR4 and earlier: Deactivate the "T.38 Fax" checkbox.
 - HiPath 3000 V8 MR5 and later: Activate the "T.38 Fax" checkbox.
5. Click **Apply**.

4.13.2.2 Resetting SIP Parameters

Proceed as follows to reset the SIP parameter (condition: WBM is running):

1. Select the following menu items: **Explorers -> Voice Gateway -> SIP Parameters.**
2. Select **SIP Parameters** (right mouse button) -> **Edit SIP Parameters.** The "SIP Parameters" menu is displayed.
3. Reset the SIP parameters to the default settings. These are:
 - SIP Transport Protocol
 - SIP via TCP: Yes
 - SIP via UDP: Yes
 - SIP via TLS: Yes
 - SIP session timer
 - RFC 4028 support: Yes
 - Session-Expires (sec): 1800
 - Minimal-SE (sec): 90
 - Provider calls
 - Maximum number of calls possible via the provider: 0
4. Click **Apply.**
5. Click the diskette icon. The changes are stored.
6. Click the reset icon. HG 1500 is shut down and restarted.
7. Once HG 1500 is ready for operation again, quit WBM and restart.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.2.2.3 Adding and Configuring PBX Nodes

Networking Scenarios

All IP addresses that communicate with HiPath 3000 must be configured as separate PBX nodes. If HiPath 3000 is networked with OpenScape Voice, multiple networking scenarios are available because of the different variants of OpenScape Voice.

Networking scenarios for OpenScape Voice V4 R0 and earlier:

- Scenario 1: OpenScape Voice – Networking with HiPath 3000 with TCP. The following IP addresses must be configured as separate PBX nodes:
 - IP address of sipsm1 for node 1
 - IP address of sipsm1backup (sipsm1_vip2) for node 1
 - IP address of sipsm2 for node 2
 - IP address of sipsm2backup (sipsm2_vip2) for node 2
 - IP address of proxy server if HiPath 3000 is registered via a proxy server.
- Scenario 2: OpenScape Voice – Networking with HiPath 3000 with TLS. The following IP addresses must be configured as separate PBX nodes:
 - IP address of sipsm3 for node 1
 - IP address of sipsm3backup (sipsm3_vip2) for node 1
 - IP address of sipsm4 for node 2
 - IP address of sipsm4backup (sipsm4_vip2) for node 2
 - IP address of proxy server if HiPath 3000 is registered via a proxy server.

Networking scenario for OpenScape Voice V4 R1 and later:

The following IP addresses must be configured as separate PBX nodes:

- IP address of sipsm1 for node 1
- IP address of sipsm2 for node 2
- IP address of sipsm3 for node 1
- IP address of sipsm4 for node 2
- IP address of proxy server if HiPath 3000 is registered via a proxy server.

Procedure

Adding PBX nodes:

Proceed as follows to add a PBX node:

1. Start WBM for HG 1500 (in the Manager E: **Systemview -> HG 1500 / Xpress@LAN**).
2. Select the following menu items: **Explorers -> Voice Gateway -> PBX -> Nodes**.
3. Adding PBX nodes:
 - a) Select **Nodes** (right mouse button) -> **Add PBX Node**. The "Add PBX Node" menu is displayed.
 - b) Enter the node number.
 - c) Click **Apply**.

Configuring PBX nodes:

Proceed as follows to configure the added PBX node:

1. Start WBM for HG 1500 (in the Manager E: **Systemview -> HG 1500 / Xpress@LAN**).
2. Select the following menu items: **Explorers -> Voice Gateway -> PBX -> Nodes -> <Node number of the added PBX node>**.
3. Configuring PBX nodes:
 - a) Select **<Node number of the added PBX node>** (right mouse button) -> **Edit IP Addresses**. The "PBX Node / IP Addresses" menu is displayed.
 - b) Make the following settings:
 - LAN trunking protocol: **SIP-Q**
 - LAN trunking type: **Ext . SIP**
 - HXG Gatekeeper Board 1 - IP Address: Enter the IP address of the SIP Signaling Manager (SIPSM) of OpenScape Voice, see Section "Networking Scenarios".
 - Alive Monitoring: Deactivate the checkbox
 - Security Level of Node Encryption:
in TCP networking: **traditional**
in TLS networking: **secure**
 - c) Click **Apply**.
4. Click the diskette icon. The changes are stored.
5. Click the reset icon. HG 1500 is shut down and restarted.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

- Once HG 1500 is ready for operation again, quit WBM and restart.



Important: For OpenScape Voice, no phone numbers need to be configured in WBM under **Explorers -> Voice Gateway -> PBX -> Routing**.

4.13.2.2.4 Importing the Certificate for TLS

Overview

For signaling and payload encryption via TLS, certificates must be imported in HG 1500. This pertains to the following certificates:

- rootcert.pem:** This certificate must be generated from the root.pem certificate. This certificate is located under: `/usr/local/ssl/certs/root.pem`.
- client.pem:** This certificate is located in OpenScape Voice under `/usr/local/ssl/private/client.pem`.

Procedure

Generate certificate `rootcert.pem`:

Proceed as follows to generate the certificate:

- Copy the `/usr/local/ssl/certs/root.pem` certificate and rename to the copy to `rootcert.pem`.
- Open the certificate with an editor and delete the RSA PRIVATE KEY out of the certificate. The text begins with `BEGIN RSA PRIVATE KEY` and ends with `END RSA PRIVATE KEY`.
- Store the changes.

Importing the `rootcert.pem` certificate:

Proceed as follows to import the certificate:

- Start WBM for HG 1500 (in the Manager E: **Systemview -> HG 1500 / Xpress@LAN**).
- Select the following menu items: **Explorers -> Security -> Signaling and Payload Encryption (SPE) -> SPE CA Certificates** .
- Select **SPE CA Certificates** (right mouse button) -> **Import trusted CA Certificate (PEM or binary format)** . The "Load an SPE CA Certificate via HTTP" menu is displayed.
- Click on the **Browse** button and select the `rootcert.pem` certificate.
- Click **View Fingerprint of Certificate**. The finger print of the certificate is displayed.
- Check whether the finger print of the certificate matches the expected finger print. Then click **OK**.

7. If they match: Click **Import Certificate from File**. A message indicating that the action was successful is displayed.

Importing the `client.pem` certificate:

Proceed as follows to import the certificate:

1. Start WBM for HG 1500 (in the Manager E: **Systemview -> HG 1500 / Xpress@LAN**).
2. Select the following menu items: **Explorers -> Security -> Signaling and Payload Encryption (SPE) -> SPE Certificate** .
3. Select **SPE Certificate** (right mouse button) -> **Import SPE certificate plus private key (PEM or PKCS#12)** . The "Load a SPE Key Certificate via HTTP" menu is displayed.
4. Click the **Browse** button and select the `client.pem` certificate.
5. Click the **View Fingerprint of Certificate** button. The finger print of the certificate is displayed.
6. Check whether the finger print of the certificate matches the expected finger print. Then click **OK**.
7. If they match: Click **Import Certificate from File**. A message indicating that the action was successful is displayed.

HG 1500 is shut down automatically and restarted. This activates the imported certificate.

Deactivating the "Subject name check" security setting:

Proceed as follows to check this setting:

1. Start WBM for HG 1500 (in the Manager E: **Systemview -> HG 1500 / Xpress@LAN**).
2. Select the following menu items: **Explorers -> Security -> Signaling and Payload Encryption (SPE)** .
3. Select **Signaling and Payload Encryption (SPE)** (right mouse button) -> **Edit Security Configuration**. The "Edit SPE Security Setup" menu is displayed.
4. Check whether the **Subject name check** checkbox is deactivated. If not, deactivate it.
5. After a change is made: Click **Apply**. The change is stored.

4.13.3 Configuring OpenScape Voice

Overview

HiPath 3000 as a gateway (endpoint) and OpenScape Voice stations must be in separate private numbering plans but in the same business group. Thus, each location receives a separate private numbering plan for the stations and a separate private numbering plan for the gateways (endpoints).

Settings must be made in the Common Management Portal and in StartCli to configure OpenScape Voice.

Contents

This section describes the following topics:

- Section 4.13.3.1, "Settings in the Common Management Portal"
- Section 4.13.3.2, "Settings in StartCli"

4.13.3.1 Settings in the Common Management Portal

Procedure

1. Start the Common Management Portal.
2. Work through the following sections in sequence.

Contents

This section describes the following topics:

- Section 4.13.3.1.1, "Creating a New, Private Numbering Plan for the Gateways"
- Section 4.13.3.1.2, "Creating and Configuring the Endpoint Profile for a HiPath 3000 Endpoint"
- Section 4.13.3.1.3, "Creating and Configuring the Endpoint for HiPath 3000"
- Section 4.13.3.1.4, "Creating a Digest Authentication for HiPath 3000"
- Section 4.13.3.1.5, "Configuring a Gateway Numbering Plan for Incoming Calls"
- Section 4.13.3.1.6, "Configuring Outgoing Calls"
- Section 4.13.3.1.7, "Changing the Display Number for OpenScape Voice V5"

4.13.3.1.1 Creating a New, Private Numbering Plan for the Gateways

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - a) Available Switches: Select **OpenScape Voice**.
 - b) Available Business Groups: Select the business group for which the new private numbering plan is to be created, e.g. **bg_so1**.
3. In the left window area, select **Private Numbering Plans**. The right window area shows a list of all private numbering plans.
4. To create a new private numbering plan, click the **Add** button. The configuration window is displayed.
5. In the "Name:" entry field, enter the name of the private numbering plan to be created, e.g. **NP_br13_gw**.
6. Click **Save**. The changes are stored.

4.13.3.1.2 Creating and Configuring the Endpoint Profile for a HiPath 3000 Endpoint

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - a) Available Switches: Select **OpenScape Voice**.
 - b) Available Business Groups: Select the business group for which the endpoint profile is to be created, e.g. **bg_so1**.
3. In the left window area, select **Profiles** -> **Endpoint Profiles**. The right window area shows a list of the endpoint profiles.
4. To create a new endpoint profile, click the **Add** button. The configuration window for this endpoint profile is displayed.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

5. Open the **General** tab. Make the following settings on this tab:

Endpoint Profile:

- Name: Enter a name for the endpoint profile, e.g. **EP_hg1500.br13**.
- Numbering Plan: Select the numbering plan for the endpoint profile, e.g. **NP_br13_gw**.

Management Information:

- Class of Service: No setting necessary.
- Routing Area: No setting necessary.
- Calling Location: No setting necessary.
- SIP Privacy Support: **Basic**
- Failed Calls Intercept: **Disabled**
- Language: e.g. **German**

6. Open the **Services** tab. Make the following settings on this tab:

[OpenScape Voice V4 R1 and earlier:](#)

Make the following settings on the "Services" tab:

General:

- Name delivery: **Yes**
- Voice mail: **Yes**
- Called name delivery: **Yes**
- Called number delivery: **Yes**
- Call transfer: **No**
- Call Forward Invalid Destination: **Yes** and enter the phone number.

Toll and Call Restrictions:

- International World Zone 1: **No**
- International: **No**
- National: **No**
- Local: **No**

[OpenScape Voice V5 R0 and later:](#)

Make the following settings on the "Services" tab:

- Voice mail: **Yes**
 - Call Transfer: **No**
 - Call Forward Invalid Destination: **Yes** and enter the phone number.
 - Toll and Call Restrictions: **No**
7. Click **OK**. The changes are stored. The endpoint profile is created and configured. The new endpoint profile in the table on the right side of the window (<Nodes> - Endpoint Profiles - **bg_sol**) now looks similar to the following example:

Name	Class of Service	Routing Area	Calling Location	Remark	Numbering Plan Name
EP_hg1500.br13	international	-	-	no	NP_br13_gw

4.13.3.1.3 Creating and Configuring the Endpoint for HiPath 3000

Proceed as follows:

1. Select **OpenScape Voice -> Business Group**.
2. Select the following in the left window area:
 - a) Available Switches: Select **OpenScape Voice**.
 - b) Available Business Groups: Select the business group for which the endpoint is to be created, e.g. **bg_sol**.
 - c) Available Branch Offices: Select the branch office for which the endpoint is to be created, e.g. **BR13**.
3. In the left window area, select **Members -> Endpoints**. The list of endpoints is displayed.
4. To create a new endpoint, click the **Add** button. The configuration window for this endpoint is displayed.
5. Open the **General** tab. Make the following settings on this tab:
 - Name: Enter a name for the endpoint, e.g. **EP_hg1500.br13**.
 - Profile: Select the endpoint profile that was selected in the previous step, e.g. **EP_hg1500.br13**.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

6. Open the **SIP** tab. Make the following settings on this tab:
 - a) SIP-Q Signaling: Activate the option field.
 - b) for: Select **HiPath 4000/3000**.
 - c) Transport protocol:
 - For a traditional network: Select **TCP**.
 - For a secure network: Select **MTLS**.
7. Open the **Attributes** tab. Make the following settings on this tab:
 - a) Activate the "Rerouting Forwarded Calls" checkbox.
 - b) Deactivate all other checkboxes.
8. Open the **Aliases** tab. Make the following settings on this tab:
 - a) Click **Add** and enter the registration number for HiPath 3000, e.g. **13310**.
 - b) Click **Add** and enter the IP address of HG 1500, e.g. **10.22.113.191**.
9. Open the **Accounting** tab. Make the following settings on this tab:
 - Accounting Type: **PSTN Gateway**
 - Endpoint Location Name: No setting necessary.
 - Endpoint Location Code: No setting necessary.
 - Endpoint Service Provider: No setting necessary.
10. Click **Save**. The changes are stored.

The endpoint is created and configured.

4.13.3.1.4 Creating a Digest Authentication for HiPath 3000

Proceed as follows:

1. Select **OpenScape Voice -> Administration**.
2. In the left window area, select **Signaling Management -> Digest Authentication** . The "Digest Authentication" window opens.
3. Open the **Realms** tab.
4. To create "Digest Authentication" access, click the **Add** button. The "SIP Configuration" window opens.
5. Make the following settings:
 - Trusted entity: Deactivate the checkbox.
 - Signaling IP: Enter the IP address of the HG 1500, e.g. **10.22.113.191**.
 - All Ports: Do not activate the option field.
 - Port Range: The option field can be neither activated nor deactivated.
 - *Local Realm*: Enter the local realm, e.g. **so1**.
 - Local User Name: Enter the local user name, e.g. **hipath3000br13**.
 - Local Password: Enter the local password.
 - Confirm Local Password: Enter the local password once more.
 - *Remote Realm*: Enter the realm of the branch office, e.g. **so1**.
 - Remote User Name: Enter the user name for the branch office, e.g. **hipath3000br13**.
 - Remote Password: Enter the password for the branch office.
 - Confirm Remote Password: Enter the password for the branch office once more.
6. Click **OK**. The "SIP Configuration" window is closed.
7. Click **Save**. The changes are stored and the "Digest Authentication" window is closed.

4.13.3.1.5 Configuring a Gateway Numbering Plan for Incoming Calls



Important: This is a simple example of how to configure the routing of incoming calls. A detailed description is contained in the routing concept under "Reference Architecture".

This section describes how to configure destination codes for incoming calls. These destination codes are required for forwarding incoming calls.

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group for which the destination code is to be configured, e.g. **bg_so1**.
 - Available Private Numbering Plan: Select the private numbering plan for which the destination code is to be configured.
3. In the left window area, select **Translation** -> **Destination Codes**.
4. To create a new destination code, click the **Add** button. The "Add Destination Code" window opens.
5. Create a new E.164 destination code with the following parameters:
 - Destination Code: z.B. **49695113**
 - Nature of Address: **International**
 - Destination Type: **Home**
 - Office Code: e.g. **+49 (69) 5113**
6. Click **Save**. The changes are stored and the "Add Destination Code" window is closed.

4.13.3.1.6 Configuring Outgoing Calls



Important: This is a simple example of how to configure the routing of outgoing calls. A detailed description is contained in the routing concept under "Reference Architecture".

Station numbering plan – Prefix Access Codes

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group for which the prefix access codes are to be configured, e.g. **bg_sol**.
 - Available Private Numbering Plan: Select the private numbering plan in which the station is located.
3. In the left window area, select **Translation** -> **Prefix Access Codes**.
4. To create a new prefix access code, click the **Add** button. The "Add Prefix Access Code" window opens.
5. Make the following settings in the configuration window:
 - Prefix Access Code: e.g. **0**
 - Minimum Length: e.g. **1**
 - Maximum Length: e.g. **30**
 - Digit Position: e.g. **1**
 - Digits to insert: e.g. **4969**
 - Prefix Type: e.g. **On-net Access**
 - Nature of Address: e.g. **International**
 - Destination Type: e.g. **BG Common Destination**
 - Destination Name: No settings necessary.
6. Click **Save**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

General numbering plan – Destinations

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group for which the destinations are to be configured, e.g. **bg_so1**.
 - Available Private Numbering Plan: Select the general numbering plan.
3. In the left window area, select **Destination and Routes** -> **Destinations**.
4. To create a new destination, click the **Add** button. The "Add Destination" window is displayed. Proceed as follows in this window:
 - a) Open the **General** tab.
 - b) Enter the name of the destination in the "Name" entry field, e.g. **c.hg1500.br13**
 - c) Click **Save**. The changes are stored and the "Add Destination" window is closed.
5. Open the new destination for editing. The "Edit Destination" window is displayed. Proceed as follows in this window to create an endpoint:
 - a) Open the **Routes** tab.
 1. Click the **Add** button.
 2. Make the following settings:
 - ID: e.g. **100**
 - Type: **SIP Endpoint**
 - SIP Endpoint: e.g. **hg1500.br13**
 - Nature of Address: **Undefined**
 3. Click **Save**. The changes are stored.
 - b) Open the **Route Lists** tab. Proceed as follows on this tab:
 1. Make the following settings:
 - Prioritized: Activate the checkbox.
 - Fallback to Local Numbering Plan: Leave the checkbox deactivated.
 2. Click **Save**. The changes are stored.

On the **Routes** tab, use the **Add** button to add another endpoint as a fallback in case HiPath 3000 fails.

General numbering plan – Prefix Access Codes

Proceed as follows:

1. Select **OpenScape Voice -> Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group for which the prefix access codes are to be configured, e.g. **bg_sol**.
 - Available Private Numbering Plan: Select the general numbering plan.
3. In the left window area, select **Translation -> Prefix Access Codes**.
4. To create a new prefix access code, click the **Add** button. The "Add Prefix Access Code" window opens.
5. Make the following settings in the configuration window:
 - Prefix Access Code: e.g. **4**
 - Minimum Length: **1**
 - Maximum Length: **30**
 - Digit Position: **0**
 - Digits to insert: Leave this entry field empty.
 - Prefix Type: **On-net Access**
 - Nature of Address: **International**
 - Destination Type: **None**
 - Destination Name: No settings necessary.
6. Click **Save**. The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

General numbering plan – Destination Codes

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group for which the destination code is to be configured, e.g. **bg_sol**.
 - Available Private Numbering Plan: Select the general numbering plan.
3. In the left window area, select **Translation** -> **Destination Codes**.
4. To create a new destination code, click the **Add** button. The "Add Destination Code" window opens.
5. Make the following settings:
 - Destination Code: e.g. **4969**
 - Nature Of Address: **International**
 - Destination Type: **Destination**
 - Destination Name: Select the previously created destination, e.g. **c.hg1500.br13**.
6. Click **Save**. The changes are stored and the "Add Destination Code" window is closed.

4.13.3.1.7 Changing the Display Number for OpenScape Voice V5

Display Number Definition

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group, e.g. **bg_so1**.
3. In the left window area, select **Display Number Modification** -> **Definitions**.
4. To define a new display number, click the **Add** button. The "Display Number Definition" window opens.
5. Make the following settings:
 - Business Group: Select the business group being used, e.g. **bg_so1**.
 - Numbering Plan: **ANY**
 - Numbering plan indicator: **Public**
 - Country/L2 Code: **49**
 - Area/L1 Code: **69**
 - Local Office/L0 Code: **5113**
 - Number of digits to skip: Enter the number of digits in the station phone numbers, e.g. **4**.
 - Min. Digits: **8**
 - Max. Digits: **30**
6. Click **Save**. The changes are stored and the "Display Number Definition" window is closed.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

Prefixes

Proceed as follows:

1. Select **OpenScape Voice -> Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group, e.g. **bg_sol**.
3. In the left window area, select **Display Number Modification -> Prefixes**.
4. To create a global prefix definition, click the **Add** button. The "Edit Display Number Prefix" window opens.
5. Make the following settings under "Public Prefix Definition":

	Public Network Access Code	Prefix
International	0	00
National	0	0
Subscriber	0	

6. Click **Save**. The changes are stored and the "Edit Display Number Prefix" window is closed.

Modifications – Gateway numbering plan

Proceed as follows:

1. Select **OpenScape Voice -> Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group, e.g. **bg_sol**.
3. In the left window area, select **Display Number Modification -> Modifications**.
4. Click the **Add** button. The "Display Number Modification" window opens.
5. Make the following settings in the "Originating Context Setting" window area:
 - Business Group: **ANY**
 - Numbering Plan: **ANY**

6. Make the following settings in the "Terminating Context Setting" window area:
 - Business Group: Select the business group being used, e.g. **bg_sol**.
 - Numbering Plan: Select the numbering plan of the endpoint, e.g. **NP_br13_gw**.
 - Endpoint: **NONE**
7. Make the following settings in the "Modification Rule" window area:
 - Input Type Of Number: **ANY**
 - Priority: **1**
 - Output Type Of Number: **International**
 - Number Source: **Input Number**
 - Presentation Restricted: Leave the checkbox deactivated.
 - Prefix Required: Leave the checkbox deactivated.
 - Optimize Type Of Number: **None**
8. Click **Save**. The changes are stored and the "Display Number Modification" window is closed.

Modifications – Station numbering plan

Proceed as follows:

1. Select **OpenScape Voice** -> **Business Group**.
2. Select the following in the left window area:
 - Available Switches: Select **OpenScape Voice**.
 - Available Business Groups: Select the business group, e.g. **bg_sol**.
3. In the left window area, select **Display Number Modification** -> **Modifications**.
4. Click the **Add** button. The "Display Number Modification" window opens.
5. Make the following settings in the "Originating Context Setting" window area:
 - Business Group: **ANY**
 - Numbering Plan: **ANY**

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

6. Make the following settings in the "Terminating Context Setting" window area:
 - Business Group: Select the business group being used, e.g. **bg_sol**.
 - Numbering Plan: Select the numbering plan of the endpoint, e.g. **NP_br13_eg**.
 - Endpoint: **NONE**
7. Make the following settings in the "Modification Rule" window area:
 - Input Type Of Number: **ANY**
 - Priority: **4**
 - Output Type Of Number: **ANY**
 - Number Source: **Input Number**
 - Presentation Restricted: Leave the checkbox deactivated.
 - Prefix Required: Activate the checkbox.
 - Optimize Type Of Number: **Extension**
8. Click **Save**. The changes are stored and the "Display Number Modification" window is closed.

4.13.3.2 Settings in StartCli

OpenScape Voice V4 R1 and earlier

Set the CLI parameter `Srx/Main/OutGoingCallingPartyNumberType` to the value **0**. This setting is needed for the phone number of the caller to be sent with the Type of Number "International".

OpenScape Voice V5 R0 and later

The above-mentioned CLI parameter is no longer needed. The phone number of the caller is set under "Display Number Modification".

4.13.4 Configuring OpenScape Branch



Important: This section only contains certain specific information on HiPath 3000. Detailed information on OpenScape Branch can be found in the Administrator Documentation found on SEN E-Docu.

Procedure

1. Start the Common Management Portal.
2. Work through the following sections in sequence.

Contents

This section describes the following topics:

- Section 4.13.4.1, "Network Services"
- Section 4.13.4.2, "VoIP"

4.13.4.1 Network Services

Proceed as follows:

1. Select **OpenScape Branch -> Network Services**.
2. Make the settings described in the following sections:
 - Section 4.13.4.1.1, "Interface 1"
 - Section 4.13.4.1.2, "Routing"
 - Section 4.13.4.1.3, "NTP"
 - Section 4.13.4.1.4, "DNS Server"
 - Section 4.13.4.1.5, "DNS Client"
 - Section 4.13.4.1.6, "DHCP"
3. After working through a section: Click **Save and Commit** . The changes are stored.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.4.1.1 Interface 1

In this area, enter the following values for the OpenScape Branch proxy server :

- IP address: e.g. **10.22.113.10**
- Subnet mask: e.g. **255.255.255.0**

Continue with the next section.

4.13.4.1.2 Routing

In this area, enter the following value for the IP address of the default gateway:

- Default gateway address: e.g. **10.22.113.254**

Continue with the next section.

4.13.4.1.3 NTP

Make the following settings in this area:

- Timezone: e.g. **GMT+1:00**
- Enable local NTP server: Activate the checkbox.
- Synchronize with NTP server: Select the option field.
- NTP server: Enter the IP address of the NTP server, e.g. **10.21.255.7**.
- Synchronize now: Click the button.

Continue with the next section.

4.13.4.1.4 DNS Server

Make the following settings in this area:

- OpenScape Branch domain name: Enter the "DNS-SRV" name of the branch office (**Domain Name System SERVICE**), e.g. **br13.sol.de**
- Enable DNS server: Activate the checkbox.
- DNS configuration: Click the button; for more, see "DNS Configuration".

DNS Configuration

Settings

Complete the "Zone configuration" table as shown in the following example:

Row	Type	Zone name	IP Master/Forward	File name
1	slave	so1.de	10.22.100.100	so1.de

Procedure

Proceed as follows:

1. Complete the table as follows:
 - a) Click **Add** to insert a row in the table.
 - b) Complete the row; see "Settings".
2. Click **Save**. The changes are stored.

Forward IP

The IP address of the customer DNS server must be entered in the "Forward IP Address list". The customer DNS server is required for queries outside of the transmitted zone. Proceed as follows:

1. Enter the customer DNS server IP address in the entry field, e.g. **10.22.100.100** and then click **Add**. The IP address is added to the "Forward IP Address list".
2. Click **Save**. The changes are stored.

Continue with the next section.

4.13.4.1.5 DNS Client

Enter the IP address of the customer DNS server in the "DNS server list". Proceed as follows:

1. Enter the customer DNS server IP address in the entry field, e.g. **10.22.100.100** and then click **Add**. The IP address is added to the "DNS server list".
2. No further IP addresses need to be added.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.4.1.6 DHCP

Make the following settings in this area:

- Enable DHCP server: Activate the checkbox.
- DHCP configuration: Click the button; for more, see "DHCP Configuration".

DHCP Configuration

Most important setting

In the "DNS server list" of the "DHCP Server" window, the IP addresses of the OpenScape Branch proxy server and customer DNS server must be specified. Proceed as follows:

1. Enter the IP address of the OpenScape Branch proxy server in the entry field, e.g. **10.22.113.10** and then click **Add**. The IP address is added to the "DNS server list".
2. Enter the customer DNS server IP address in the entry field, e.g. **10.22.100.100** and then click **Add**. The IP address is added to the "DNS server list".

Additional settings

Make the following settings in the "DHCP Server" window:

- Subnet: e.g. **10.22.113.0**
- Netmask: e.g. **255.255.255.0**
- IP address from: e.g. **10.22.113.100**, to: e.g. **10.22.113.129**
- Static IP address list configuration: Do not click the button.
- Lease time: e.g. **86400**
- Max lease time: e.g. **604800**
- Interface: e.g. **Interface 1**
- Update style: e.g. **None**
- Broadcast address: e.g. **10.22.113.255**
- Domain name: "DNS-SRV" name of the branch office (**Domain Name System SERVICE**)
e.g. **br13.sol.de**
- DLS server: Enter the IP address of the DLS server, e.g. **10.22.100.101**.
- DLS port: Enter the port for the DLS server, e.g. **18443**.
- Routers: e.g. **10.22.113.254**

Return to Section 4.13.4.1, "Network Services".

4.13.4.2 VoIP

Proceed as follows:

1. Select **OpenScape Branch** -> **VOIP**.
2. Make the settings described in the following sections:
 - Section 4.13.4.2.1, "SIP Configuration"
 - Section 4.13.4.2.2, "SIP Manipulation"
 - Section 4.13.4.2.3, "Gateways/Trunks"
 - Section 4.13.4.2.4, "QoS"
 - Section 4.13.4.2.5, "Codecs"
3. After working through a section: Click **Save and Commit** . The changes are stored.

4.13.4.2.1 SIP Configuration

The SIP connection to OpenScape Voice is only briefly described in this section by way of example. Detailed information on this topic can be found under "How to Configure the Communication System" in the OpenScape Branch Administrator Documentation.



Important: The settings in this section refer to the settings in Section 4.13.2.1.5, "Network -> Ext. SIP", executed in Manager E.

Make the following settings in this area:

- OpenScape Branch mode: e.g. **Proxy**
- OpenScape Voice mode: e.g. **Simplex**
- Options destination port: **5060**
- SIP listening ports:
 - TCP: **5060**
 - UDP: **5060**
 - TLS: **5061**
- Node 1:
 - Target type: **SRV Record**
 - Primary server: e.g. **10.22.14.24**, Transport: **TCP**, Port: e.g. **5060**
 - Backup server: e.g. **10.22.14.25**, Transport: **TCP**, Port: e.g. **5060**
 - SRV record, Transport: No settings necessary.

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

- Node 2:
 - Target type: **Binding**
 - Primary server: e.g. **10.22.15.24**, Transport: **TCP**, Port: e.g. **5060**
 - Backup server: e.g. **10.22.15.25**, Transport: **TCP**, Port: e.g. **5060**
 - SRV record, Transport: No settings necessary.
- Outbound SIP Server: **Node 1**
- Enable Far End NAT: Leave the checkbox deactivated.
- Other Trusted Servers: No settings necessary.
- Error codes: No settings necessary.
- SIP Manipulation: Click the button; for more, see "SIP Manipulation".
- SIP routing: No settings necessary.

Return to Section 4.13.4.2, "VoIP".

4.13.4.2.2 SIP Manipulation

Settings

The settings in the "SIP Manipulation provisioning" table are required for emergency handling. Complete the table as follows:

Row	Match digits	Match position	Header	Delete/in-insert position	Number of digits to delete	Insert digits	Add prefix	Replace all with	Call type
1	4	0	From				+		All
2	+	0	R-URI		1				All
3	1	0	R-URI				e.g. 49695113		All
4	2	0	R-URI				e.g. 49695113		All
5	3	0	R-URI				e.g. 49695113		All

Explanations:

- First row: The phone number must have a plus "+" at the beginning so HiPath 3000 can recognize this as an international phone number.
- Second row: The plus "+" in the Request-URI (R-URI) must be deleted, as SIP telephones of OpenScape Voice are not registered with a plus "+".
- Third to fifth rows: These settings enable SIP telephones to dial a short internal number and not international dialing.

Procedure

Proceed as follows to configure the SIP header:

1. Complete the "SIP Manipulation" table as follows:
 - a) Click **Add** to insert a row in the table.
 - b) Complete the row; see "Settings".
 - c) For the next row begin with step a.
2. Click **Save**. The changes are stored.

Return to Section 4.13.4.2, "VoIP".

4.13.4.2.3 Gateways/Trunks

Add HG 1500 as a gateway.

Settings

Complete the "Gateways/Trunks provisioning" table as follows:

Row	IP Address or FQDN	Port	Interface	Transport	Routing prefix/FQDN	Gateway/Trunk type	Functional type	Trunk Profile	Output digit strip	Output digit add	Priority
1	e.g. 10.22.113.191	e.g. 5060	LAN	TCP	%	3k/4k	All modes Egress/Ingress	Gateway	0		1

The entries in this table are examples. Detailed information can be found under "Configuration of Gateways" in the Administrator Documentation of OpenScape Branch.

Procedure

Proceed as follows in the Gateways/Trunks area:

1. Activate the "Enable Gateways/Trunks" checkbox.
2. Click the **Gateways/Trunks configuration** button. The "Gateways/Trunks provisioning" table is displayed.
3. To add the HG 1500 as a gateway, complete the table as follows:
 - a) Click **Add** to insert a row in the table.
 - b) Complete the row; see "Settings".
4. Click **Save**. The changes are stored.

Return to Section 4.13.4.2, "VoIP".

Networking Scenarios for HiPath 3000/5000 V8

Networking of HiPath 3000 with OpenScape Voice via SIP-Q V2

4.13.4.2.4 QoS

Set the Layer 3 priority for QoS (Quality of Service).

Settings

Complete the "QoS provisioning" table as follows, for example:

Row	Protocol	In Interface	Out Interface	Port	DSCP	Mark
1	UDP	a11	a11	5060	26	
2	TCP	a11	a11	5060	26	

Procedure

Proceed as follows in the QoS area:

1. Activate the "Enable QoS" checkbox.
2. Click the **QoS configuration** button. The "QoS" window is displayed.
3. Complete the entry fields as follows:
 - DSCP for SIP: **26** (for L3 QoS Priority Diffserv AF31)
 - DSCP for RTP: **46** (for L3 QoS Priority Diffserv EF)
4. Complete the table as follows:
 - a) Click **Add** to insert a row in the table.
 - b) Complete the row; see "Settings".
5. Click **Save**. The changes are stored.

Return to Section 4.13.4.2, "VoIP".

4.13.4.2.5 Codecs

The codec priority is set up as for the HG 1500.

Settings

Complete the "Codecs" table as shown in the following example:

Priority	Codec
1	G711A
2	G711U

Procedure

Proceed as follows in the "Codecs" area:

1. Complete the table as follows:
 - a) Click **Add** to insert a row in the table.
 - b) Complete the row; see "Settings".
2. Click **Save**. The changes are stored.

Return to Section 4.13.4.2, "VoIP".

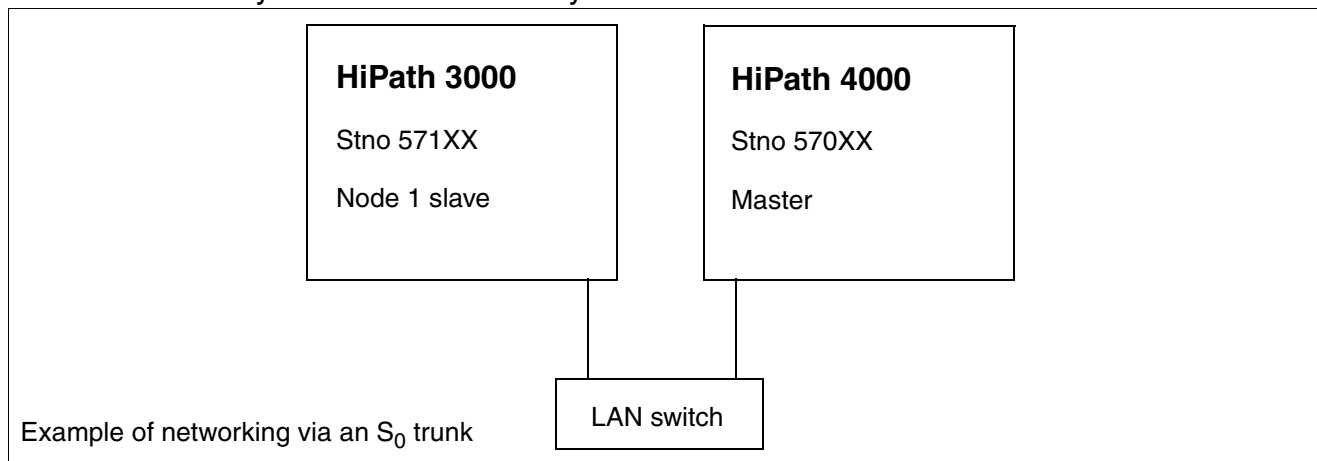
Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with External Systems via ISO-QSIG or ECMA-QSIG

4.14 Networking HiPath 3000 V9 with External Systems via ISO-QSIG or ECMA-QSIG

4.14.1 Target Configuration

The target configuration involves using ISO-QSIG or ECMA-QSIG to establish a network in a HiPath 3000 V8 system to an external system.



4.14.2 Configuring HiPath 3000 Node1

Setup is performed via Manager E.

Add trunks

1. Start HiPath 3000 Manager E and read the customer database (CDB).
2. Select "Lines/networking > Trunks".
3. Double-click the parameter field once in the row containing the required STLS or STMD trunk.
4. Select the protocol in the pop-up window under "ISDN flags > Protocol: Description" (e.g., S0: ISO-QSIG Slave CR=2 CHI=S2 (Standard)); the protocol applies at all times to the port; in other words, there are always two trunk assigned to an S0 port.
5. Click Apply.
6. Click Close.
7. Select a free route in the row containing the required STLS or STMD trunk (e.g., Trk Grp 2).
8. Assign the same route (e.g., Trk Grp 2) to the second trunk associated with the S0 port.
9. Click Apply.

Configure routes

1. Select "Lines/networking > Routes".
2. Under Routes: Click the selected route (e.g., Trk Grp 2).
3. Enter the route name (e.g., Tie).
4. Enter the 2nd trunk code (e.g., 0) for the missed calls list.
5. If a routing prefix is set, delete it.
6. Click Apply.

Configure routing parameters

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number (e.g., 1).
3. Click Apply.

Configure QSIG features

1. Select "Lines/networking > QSIG features > Own system data".
2. Enter the system number (e.g., 1).
3. Click Apply.

Configure LCR

1. Select "Least cost routing > Codes and flags".
2. Select "Activate LCR".
3. Click Apply.

Configuring least cost routing

1. Select "Least cost routing > Dial plan > Dialed digits".
2. Enter the subscriber numbers for the external system, for example, -570XX.
3. Assign a route table to the station number (e.g., route table 2).
4. Select the chosen route (e.g., Trk Grp 2) for the route table.
5. Assign a dial rule to the route (e.g., dial rule 2).
6. Select "Corporate network" as the network provider's method for dial rule 2 in the Dial rule wizard.

Networking Scenarios for HiPath 3000/5000 V8

Networking HiPath 3000 V9 with External Systems via ISO-QSIG or ECMA-QSIG

7. Enter "E1A" as the dial rule format.
8. Click Apply.
9. Transfer the CDB to HiPath 3000 (delta mode possible).

4.15 Information on Configuring Networking Routes

The following section focuses on modified or new parameters in V7. Parameters not covered here have not changed since V4.0, 5.0, and 6.0.

4.15.1 ISDN Numbering Plan

In the version 7 or higher, ISDN numbering plan is no longer set for E.164 networks under Lines/networking > Special > Numbering plan.

4.15.2 E.164 Network

"System check" is set under "Numbering plan" and "All others" for E.164 networks in version 7 and higher. The advantage of an E.164 network with the same format as the ISDN numbering plan is that the same station number is dialed in both the network and the public network. This also means that internal extensions can be assigned more than once in the network.

Prerequisite

All ISDN ports should support the feature "CLIP no screening". This feature is provider-dependent and subject to a charge.

In a nutshell:

The called party number and calling party number are transmitted in international format in an E.164 network.

The type of number (TON) is set via the dial rule in the LCR system in an E.164 network. "Country code" should generally be selected here.

4.15.3 Configuration via Manager E

Enable E.164 numbering

Select "System parameters > Flags > E.164 numbering scheme".
This sends the internal extension as a long-format station number (international).

Configure routes

Select "Lines/networking > Routes > PABX number-incoming".
In a typical network with E.164 (ISDN) numbering plan, the called party number is based on the ISDN station number + the extension. To reach a DID destination, the complete international station number of the individual location must always be configured in the PBX route. This station number is generally identical to the location number.

Networking Scenarios for HiPath 3000/5000 V8

Information on Configuring Networking Routes

The "PABX number-outgoing" only has to be configured if it differs from the "PABX number-incoming".

Configure routing parameters

1. Select "Lines/networking > Routing parameters".
2. Add direction prefix incoming: = leave active (important for IVM and E.164 networking).
3. Add direction prefix outgoing: = leave active.
4. No. and type, outgoing: The "Type of Number" for the "Calling Party Number" is set here. As a rule, "Country code" should always be set here.
5. Callnumber typ: "Internal / DID" should generally be set here. If you only want to the DID number to be transferred, select the "DID" option.

Configure special networking

1. Select "Lines/networking > Special".
2. Called Party Number: leave the "System check" setting.
3. All others: leave the "System check" setting.

Note

If a node does not have a local trunk access, the "incoming" and, where applicable, "outgoing" PABX numbers are configured with appropriate entries (customer's CO number) in the networking route. The "Location number current" flag is also set for this route.

4.16 Information on the Rerouting Parameter and Path Optimization Flag

The following table shows the settings to be made, depending on the networking scenario.

Networking scenario	HiPath 3000/5000 Manager E: Settings > Lines / networking... > Routing parameters > Rerouting		HiPath 3000/5000 Manager E: System parameters... > Flags > Path optimization
	TDM	IP	
HiPath 3000–TDM–HiPath 3000	active	not relevant	active
HiPath 3000–TDM–HiPath 3000–IP– HiPath 3000	not active	not active	active
HiPath 3000–IP–HiPath 3000	not relevant	not active	active
HiPath 3000–IP–HiPath 3000–TDM– Xpressions	not active	not active	active
HiPath 3000–TDM–HiPath 4000	active	not relevant	active
n times HiPath 3000–IP–HiPath 4000 with DMC	not relevant	not active	not active
n times HiPath 3000–IP–HiPath 4000 without DMC	not relevant	off / not ac- tive	active
HiPath 3000–TDM–HiPath 3000–IP– HiPath 4000	not active	not active	active (HiPath 4000 without DMC) not active (HiPath 4000 with DMC)
HiPath 3000–IP–HiPath 3000–TDM– HiPath 4000	not active	not active	
Xpressions–TDM–HiPath 3000–IP– HiPath 4000	not active	not active	
HiPath 3000–IP–HiPath 4000–TDM– Xpressions	not active	not active	
HiPath 3000–IP–HiPath 4000–TDM– HiPath 3000	not active	not active	
HiPath 5000 RSM–IP–HiPath 3000– TDM–HiPath 4000	not active	not active	

4.17 Least Cost Routing (LCR) for E.164

Overview

Least cost routing enables HiPath 3000 to control via which route an outgoing external connection is to be switched. The calls may be routed via the public network, various network providers (ISPs) or via a private network. With the proper configuration, this allows the most cost-effective ISP to be used in individual cases, depending on the dialed number (LCR dial plan) and the current time (LCR schedule).

All call numbers and codes leaving the system must be entered in the LCR dial plan (this includes stations of networked systems, for example, as well as CO codes in a single system and possibly CO codes in the remote system).

Simplified dialing (prime line) cannot be used when Least Cost Routing is enabled.

General Operating Principle

HiPath 3000 analyses the call number dialed from the station to determine whether the entered digits are valid. If the digits are recognized, the associated route table is examined to determine the available connection paths. As soon as the connection path is selected, the availability of the connection is determined on the basis of the schedule. If the connection path is also available at the required time, the LCR class of service assigned to this route is compared with the LCR class of service of the station. If the LCR class of service assigned to the station is greater than or equal to that of the connection path, the corresponding route can be seized. After this, the direct trunk access tables (allowed or denied lists) are checked to determine whether dialing the call number is allowed for the station. If this is the case, the connection is set up.

4.17.1 Setting up Least Cost Routing



Important:

- When configuring a HiPath 3000 system for E.164, at least the following dial plans must be set up:
 - Dial plan 0CZ with outdial rule A
 - Dial plan 0C00<country_code>Z, with outdial rule E3A (e.g., 0C0049Z)
- For the sake of simplicity, these requirements were not taken into account in this configuration example. The configuration example is not binding and must be adapted to the prevailing conditions.

This example is based on setting up Least Cost Routing in three levels.

- Section 4.17.1.1, "Basic LCR"
- Section 4.17.1.2, "Extension Through a Time-dependent Component (Schedule)"
- Section 4.17.1.3, "Extension of Least Cost Routing Through LCR Classes of Service"

4.17.1.1 Basic LCR

Different network providers (ISPs) are to be used for external calls, depending on the call number and time of the call.

- The digit transmission is to occur on a digit-by-digit basis.
- Dialing rules must be set up for the following ISPs:
 - Deutsche Telekom (main network supplier)
 - 01070 (Arcor Call by Call)
 - 01078 (3U Call by Call)
 - 01081 (01081 Telecom Call by Call)

For the ISP 01078, rerouting is to be set in the route table for all busy states reported by the ISP.

- Local calls, national calls and international calls are to be routed via the following ISPs:
 - Local calls: always via Deutsche Telekom
 - National calls:
 - First priority via 01078
 - Second priority via 01070
 - Last route via Deutsche Telekom (with display and warning tone)

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

- International calls:
 - First priority via 01081
 - Second priority via 01078
 - Last route via Deutsche Telekom (with display and warning tone)

For testing purposes, the display of the dialing rule name can be set up for all call by call ISPs.

A Fax machine should basically always make external connections via Deutsche Telekom.

Download and save the existing HiPath 3000 CDB

Proceed as described in Section 1.1, "Transferring CDBs (HiPath 5000 RSM/AllServe Server)".

Enabling "Least Cost Routing" and setting "Digit Transmission"

1. Go to "Settings > Least cost routing" and select the tab **Flags and COS**.
2. In the area "LCR flags" check the "Activate LCR" checkbox.
3. Click the **Apply** button.

Notes: No check for overlaps of call numbers between the LCR dial plan and other numbering plans of the system are performed.

On enabling least cost routing, all outgoing external connections are evaluated by the least cost routing.



Line codes

Trunks can still be directly seized with line codes (trunk keys). These bypass the least cost routing.

Note: If all line codes are deleted, no new line codes can be set up after enabling the least cost routing. Trunk keys that have already been configured remain operational.

Trunk group codes

In order to ensure that the Missed Calls List and the Name Display for speed-dialing entries works properly for incoming calls, the seizure code (also called routing code) for the corresponding route must be entered (under "Lines/networking: Routes").

4. Digit transmission:
 - The setting to be selected is country-specific.
 1. Go to "Settings > Lines/networking" and select the tab **Routes**.
 2. Under "Digit transmission" area select "Digit-by-digit" or "en-bloc sending".

- Digit-by-digit
Digit transmission begins while the station is still dialing.
 - En-bloc sending
All digits up to the end-of-dialing are accepted and examined by HiPath 3000 before transmission. If the end-of-dialing is not evident from the LCR dial plan, a simulated end-of-dialing must be implemented through a waiting period (after 5 s).
3. Click the **Apply** button.

In this configuration example, digit-by-digit transmission was selected.

5. LCR - authorization codes (no entry necessary because not relevant for the configuration examples available).

Configuring the LCR dial plan to enable different handling for local, national, and international calls

6. Click the "Dial plan" tab.
7. Go to the upper table for configuring call number analysis.
8. Call up the "Digit analysis wizard":
 Select the relevant option (City, Inland or Ausland), depending on whether you want to configure call number analysis for city, national or international calls. The corresponding values are automatically entered in the "Name" and "Dialed digits" fields.

In this configuration example, the following entries were made in the LCR dial plan:

Name	Dialed digits	Route table	ACCT	Wako	Emergency
Ausland	0C00Z	3	No	Yes	No
City	0C1Z	1	No	Yes	No
City	0CNZ	1	No	Yes	No
Inland	0C0Z	2	No	Yes	No

- Name column: Name of the call number analysis.
- Dialed digits column: The external call numbers dialed from the station are evaluated on the basis of the digit sequences entered here.
 Note: In the case of external calls, the trunk group code ("0", for instance) must be included in every digit sequence and separated from the remaining digits to be dialed by a field separator ("C").
- Route table column: This column is used to assign the appropriate route tables to the dialed digits in order to enable different handling for national and international calls, for example. The route tables themselves are configured using the lower table.
- Acc. code column (not relevant for this configuration example).

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

- COS column: This column determines whether or not a toll restriction check via the Allowed and Denied lists is to be performed for the corresponding dial plan entry.
- Emergency column (not relevant for this configuration example).

LCR dial plan entries are sorted automatically. The entry specified in the greatest detail is placed at the first position.

The entry "C" means "create simulated dial tone" and also works as a field separator. In this example, it is used to separate the trunk group code "0" (field 1) from the rest of the digits to be dialed (field 2).

The entry "0C00Z" is used to evaluate international calls and branch to route table 3. The entries "0C1Z" and "0CNZ" are used to evaluate local calls and to branch to route table 1. 1 or 2 - 9 ("N") is the first digit of the dialed call number.

The entry "0C0Z" is used to evaluate national calls (0 is the first digit of the dialed call number) and to branch to route table 2.

The "yes" under "COS" means that a toll restriction check via the Allowed and Denied lists is to be performed for the corresponding dial plan entry.

Configuring LCR path tables and dialing rules for different ISPs

9. Click the "Dial plan" tab.
10. Select the lower route table.
11. Use the drop-down list to select the route table you want to configure.
12. Call up the "Dial rule wizard":
 - Edited dial rule: You can select the dial rule and assign a name comprising up to 16 characters here.
 - Network provider's method of: A suitable access procedure for each Internet Service Provider must be selected here.
 - Access code: A suitable access code for each Internet Service Provider must be entered here.
 - Dial rule format: This entry is automatically generated by the Dial rule wizard based on the values entered previously. The formats entered here determine how the digits dialed from the station are converted by the system and on which route the dialing is to occur. This enables access to the various ISPs.

In this configuration example, the following entries were made using the Dial rule wizard:

Rule name	Procedure	Access code	Rule format
Deutsche Telekom	Main network provider		A
Internet Service Provider	Dial-in control server	01070	D01070A

Rule name	Procedure	Access code	Rule format
ISP 01078	MCL single-stage	01078	D01078A
ISP 01081	Dial-in control server	01081	D01081A

Note: If rerouting to an alternative route (e.g., another ISP) is to be enabled on a busy signal, "Main network supplier" should never be entered as the Procedure.

Rule format "A" sends (dials) all digits dialed at the station except field 1 (trunk group code). The "D010xxA" rule formats dial the appropriate ISP (010xx) via parameter "D" and then transmit all the digits dialed at the station (without the trunk seizure code) via parameter "A".

For calls to be routed via the public network (Deutsche Telekom), the access procedure "Main network supplier" is to be selected. For all busy states reported by the ISP 01078, rerouting is to occur via the route table. This is achieved with the procedure "MCL single-stage". With the "Dial-in control server" procedure, by contrast, rerouting via the route table occurs only for a busy state of the ISP itself.

13. Configure the route table.

In this configuration example, the following entries were made in the dialing rules table:

Route table 1

Route	Dial rule	min. COS	Schedule	Warning
ISDN	Deutsche Telekom	15	–	None

Route table 2

Route	Dial rule	min. COS	Time plan	Warning
ISDN	ISP 01078	15	–	Display
ISDN	ISP 01070	15	–	Display
ISDN	Deutsche Telekom	15	–	display + tone

Route table 3

Route	Dial rule	min. COS	Time plan	Warning
ISDN	ISP 01081	15	–	Display
ISDN	ISP 01078	15	–	Display
ISDN	Deutsche Telekom	15	–	display + tone

Route table 1 = Local calls

Only one connection path exists: Seizure of the ISDN route and the dialing rule "Deutsche Telekom".

Route table 2 = National calls

Route table 3 = International calls

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

Three connection paths were entered in each case: The ISDN route is always seized with different dialing rules for the relevant network ISPs.

- Route column: A route name defined under "Lines/networking... > Routes" must be selected.
Note: For the sake of clarity, meaningful names should be assigned for routes and dial rules.
- Dial rule column: A rule name defined via the Dial rule wizard.
- min. COS column: The minimum LCR class of service (1-15) needed in order to use this connection path is specified here. The LCR class of service is compared with the LCR class of service of the station (see Level C, Page 4-137). If the LCR class of service assigned to the station is greater than or equal to that of the connection path, the connection path may be used.
This makes it possible to restrict one station to placing calls only via a specific ISP or during certain times, while allowing other stations the option of using alternative routes.
- Schedule column: This column can be used to select a time zone defined in the "LCR - schedule" (Page 4-135). The time zone is used to check whether the current time matches the interval entered in the schedule. If this is the case and if the required class of service is present, dialing occurs in accordance with the dialing rule entered in the route table.
- Warning column: This column can be used to set whether and which warning is to be issued in cases where the primary connection path in the route table cannot be used. In such cases, the station can be notified by an acoustic and/or optical signal in the terminal display that some other, possibly more expensive, connection path that was defined in the route table was selected. It can then be decided whether or not the connection is to be established.
Note: If you select "display" and "display + tone", the rule name defined in the dialing rules table is shown on the station's display. If no rule name was defined, "Expensive Connection" appears.

14. Save the CDB and transfer it to HiPath 3000.

4.17.1.2 Extension Through a Time-dependent Component (Schedule)

National calls made from Monday through Friday between the times of 07:00 to 19:59 hours are always be to handled via the ISP 01078. In the remaining times, ISP 01070 is to be used. The overflow to Deutsche Telekom remains unaffected.

Local and international calls are not to be included in the schedule in this example.

1. Download and save the existing HiPath 3000 CDB.
2. Call up the "Least Cost Routing..." dialog via the "Settings" menu.

Configuring the LCR schedule for time-dependent ISP selection

3. Click the "Schedule" tab.
4. This enables you to define a schedule for every day of the week and for various times to determine which dialing rule (see Page 4-129) should be applied. Double-click an area in the schedule, for example, to configure the separate time frames.
 A schedule can be defined individually for every day of the week. If no time zones are entered for a particular weekday, the connection paths are used on that day without taking the LCR schedule into account.

Caution: When defining schedules, it is important to ensure that a connection is possible at all times (emergency calls!).

In this configuration example, the following entries were made in the LCR schedule:

	Monday	Tuesday	Wednes- day	Thursday	Friday	Saturday	Sunday
0:00	B	B	B	B	B		
...	B	B	B	B	B		
6:00	B	B	B	B	B		
7:00	A	A	A	A	A		
...	A	A	A	A	A		
19:00	A	A	A	A	A		
20:00	B	B	B	B	B		
...	B	B	B	B	B		
24:00	B	B	B	B	B		

Three time zones were defined for the weekdays from Monday through Friday.

Time zone 1 starts at 00:00 hours and ends at 06:59.

Time zone 2 starts immediately after time zone 1 (in other words, at 07:00 hours) and ends at 19:59.

Time zone 3 completes the 24-hour day from 20:00 hours to 23:59 hours.

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

The time from 07:00 hours until 19:59 hours was assigned time zone "A". The remaining time, in other words, from 20:00 hours through midnight and until 06:59 hours, is assigned time zone "B".

Transferring the time zones defined in the LCR schedule to the corresponding LCR route tables

5. Click the "Dial plan" tab.
6. Select the lower route table.
7. Use the drop-down list to select route table 2.
8. Schedule column: This column can be used to select a time zone defined in the "LCR - schedule". The time zone is used to check whether the current time matches the time frame entered in the LCR - schedule. If this is the case and if the required class of service is present, dialing occurs in accordance with the dialing rule entered in the route table.

In this configuration example, the following entries were made in the LCR route table:

Route table 2

Route	Dial rule	min. COS	Schedule	Warning
ISDN	ISP 01078	15	A	Display
ISDN	ISP 01070	15	B	Display
ISDN	Deutsche Telekom	15	–	display + tone

For time-based control of the ISP selection for national calls, the relevant time zones were assigned to the connection paths in route table 2:

A = Monday through Friday from 7:00 hours to 19:59 hours = ISP 01078

B = Monday through Friday from 00:00 hours to 6:59 hours and from 20:00 hours to 23:59 hours = Internet Service Provider (ISP) 01070.

In this example, local calls (route table 1) and international calls (route table 3) are not handled by the schedule.

9. Save the CDB and transfer it to HiPath 3000.

4.17.1.3 Extension of Least Cost Routing Through LCR Classes of Service

1. Download and save the existing HiPath 3000 CDB.
2. Call up the "Least Cost Routing..." dialog via the "Settings" menu.

Configuring the LCR classes of service for stations

3. Click the "Classes of service" tab.
 - Call No. column: The call numbers of all stations in the communication system are listed here.
 - Name column: All the station names that are allocated to the call numbers are listed here.
 - Class of service column: Each station can be assigned an LCR class of service (1-15) here. This is compared against the LCR class of service of a connection path. If the LCR class of service assigned to the station is greater than or equal to that of the connection path, the path may be used.
The lowest LCR class of service is 1; the highest class of service is 15. A higher class of service automatically includes all lower classes of service.

In this configuration example, the following LCR classes of service were configured for stations:

Call no.	Name	Class-of-service
100	Ballack	15
101	Charistead	15
102	Owen	15
103	Raúl	15
104	Zidane	15
105	Totti	15
106	Makaay	15
107	Figo	15
108	Johuri	15
109	Fax	1
110		15

The Fax machine is assigned the LCR class of service 1. All other stations remain at the default class of service 15.

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

Transferring the LCR classes of service to the LCR route tables

- Click the "Route table" tab.

Caution: When combining schedules and LCR classes of service, it is important to ensure that a connection is possible at all times (emergency calls!).

- min. COS column: The LCR class of service (1-15) needed to use this connection path is specified here. The LCR class of service is compared with the LCR class of service of the station. If the LCR class of service assigned to the station is greater than or equal to that of the connection path, the connection path may be used.

In this configuration example, the following LCR classes of service were entered in the LCR route tables:

Route table 1

	Route	Dial rule	min. COS	Schedule	Warning
1	ISDN	Deutsche Telekom	1	–	None
2	–	–	15	–	None

Route table 2

	Route	Dial rule	min. COS	Time plan	Warning
1	ISDN	ISP 01078	15	A	Display
2	ISDN	ISP 01070	15	B	Display
3	ISDN	Deutsche Telekom	1	–	display + tone
4	–	–	15	–	None

Route table 3

	Route	Dial rule	min. COS	Time plan	Warning
1	ISDN	ISP 01081	15	–	Display
2	ISDN	ISP 01078	15	–	Display
3	ISDN	Deutsche Telekom	1	–	display + tone
4	–	–	15	–	None

In all LCR route tables, the minimum required class of service for the connection path "Deutsche Telekom" was reduced to 1. Consequently, due to an LCR class of service that is too low, the fax machine can no longer seize the ISP routes and is always rerouted to the connection path "Deutsche Telekom".

- Save the CDB and transfer it to HiPath 3000.

Configuring a type of number (TON)

When using E.164, the type of number (TON) is added to the dial rules in least cost routing. The types available for selection are "Unknown", "PABX number", "Local area code", and "Country code".

1. Unknown: Used for networking without E.164 and trunk connections (analog and ISDN). As in V4, V5, and V6.
2. Country code: Should always be used in E.164 networks. The following dial rule formats apply here (for example, for the station number: 0049 89 722 12345)
 - a) Country: (e.g., E3A)
 - b) Location: (e.g., D49E3A)
 - c) PABX number: (e.g., D4989E2A)

The relevant dialed digits are:

for A) 0C00-49-89-Z

for B) 0C0-89-Z

for c) 0C722-Z

3. As a rule, "Local area code" and "PABX number" should not be used as the type of number (TON). If they are used, however, the dial rule format and, where applicable, the dialed call number must be adapted.

4.17.1.4 Function Check

No.	Action
Test basic LCR	
1.	<p>Test local calls: Dial call no. for local call. In this example, local calls are to be handled exclusively via Deutsche Telekom. When entering the digits, it is therefore important to ensure that an Internet Service Provider does not appear in the display ("Warning" parameter in the route table). Note: The digits should be entered slowly, since the ISP display, if any, will only appear for a brief period and will be overwritten by the call number on pressing the next key.</p>
2.	<p>Test national calls: Dial call no. for national call. When entering the digits, pay attention to the Internet Service Provider display ("Warning" parameter in the route table). Note: The digits should be entered slowly, since the ISP display will only appear for a brief period and will be overwritten by the call number on pressing the next key.</p>

Networking Scenarios for HiPath 3000/5000 V8

Least Cost Routing (LCR) for E.164

No.	Action
3.	<p>Test international calls: Dial call no. for international call. When entering the digits, pay attention to the Internet Service Provider display ("Warning" parameter in the route table). Note: The digits should be entered slowly, since the ISP display will only appear for a brief period and will be overwritten by the call number on pressing the next key.</p>
4.	<p>Test alternative connection paths: The test for alternative connection paths in a route table can be performed by temporarily ensuring that no route is assigned to all other paths. The minimum required LCR class of service and the schedule must be taken into account. After the test, the original configuration must be restored!</p>
Test LCR schedule	
5.	<p>The LCR schedule test can be performed by temporarily changing the system time. Note that when the system time is changed by less than 1 hour, it is automatically corrected via ISDN at the next trunk call. After the test, the original system time must be restored!</p>
Test LCR class of service	
6.	<p>In this example, the minimum required class of service for the connection path "Deutsche Telekom" was reduced to 1. Consequently, due to an LCR class of service that is too low, the fax machine can no longer seize the ISP routes and is always rerouted to the connection path "Deutsche Telekom". The LCR class of service test for the fax machine can be performed by temporarily ensuring that no route is assigned to any connection paths other than "Deutsche Telekom". After the test, the original configuration must be restored!</p>

4.18 IP Networking with SPE

4.18.1 IP Networking with SPE Between HiPath 2000 / HiPath OpenOffice EE and HiPath 3000/5000

The encryption setting for the node must be configured for SPE-based IP networking between HiPath 2000 V2.0 MR 4 / HiPath OpenOffice EE and HiPath 3000/5000 from V7 R 4 (default: traditional). You can set whether IP trunking is encrypted or unencrypted for SIP-Q on a node-by-node basis.

The following example describes the encryption setting for node 1.

This setting is made via the HG 1500 WBM.

Node encryption setting

1. Start WBM.
2. Select "Explorers > Voice Gateway > PBX > Nodes".
3. Right-click "1". The menu "PBX Node / IP Addresses" is displayed.
4. Set "secure" under Security Level of Node Encryption (click).
5. Click "OK".

4.19 E.164 Connection with OpenScape Office - General Rules

4.19.1 Gateway Node (Node with direct CO access)

1. "E164 numbering scheme" system-wide flag is activated.
2. Country code is always filled at CO route.
3. Location number is set at this route.
4. International prefix should always be filled-in.
5. Following pairs of LCR rules are needed:
 - **0CZ** LCR dial plan with Dialing Rule: **A** and Route: **CO**
 - **0C00[Country code]-Z** LCR dial plan with Dialing Rule: **E3A** and Route: **CO**
6. Numbering Plan: **System check**
7. CO route: Route prefix: **0**
8. Networking Route: Route prefix: -
9. Networking Route: 2nd trunk code: **0**

4.19.2 Sub node (Node without direct CO access)

1. "E164 numbering scheme" system-wide flag is activated.
2. Country code is always filled-in at CO route (although no CO trunks are available).
 - Location number flag is set at this route.
3. International prefix should always be filled-in.
4. Following pairs of LCR rules are needed:
 - **0CZ** LCR dial plan with Dialing Rule: **E1A** and Route: **Networking**
 - **0C00[Country code]-Z** LCR dial plan with Dialing Rule: **E1A** and Route: **Networking**
5. Numbering Plan: **System check**
6. CO route: Route prefix: **0**
7. Networking Route: Route prefix: -
8. Networking Route: 2nd trunk code: **0**

4.19.3 Configuration Groups

Group 1: (e.g. proposal for Germany, UK, France, Italy)

Country code:	[Country code]
Local area code:	[Local area code]
PABX number:	[PABX number]
International Prefix:	[Country's international prefix]
National Prefix:	[Country's national prefix]

Group 2: (e.g. proposal for Denmark, Spain, Portugal, Tunisia)

Country code:	[Country code]
Local area code:	-
PABX number:	[National number] (Local area code + PABX number)
International Prefix:	[Country's international prefix]
National Prefix:	-

Group 3: (e.g. proposal for Greece)

Country code:	[Country code]
Local area code:	[Local area code]
PABX number:	[PABX number]
International Prefix:	[Country's international prefix]
National Prefix:	-

Group 4: (MSN, Multi-Subscriber)

Country code:	[Country code]
Local area code:	[Local area code]

Networking Scenarios for HiPath 3000/5000 V8

E.164 Connection with OpenScape Office - General Rules

PABX number:	-
International Prefix:	[Country's international prefix]
National Prefix:	[Country's national prefix]
DID numbers:	[PABX number]+[DID]

GROUP 5: (MSN, Multi-Area)

Country code:	[Country code]
Local area code:	-
PABX number:	-
International Prefix:	[Country's international prefix]
National Prefix:	[Country's national prefix]
DID numbers:	[Local area code]+[PABX number]+[DID]

5 Sample Configuration for Xpressions Compact

Contents

This chapter covers the following topics:

- Section 5.1, "Basic Configuration of Xpressions Compact and HiPath 3000/5000"
- Section 5.2, "Configuring the Conference Server"
- Section 5.3, "Configuring and Opening Conference Spaces"

Sample Configuration for Xpressions Compact

Basic Configuration of Xpressions Compact and HiPath 3000/5000

5.1 Basic Configuration of Xpressions Compact and HiPath 3000/5000

For basic configuration of the HiPath 3000 system and Xpressions Compact, please follow the instructions provided in the administration manual (see HiPath 3000/5000 V8, service documentation).

Ensure that Xpressions Compact is reachable via LAN.

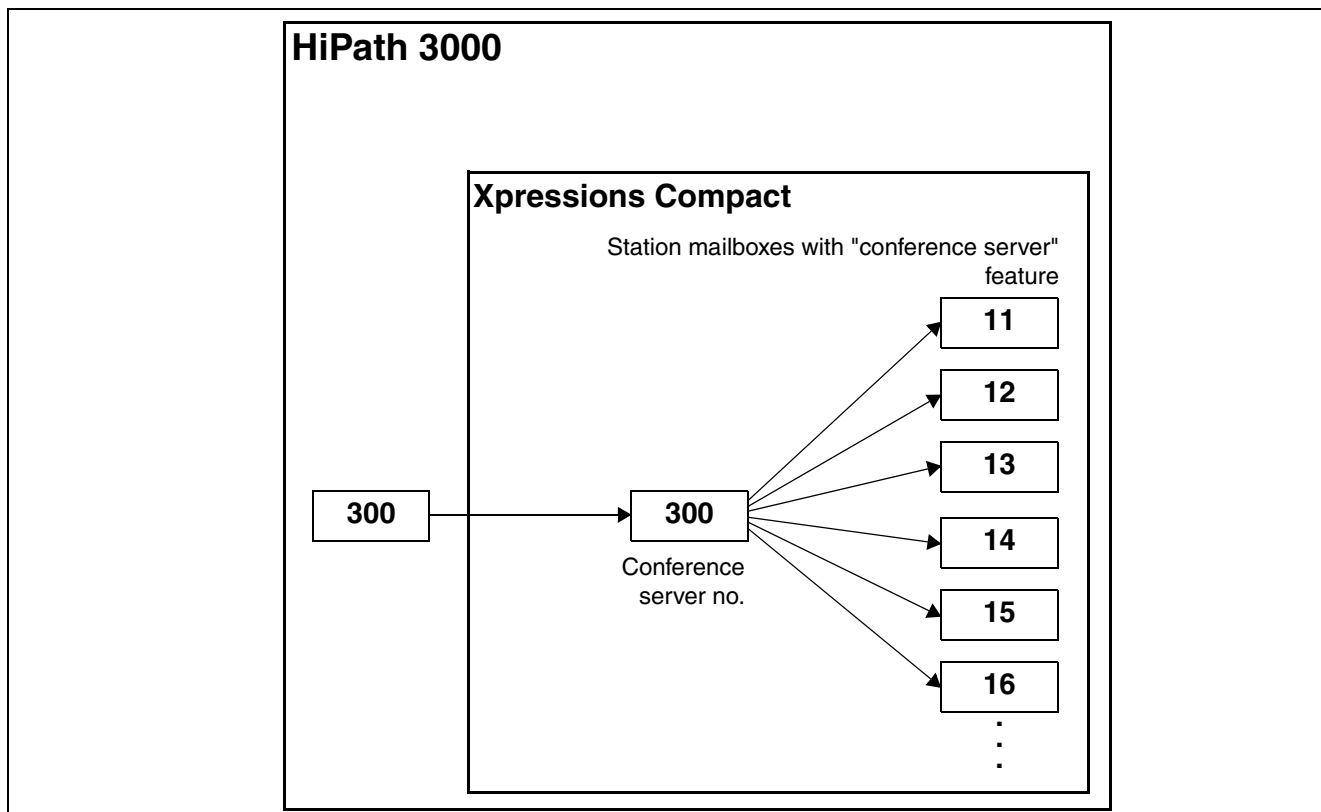
5.2 Configuring the Conference Server

Required components

The following components are required:

- Licences
- HiPath 3000 Manager E
- Xpressions Compact WBM

Configuration overview



For conference server basic configuration, a virtual station is set up in the HiPath 3000 system and configured for forwarding to the Xpressions Compact hunt group. This call number is used as the central dial-in number in the conference server.

At least one license is required for the "conference server" feature.

Contents

This section covers the following topics:

- Section 5.2.1, "Assigning Licenses"
- Section 5.2.2, "Configuring the Conference Server Number"

5.2.1 Assigning Licenses

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
2. Click **Systemview** and then click **Settings > Licensing > IVM**.
3. Under **CDB data**, assign the required licenses for **IVM Conferencing**.

5.2.2 Configuring the Conference Server Number

The dial-in number for the conference server must be configured as a virtual station in the HiPath 3000/5000 system.

5.2.2.1 Configuring the HiPath 3000 system

The necessary configuration steps in HiPath 3000 Manager E are listed here.

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.

Virtual station

2. In the menu, go to **Settings > Configure station > Stations** and open the table for the internal station.
3. Select a row for the new call number of the virtual station; the row must be configured as type **No Port** and without **Access** assignment.
4. In this row, enter the values for **Call no.**, **DID** and **Name** (e.g. 300).
5. Switch to the **Station view** to define the virtual station in this view.
6. Under **Station selection**, select the call number or name (e.g. 300).
7. In the **Flags** tab, activate the **Virtual station** checkbox.

Incoming calls

Assign the virtual call number to Xpressions Compact via **Incoming calls**.

8. Click **Call forwarding**.
9. In the **Call destination lists** table, select a free list (e.g. List 3).
10. As the **First destination**, enter (*).
11. As the **Second destination**, enter the call number of the Xpressions Compact hunt group (e.g. 350).

Sample Configuration for Xpressions Compact

Configuring the Conference Server

12. Leave all other rows blank
13. Reduce the number of **Cycles** to **1**.

In the **Call destination lists - assignment to stations** table, you can assign a call number to the Xpressions Compact hunt group.

14. Select the virtual station's row (e.g. 300) and enter the numbers in the call destination lists for the statuses **Day**, **Night** and **Internal**, which point to the Xpressions Compact hunt group (e.g. List 3).
15. Save the data in the system.

5.2.2.2 Configuring Xpressions Compact

The required configuration steps in Web-based Management of Xpressions Compact are set down here.

1. Open Web-based Management using Internet Explorer on your service PC.

Example:

<https://IP address> or <https://server name>

2. Log in as the user "**Service**" using the HiPath 3000 system's **User ID** and the **PIN code** to Web-based Management on Xpressions Compact.
3. In the **System administration** menu, click **Mailbox administration**.
4. In the **System administration** menu, click **Conference settings**.

Here you can configure the following parameters:

- Speaking when on hold
 - Continuing conference without conference conductor
 - Maximum call duration without conference conductor (min.)
5. Open the **System administration -> Conferencing server** window.

In the "Function number" field, enter the number of the virtual station configured in the previous section.

5.3 Configuring and Opening Conference Spaces

To initiate and run conferences, "conference spaces" are required. For this, the "Conferencing server" feature is added to station mailboxes.

Contents

This section covers the following topics:

- Section 5.3.1, "Setting up a Conference Space"
- Section 5.3.2, "Opening a Conference Space via WBM"

5.3.1 Setting up a Conference Space

The required configuration steps in Web-based Management of Xpressions Compact are set down here. Proceed as follows:

Open mailbox administration

1. Open Web-based Management using Internet Explorer on your service PC.

Example:

<https://IP address> or <https://server name>

2. Log in as the user "**Service**" using the HiPath 3000 system's **User ID** and the **PIN code** to Web-based Management on Xpressions Compact.
3. In the **System administration** menu, click **Mailbox administration**.

Configure the mailbox

If a user that wishes to use the conference server does not have their own mailbox, for example, because they use OpenScape Office for voicemail, a separate mailbox must be configured for this user. The mailbox numbers should correspond to the station extension. As forwarding to Xpressions Compact is not required for these stations, there is no conflict with OpenScape Office.

4. To configure a mailbox, select a free **Mailbox no.** in the right-hand window and enter the name and number of the mailbox.
5. Assign the class-of-service "Conferencing server" to the mailbox; see section "Assigning the class-of-service "Conferencing server" to a mailbox".
6. Define conference settings for the mailbox; see section "Defining conference settings".
7. Click **Save** to end configuration.

Sample Configuration for Xpressions Compact

Configuring and Opening Conference Spaces

Assigning the class-of-service "Conferencing server" to a mailbox

If a mailbox is already configured:

8. Click **Edit** in the mailbox row and then, under **Mailbox administration** in the menu on the left, click **CoS**.
9. Under "Select CoS", select **User-defined**.
10. Activate the **Conferencing server** checkbox.
11. Click **Save** to apply the changes.
12. Repeat steps 8 to 11 for each additional station that needs to use the conferencing server.

Defining conference settings

If a mailbox is already configured:

13. Open the **Mailbox administration -> Conference settings** window.
14. Activate/deactivate the "Allow recording" checkbox. If the checkbox is activated, the station can record conferences.



Important: In a HiPath 3000 system where OpenScape Office is being used for voice-mail, the "Allow recording" checkbox must be deactivated. If the checkbox were activated, the conference recording would be saved to the Xpressions Compact mailbox. This would result in a message waiting indication (MWI) on the station device. As OpenScape Office is used as voicemail, the station would call up the OpenScape Office voicemail when attempting to listen to the supposed message.

15. Click **Save** to apply the changes.

5.3.2 Opening a Conference Space via WBM

The required configuration steps in Web-based Management of Xpressions Compact are set down here.

1. Open Web-based Management using Internet Explorer on your service PC.

Example:

https://IP_address or https://server_name

2. Log in as **User** with the **user ID**, **mailbox number** and **PIN code** for the conference space in Xpressions Compact Web-based Management.
3. In the **Mailbox administration** menu, click **Conference space**.
4. If necessary, configure the following parameters in the right-hand window:

Number of conference participants	Required entry
Language	Language of user guidance
Code for conference space	Authentication code when dialing in
Enable self-dial-in	Enable or disable the option for stations to dial in

5. If necessary, enter the stations that may not enter the conference via dial-in in the following table. These stations are called at the beginning of the conference.

Call number	Call number type	Name	Status
-------------	------------------	------	--------

6. If you wish to open conferencing for this conference space, click **Open**.
7. Use the **Bookmark** control key to save the contents of the input fields in the Favorites list on your browser, for subsequent conferences. You can store an unlimited number of different conference participant lists in the Favorites list and access it at any time.

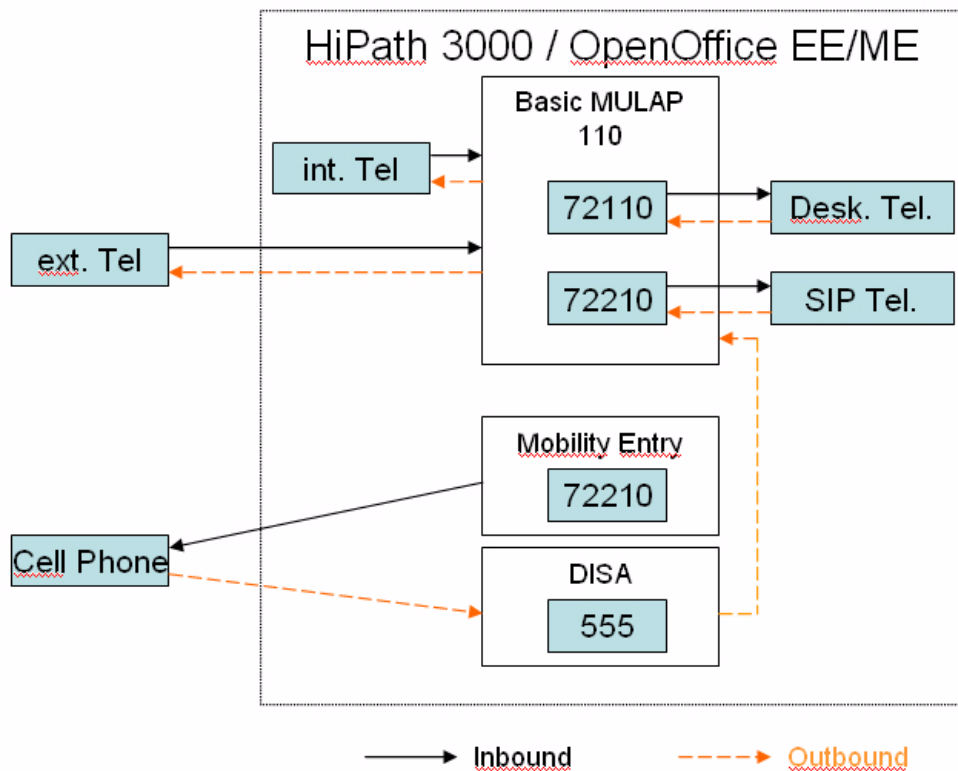
Sample Configuration for Xpressions Compact
Configuring and Opening Conference Spaces

6 Setting Up Dual Mode Mobility Entry

Required components:

- Mobility licenses
- Comscendo licenses
- HiPath Manager E
- SIP-capable GSM phone

Dual Mode Mobility Entry



A Basic MULAP is set up in the HiPath 3000 system for the basic configuration "Dual Mode". In the Basic MULAP, both the fixed connection and the SIP station are integrated.

The assignment and the automatic call forwarding to the GSM phone when the SIP phone is logged off occurs via the Mobility Entry list.

Dialing of the GSM phone in the HiPath system occurs via the call number of the DISA port.



The timeout for detecting that the SIP client is not reachable is about 120 seconds. At least one license for Mobility Entry is required.

Setting Up Dual Mode Mobility Entry

Assigning a License

6.1 Assigning a License

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
2. Click on **System View** and then on **Settings > Licensing**.
3. Assign the required licenses for the SIP station and Mobility under **CDB Data**.
4. Confirm the configuration with **Apply**.
5. Save the data and send it back to the system.

6.2 Setting up the SIP Station

6. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
7. Click on **System View** and then on **Settings > Set up station > Gatekeeper**.
8. Select the station to be configured as an SIP station in the **Stations** area.
9. Under **Selected station...**, select the item **SIP Client** and click **Setup**.
10. Confirm the configuration with **Apply**.
11. Click on **Station View** and select the call number of the SIP client to be configured in the **Station selection** table.
12. Open the **Workpoint Clients** tab and make any configuration settings that may be required in the **SIP Client** area.



The required settings under **SIP Client** depend on the client software being used and its configuration.

13. Confirm the configuration with **Apply**.
14. Save the data and send it back to the system.

6.3 Setting up a Basic MULAP

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
2. Click on **System View** and then on **Settings > Incoming Calls > Groups/Hunt groups**.
3. Select an unused row in the **Group** table and enter the **Call No.**, **DID** and possibly the **Name** of the Basic MULAP here.
4. Select the item **Basic MULAP** as the **Type** of the selected group.
5. Mark the call number for the internal subscriber and the call number for the SIP client in the **Selection** table.
6. Move the subscribers from the **Selection** list over to the **Members** list of the Basic MULAP.

7. Double-click in the **Members** table on the **Parameters** column for the individual members of the Basic MULAP. The **Member Parameters** configuration window appears. Every member of the Basic MULAP must be set up as a "Master".
8. Enable the parameters **Master (M)**, **Acoustic call (R)** and **Automatic seizure outgoing (A)** for all members.
9. Close the configuration window and confirm the configuration with **Apply**.
10. Save the data and send it back to the system.

6.4 Setting up Mobility Entry

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
2. Click on **System View** and then on **Settings > Set up station > Mobility Entry**.
3. Select a free row in the **Mobile Connection** table.
4. In the **User** column, select the **SIP Port** you configured in the Basic MULAP.
5. Enter the call number of the GSM phone you want to use in dual mode in the **Mobile Number** column.



The external call number must always be entered with the seizure code.

6. Confirm the configuration with **Apply**.
7. Save the data and send it back to the system.

6.5 Configuring DISA

1. Open HiPath 3000 Manager E and load the current CDB from the HiPath system.
2. Click on **System View** and then on **Settings > System Parameters > Daylight saving time/DISA**.
3. Enter the direct inward dialing number to be used for external dialing under **DISA**.
4. Under **Security Mode**, select the item **After timeout**.
5. Confirm the configuration with **Apply**.
6. Save the data and send it back to the system.

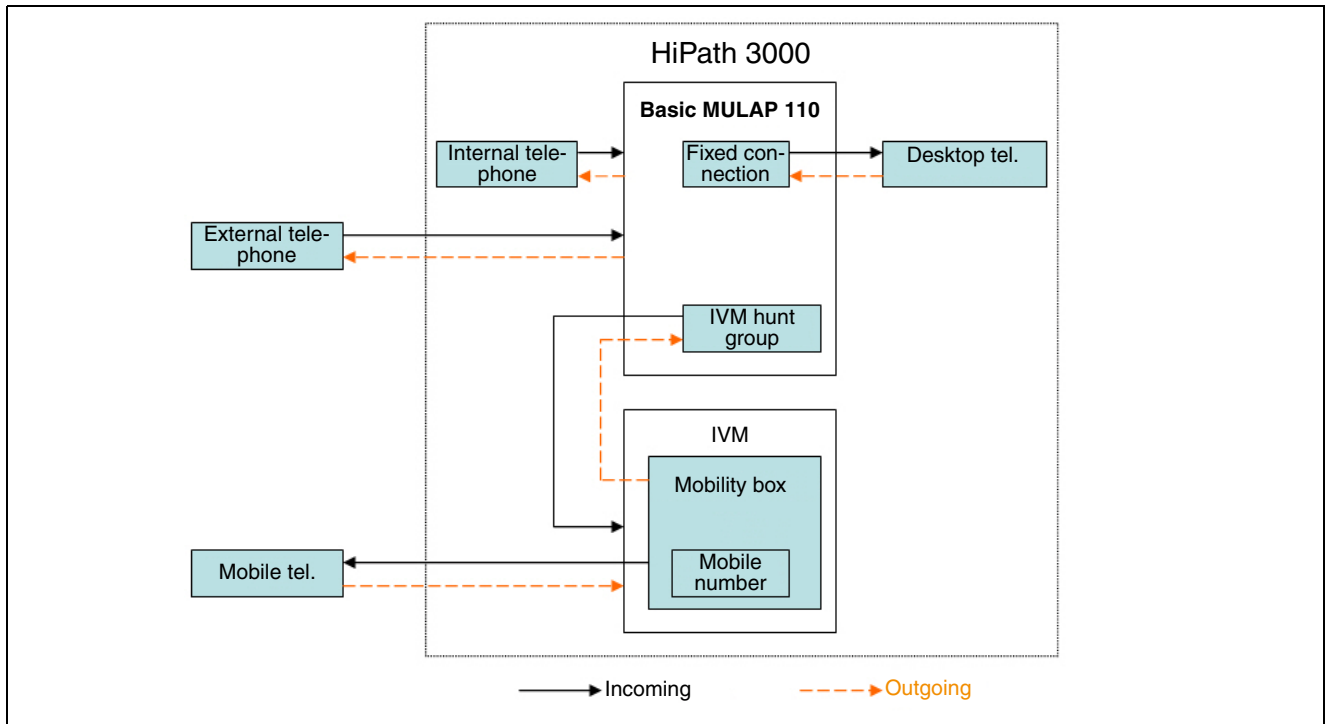
Setting Up Dual Mode Mobility Entry

Configuring DISA

7 Configuring FMC Parallel Signaling with IVM

Configuration overview

A basic MULAP is configured in HiPath 3000 for parallel signaling. Both the fixed connection and the IVM hunt group are integrated in the basic MULAP. Mobile phone dialup to HiPath 3000 is via the IVM hunt group's call number.



Contents

This section covers the following topics:

- Section 7.1, "Required Components"
- Section 7.2, "Performing Basic Configuration"
- Section 7.3, "Assigning Licenses"
- Section 7.4, "Configuring Basic MULAP"
- Section 7.5, "Configuring a Mobility Mailbox"
- Section 7.6, "Configuring Mobility Function Numbers in Manager E"
- Section 7.7, "Configuring Mobility Function Numbers in WBM"
- Section 7.8, "Configuring a Mobility Mailbox"
- Section 7.9, "Configuring Call Pickup"

Configuring FMC Parallel Signaling with IVM

Required Components

7.1 Required Components

The following components are required to configure parallel signaling:

- Mobility licenses
- HiPath Manager E
- Xpressions Compact IVM
- WBM access to Xpressions Compact IVM

7.2 Performing Basic Configuration

To perform basic configuration:

1. Follow the instructions for HiPath 3000 and Xpressions Compact basic configuration as set out in the HiPath 3000/5000 V8 service manual.
2. Ensure that Xpressions Compact is reachable via LAN.

7.3 Assigning Licenses

An FMC connection (FMC: Fixed Mobile Convergence) via the IVM always requires two B channels on the IVM. At least one license is required for FMC with IVM.

Proceed as follows:

1. Open Manager E.
2. Load the current CDB from the HiPath 3000 communication system.
3. Click **Systemview** and then click **Settings > Licensing > IVM**.
4. Under **CDB data**, assign the required licenses for IVM mobility.
5. Confirm the configuration by clicking **Apply**.
6. Save the data and return it to the communication system.

7.4 Configuring Basic MULAP

Proceed as follows:

1. Open Manager E.
2. Load the current CDB from the HiPath 3000 communication system.
3. Click **Systemview** and then click **Settings > Incoming calls > Groups/Hunt groups**.
4. In the **Group** table, select a blank row and enter the **Call No.**, **DID** and, if necessary, the **Name** for the basic MULAP.
5. Under **Type**, select **Basic MULAP** for the selected group.

6. In the **Selection** table, select the call number for the internal station and the call number for the IVM hunt group.
7. Transfer stations from the **Selection** list to the **Members** list for basic MULAP.



Important: The IVM hunt group call number should always be entered as the last member in the list.

8. In the **Members** table, double-click the **Parameters** column for the individual members of basic MULAP. The **Member parameters** configuration window appears. Each member of basic MULAP must be configured as a "master".
9. For all members, activate the **Master (M)**, **Audible call (R)** and **Automatic assignment (outgoing) (A)** parameters.



Important: For the first member in the table and for the IVM hunt group, these parameters are set automatically in the **Members** table.

10. Close the configuration window and confirm the configuration by clicking **Apply**.
11. Save the data and return it to the communication system.

7.5 Configuring a Mobility Mailbox

Proceed as follows:

1. Open Manager E.
2. Load the current CDB from the HiPath 3000 communication system.
3. Click **Systemview** and then click **Settings > Auxiliary equipment > Integrated voicemail (IVM)**.
4. In the **Mailboxes** table, select a blank row.
5. In the **Mailbox call no.** column, enter the same call number that you configured for basic MULAP.
6. Double-click the **Parameters** column. The parameter settings window for this mailbox opens.
7. Open the **COS** tab and activate the **Mobility mailbox** parameter in the **COS** table.
8. Confirm the configuration by clicking **Apply** and close the configuration window.



Important: An individually configured mailbox is designated "Type x" in the **Mailboxes** table under the **COS** column.

9. Confirm the configuration in the **Mailboxes** table by clicking **Apply**.
10. Save the data and return it to the communication system.

7.6 Configuring Mobility Function Numbers in Manager E

Proceed as follows:

1. Open Manager E.
2. Load the current CDB from the HiPath 3000 communication system.

Virtual stations

1. Click **System view** and then click **Settings > Configure station > Stations**.
2. In the **Stations** table, select eight rows to which no physical access has been assigned.
3. Assign a unique **Call no.**, a **DID** and a **Name** to each row.
4. Call numbers are required for the following functions:
 - Request callback
 - Activate forwarding to first alternative destination
 - Activate forwarding to second alternative destination
 - Activate forwarding to third alternative destination
 - Deactivate forwarding
 - Activate e-mail notification
 - Deactivate e-mail notification
 - Request call pickup



Important: Function numbers must be entered identically via WBM in Xpressions Compact IVM.

5. Confirm the configuration in the **Stations** table by clicking **Apply**.
6. Click **Station view** and select the call numbers you wish to configure in the **Station view** table.
7. For each station, open the **Flags** tab and activate the "**Virtual station**" flag.
8. Confirm the configuration by clicking **Apply**.

Incoming calls

1. Set "Associated Dialing" for an available station where call forwarding for the virtual station is activated. In Manager E, proceed as follows:
 1. Click the **Station view** button.
 2. On the left side of the window, select a station from the **Station selection** table. Station settings are displayed on the right side of the window.
 3. For this station, activate the **Associated dialing/services** checkbox.
 4. Click **Apply** to confirm the configuration changes.
 5. Save the data and return it to the communication system.
2. Set call forwarding to the desktop phone for a virtual station. On desktop phones, proceed as follows:
 1. Enter the service codes ***83**.
 2. In the `Service for:` display, enter the phone number of the virtual station (*83: associated services).
 3. In the subsequent `Service for: <Name>` display, enter the service code ***11** and **<No. of IVM hunt group>** (*11: call forwarding).
 4. Save the changes on the desktop phone.
3. Set call forwarding for all eight virtual stations.

7.7 Configuring Mobility Function Numbers in WBM

The required configuration steps for FMC in Xpressions Compact Web-based Management are set down here.

Proceed as follows:

1. Ensure that the correct Java 2™ version is installed on the service PC.
2. Open Web-based Management using Internet Explorer on your service PC.

Example:

<https://IP address> or <https://server name>

3. Log in as the user "**Service**" using the HiPath 3000 **User ID** and the **PIN code** to Web-based Management on Xpressions Compact.
4. In the **System administration** menu, click **Mobility function numbers**.
5. Enter the function numbers configured for FMC.



The function numbers should be configured in HiPath 3000 as virtual stations that are forwarded to the IVM hunt group.

Configuring FMC Parallel Signaling with IVM

Configuring a Mobility Mailbox

7.8 Configuring a Mobility Mailbox

The required configuration steps for FMC in Xpressions Compact Web-based Management are set down here.

Proceed as follows:

1. Ensure that the correct Java 2™ version is installed on the service PC.
2. Open Web-based Management using Internet Explorer on your service PC.

Example:

<https://IP address> or <https://server name>

3. Log in as the user "**Service**" using the HiPath 3000 system's **User ID** and the **PIN code** to Web-based Management on Xpressions Compact.
4. In the **Mailbox administration** menu, click **Mobility**.
5. Activate the **Mobility activated** function.
6. In the first row of the table, enter the call number of the mobile phone or the external station you wish to integrate in FMC under **Forwarding/administration**.
7. In the **Call number type** column, select **Call number**.
8. Repeat this step if necessary for up to two alternative destinations.
9. All other parameters available here may be individually configured and modified by the user.
10. Confirm the configuration by clicking **Save**.

7.9 Configuring Call Pickup

Aim of the configuration

The configuration described in this section should allow users to pick up calls from a mobile telephone on their desktop telephones. Calls are only taken on the mobile telephone once they have been signaled on both the desktop telephone and the mobile telephone simultaneously.

For this configuration, please note the following restrictions for a MULAP group:

- Starting a call: A MULAP station cannot start a call if the MULAP group is active. In an active MULAP group, calls can only be started via DSS keys.
- Call forwarding: If a station is called using a DSS key, the communication system disregards the configured call forwarding on the call management list. Call forwarding can only be performed if configured under the service code *11.

Required settings

The following settings are required to configure call pickup:

- Configuring the "Associated dialing" feature for the desktop telephone to enable call forwarding to the IVM group to be configured on a virtual station.
- Configuring a DSS key on the MULAP station for the virtual station: *<NoVirtStn>*.

Contents

This section covers the following topics:

- Section 7.9.1, "Configuring a DSS Key"
- Section 7.9.2, "Configuring "Associated Dialing" for the Desktop Telephone"
- Section 7.9.3, "Configuring Call Forwarding on the Desktop Telephone"

Configuring FMC Parallel Signaling with IVM

Configuring Call Pickup

7.9.1 Configuring a DSS Key

1. Open Manager E.
2. Click **System view** and then click **Settings** > Configure **station** > **Key programming**.
3. Activate the **Key programming** radio button.
4. In the "Key code" area, select **Call number** and assign the desired call number for DSS calls.
5. Click **Apply** to save your changes.

7.9.2 Configuring "Associated Dialing" for the Desktop Telephone

Proceed as follows:

1. Open Manager E.
2. Select **Station view**.
3. In the "Station selection" table, select the call number of the desktop telephone.
4. Activate the **Associated dialing/Services** checkbox for the desktop telephone.
5. Click **Apply** to save your changes.

7.9.3 Configuring Call Forwarding on the Desktop Telephone

Call forwarding must be configured on the desktop telephone for the virtual station. On the desktop telephone, enter the following service codes:

1. Enter service code ***83 <NoVirtStn>** (*83: associated services).
2. Enter service code ***11 <NoIVMHuntGroup>** (*11: call forwarding).

Index

A

- Account codes
 - defining 28
- Adding a busy lamp field 11
- Adding a key extension unit 10
- Allocating a station to a hunt group 16
- Allocating a station to a team 13
- Allowed list, editing 23
- Allowed list, notes and examples 24
- Announcement prior to answer 38
- Answer texts 32
- APS transfer, performing 34
- Assigning a call destination list to a station (for day service) 15
- Assigning/changing class of service groups 22

C

- Call detail recording 27
- Call forwarding 14
- Call forwarding destinations, external 14
- Call pickup 13
- Call pickup group
 - assigning 13
- Cancelling allocation to a hunt group 16
- Cancelling allocation to a team 13
- Changing info and answer texts 32
- Changing key labeling 9
- Changing parameters 8
- Changing table entries in Allowed/Denied lists 26
- Changing the COS group for day/night 23
- Changing the station's call number 6
- Classes of service 22
- Configuring an internal S0 bus 39
- Configuring attendants 44
- Configuring stations/users 6

D

- Daylight saving time 33
- Defining call charge factors per route 27
- Defining CMI data 30
- Defining ringing assignment in the hunt group 16
- Defining speed dialing system destinations 31
- Defining the key click volume 30
- Deleting a busy lamp field 11
- Deleting a key extension unit 11
- Deleting call charges 27
- Deleting table entries in Allowed/Denied lists 26
- Denied list
 - editing 24
- Denied list, notes and examples 25
- DID number
 - changing at a PCPBX system connection 7

E

- E.164 128
- Eliminating conflicts that showed up during the check 8
- Encryption 1
- Exporting call charges 27
- External call forwarding destinations 14

G

- Groups/hunt groups 16

H

- HiPath 3000 Manager E 3
- Host IP routing 9
- Hunt group 16

I

- Incoming calls that display company names 36
- Info texts 32

K

- Key programming 9

Index

L

LAN-LAN routing 19
LCR (Least Cost Routing) 128
Least Cost Routing (LCR) 128
Loading IVM data 17

M

Mobility Entry 45
MSN
 changing for a multi-device connection 6

N

Names, changing 8
Networking
 HiPath 2000 and HiPath 3000 with break-out to the ITSP 25
 HiPath 2000 and HiPath 3000 with two CorNet-NQ trunks 18
 HiPath 3000 V7 and HiPath 3000 V7 with E.164 38
 HiPath 3000 V7 and HiPath 4000 V4 with E.164 60
 HiPath 3000 V7 R4 to HiPath 8000 V3.1 R2 via SIP-Q V2 63
 HiPath 3000 V7 with a HiPath 3000 V7 via TDM 34
 HiPath 3000 V7 with an external system via ISO-QSIG or ECMA-QSIG 122
 HiPath 3000 V7 with HiPath 4000 V4 via TDM 57
 HiPath 3000 V8 with HiPath 4000 V5 via SIP-Q V2 48
 HiPath 3000/5000 V7 with HiPath 2000 V2 via CorNet-IP 2
 HiPath 3000/5000 V7 with HiPath 2000 V2 via SIP-Q V2 10
 HiPath 3000/5000 V7 with HiPath 3000 V7 via IP 27
 HiPath 3000/5000 V7 with HiPath 4000 V4 via IP 44
Notes and examples for the allowed list 24
Notes and examples for the denied list 25

O

OpenStage logo 54
OpenStage logo file 54
OpenStage logos 54

P

Printing a label sheet 10

R

Remote service via ISDN 40
Resetting to standard texts 32

S

Save options for paths, changing 34
Setting the start and end of daylight saving time 33
Setting up a call destination list 14
Setting up external destinations 16
Signaling & Payload Encryption 1
 automatic configuration 25
 certificates 4
 configuration 2
 error correction 19
 secure trace 26
 security configuration 11
 system flags 12
SPE 1
Standard texts 32
Swapping/replacing languages 35
System parameters 30

T

Texts, standard 32

U

Universal Call Distribution (UCD) 42