SIEMENS

Hicom 150 H / Hicom 150 E Office

Administration Instructions for HiPath HG 1500

Information and
Communications

Scope

This manual is valid for HiPath HG 1500 Version 2.0.

HiPath HG 1500 can be operated either at a Hicom 150 E Office Point/Com/Pro (Release 2.2 and later) or at a Hicom 150 H Office Point/Com/Pro (Version 1.0 and later).

The "system clients" mentioned in the manual refer to the "C55 optiClient"/"optiClient 130" and the "optiPoint IPadapter" adapter.

Guide to reading the manual

Terms highlighted in **bold** in the text are original terms that you will find in this exact form as buttons or text entries in the Assistant I administration program or in the operating system.

- Texts introduced by this symbol are bullet lists
- Numbered texts describe tasks that must be performed in this exact order.

➡ This symbol indicates particularly important instructions and additional information!

Intended users

This manual is intended for the network administrator responsible for LANs and external LAN communication. The administrator should possess basic ISDN knowledge. All functions required by particular customers can be customized by the administrator using the Assistant I administration program.

Structure of the manual

The chapter entitled **Overview of features** provides a brief overview of the properties of the installed board.

The chapter entitled **Startup** describes the steps required to start up the system and configure the HiPath HG 1500 administration program.

The chapter entitled **Administration with** Assistant I describes and lists the individual menu commands and icons. It provides you with an overview of all modifiable parameters.

The chapter entitled **Applications** lists the individual applications such as Voice over IP, routing, telematics services, etc. The steps involved in the configuration of the individual applications are described in detail.

The chapter entitled **Configuration examples** contains a list of tools that can be used to configure HiPath HG 1500 and its associated applications.

The chapter entitled **Appendix** contains information about eliminating errors that arise during the configuration or operation of HiPath HG 1500. This chapter also contains a description of other useful utility programs.

Important Information

Safety Precautions

Do not operate the hardware component of your HiPath HG 1500 in environments where there is risk of explosion.

Only use original Siemens accessories. The use of non-Siemens accessories is dangerous and invalidates the warranty and CE symbol.

Never open the hardware components of your HiPath HG 1500. In the event of problems, contact an authorized technician.

Avoid contact between the hardware components of your HiPath HG 1500 and colored or aggressive liquids, such as tea, coffee, juices or soft drinks.

CE symbol

The devices meets the requirements contained in the EU Directive 1999/5/EU and thus carries the CE symbol.

Environmental symbol

This device was manufactured in accordance with our certified environmental management system (ISO 14001). This process ensures that use of primary raw materials, energy consumption and waste is kept to a minimum.

Overview of features

HiPath HG 1500 is an expansion board for Hicom 150 H Office point/Com/Pro. It allows you to connect Hicom 150 H to a local LAN and to set up connections to external LANs using the ISDN network. The Hicom 150 H is used therefore as the central communication server in the LAN. The TCP/IP or IPX/SPX transport protocol and the Windows 95/98, Windows NT 4.0 or Windows 2000 operating system are the prerequisites for this facility.

Functions of HiPath HG 1500:

- **Voice over IP**

  The "Voice over IP" function allows HiPath HG 1500 clients to set up telephone connections on the PC via the LAN and to use the features of Hicom 150 H Office Point/Com/Pro. H.323 clients can also be configured, for example, for NetMeeting.
- **Routing**

  HiPath HG 1500 supports the standard functions of an ISDN (IP/IPX) router. This enables you to use the routing and security functions integrated in HiPath HG 1500 (for example, central firewall, short-hold mode with optimized call details, channel bundling as required, up to 16 B channels (configurable), broadcast filtering).
- **LAN-LAN connection / RAS**

  The LAN-LAN link allows Ethernet LANs in different locations to be connected to one single company network using ISDN dial-up lines. Field services and teleworking PCs (via RAS) can access network resources in this way (for example, access to databases, emails, fax mailboxes, triggering of a print job, etc.).
- **vCAPI interface telematics services**

  The virtual CAPI interface supports PC-controlled telephony. Telematics functions such as fax-on-demand,
  Eurofile transfer, online services can be used.
- **TAPI interface for CTI services**

  The TAPI interface (CSTA) supports PC-controlled telephony. CTI functions such as automatic dialer, call journal or "Smartset for ISDN" can be used.
- **Internet access**

  The Internet access provides the following features:

  - dynamic reference of the Internet provider (IP) address
  - access to the Internet via a single IP address of an Internet provider, i.e. cost-effective solution for all PCs in the network
  - dynamic or static channel bundling (activation of B channels depending on the load)
  - connection to the provider via T-DSL
  - second LAN interface for disconnection from the WAN interface

- **Administration using the** Assistant I **PC program**

  The HiPath HG 1500 can be configured with the Assistant I administration program using an Admin PC.
- **Channel bundling (PPP multilink)**

  The data transmission rate can be increased to x times 64 Kbit/s using "channel bundling" when data is exchanged using ISDN (up to 16 channels, system-specific). The PPP multilink protocol allows data packets to be distributed via several data connections.
- **Access control facility**

  An access control facility (firewall) prevents unauthorized access to the company LAN. The firewall mechanisms include:

  – ISDN call number verification

  – Automatic callback request without setting up a toll ISDN connection

  – Verification of the IP or IPX address

  – MAC firewall (verification of the MAC/IP address combination)

  – Verification of IP address with regard to port numbers
- **External gatekeeper support**

  The gatekeeper registers the H.323 clients and administers their rights and services. It converts client call numbers into logical names or IP addresses and vice versa. In addition, it registers the gateways and can be networked with neighboring gatekeepers.
- **Quality of Service (QoS)**

  To guarantee the required bandwidth for Voice over IP, IP packages can be marked the thus given priority for transport in the LAN/WAN.
- **Networking multiple systems via IP**

  Multiple Hicom PBXs can be networked via Voice over IP (H.323) for telephony (valid from Hicom 150 H).
- **Authentication**

  If an external connection is set up using HiPath HG 1500, the PAP (password authentication protocol) and CHAP (challenge handshake authentication protocol) can be used to authenticate stations to increase security in data networks.
- **Second LAN interface (optional)**

  A second LAN interface is configured for disconnecting the DSL-WAN interface. The connection to the first LAN is set up via a routing function.
- **DSL support (optional)**

The configuration database has been extended to include an additional interface. The information needed to dial into the DSL network is specified here. The extended configuration parameters can be entered via Assistant I. The DSL function is only available in the case of a second LAN interface.

Startup

Overview

HiPath HG 1500 is started up by the network administrator and your Siemens technician.

HiPath HG 1500 (see → 13) is initially configured in general via the LAN port. The system can also be started up for the first time remotely (e.g. from a service center). A V.24 adapter (S30122-X5468-X3) is required for initial configuration via SLIP. The Admin PC can be connected using Dial-Up Networking. The configuration of Dial-Up Networking on the Admin PC is described in the chapter entitled"Configuring the Admin PC" on page 13. The administration program for HiPath HG 1500 must already be configured on the Admin PC.

Start the initial startup process by transferring a customer database (CDB) to the Admin PC. Process this CDB and then transfer it to HiPath HG 1500. You can view the software version of HiPath HG 1500 now by selecting the Basic settings command.

Only perform the initial startup of HiPath HG 1500 in conjunction with your service technician!
The incorrect configuration of HiPath HG 1500 may block access to HiPath HG 1500!

If appropriately configured, the HiPath HG 1500 can set up toll connections autonomously. Accordingly, the LAN can also be connected automatically to other partners by means of routing. We therefore strongly recommend using suitable tools (e.g. line keys) and, if in doubt, traces to check and verify the board's ISDN traffic.

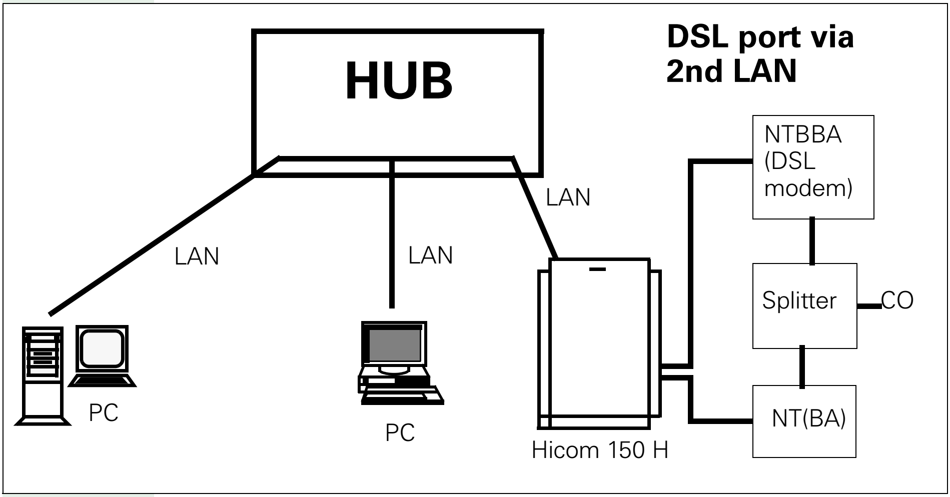
Integration of HiPath HG 1500 in different network topologies

HiPath HG 1500 is equipped with a twisted pair port with a 10/100-MB autosense capacity.

A bus cabling system is used to represent and illustrate all Ethernet LAN types for the purposes of simplification.

Star topology with hub (10/100 BaseT)

A hub or switch is used as the central element in this network topology. Every data terminal is connected to the hub by means of a separate twisted-pair cable (e.g. 10/100 BaseT-Ethernet). A standard hub emulates a bus internally. Only one terminal is affected in the event of cable failure. The integrated HiPath HG 1500 can be directly connected.



Notes:

- Max. overall length of cable between HUB/switch and HiPath HG 1500 = 100 m.
- In the case of other bus topologies (e.g. 10 Base 2), the HiPath HG 1500 can only be connected via a hub or switch that provides for an appropriate implementation.

Configuring the Admin PC

Windows 3.11 is no longer supported.

Prerequisite:

The network card must be installed on the Admin PC with the TCP/IP protocol.

Configuring the administration program

You can configure and manage Assistant I with the HiPath HG 1500 administration program. Assistant I should be configured on the Admin PC by the Siemens technician during startup.

1. Open the setup program from the disk or the installation CD. To do this, start Windows Explorer and switch to the disk or CD-ROM drive. Double-click the "setup.exe" file.
2. The Assistant I setup program opens. Follow the instructions of the setup program.
3. The program files copied to your hard drive and Assistant I is configured in the Windows start button. This installation of Assistant I is complete.

The configuration of HiPath HG 1500 with the help of Assistant I is described in the chapter "Administration with Assistant I".

Initial startup via the first LAN interface

1. If the default IP address "10.144.233.63" is configured on HiPath HG 1500 (basic factory setting, default CDB), then a special mechanism is activated to simplify startup.
   If the board containing this CDB is put into service, then it sends prompts to the LAN to request an IP address.
   If an IP address is returned in answer to this prompt, then the board is put into service with this address and can be used for the administration of the PC that responded to the prompt.
   The HiPath HG 1500 can be assigned an IP address with a static entry in the administration PC's ARP table.
   To this end, the command
   `arp -s ipadresse macadresse` is entered in an MSDOS command window (see also -> arp page 160).
   Example of format:
   `arp -s 192.168.100.245 08-00-06-0f-ec-04`
   The MAC address of the board is indicated on a sticker attached to the board.

2. Using the new IP address, start a ping command to HiPath HG 1500 in the MSDOS command window. You can proceed with administration if HiPath HG 1500 responds correctly to the ping command.

These settings are only temporary and are only permanently saved to the board with an entry in the CDB.
Security information:
The mechanism described above can be used by every PC in the LAN as long as no CDB was transferred to the board!

Remote startup (service center)

Depending on the administrative procedures performed by the Hicom system's service technician, an ISDN peer and the ISDN2 interface can be generated during initial HiPath HG 1500 booting for the purpose of startup by the service center. The IP address 10.186.237.64 is also enabled for configuration in this case. This access can only be created during startup. In accordance with the service concept selected, this entry must, where applicable, be removed.

Initial startup via a serial interface

The Admin PC should only be started up for the first time via the serial interface if it cannot be started up via the LAN interface.

Prerequisites:

The SLIP connection (Dial-Up Networking) must be installed in accordance with the operating system used.

1. Connect the serial interface cable (S30122-X5468-X3).

2. Install Dial-Up Networking and configure as described below.
3. Set the IP address of Admin PC (SLIP) "1.0.0.2" in Dial-Up Networking.
4. Set up a connection to HiPath HG 1500 by means of Dial-Up Networking.

Preparing the Admin PC with WIN 95 Version A or B

Winsock2 must be updated if Windows 95 is installed. This Windows Socket 2 update is available on the Microsoft homepage.

Check whether Dial-Up Networking is already installed:

Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**. If there is a check mark next to Dial-Up Networking, it is already installed. In this case, you can configure Dial-Up Networking. If it is not marked, it must first be installed.

Installing Dial-Up Networking:

1. Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**.
2. Click **Dial-Up Networking** and confirm with OK.
3. Insert the Windows CD in the CD-ROM drive. Dial-Up Networking is installed.

Dial-Up Networking configuration:

1. Double-click **My Computer/Dial-Up Networking.**
2. The wizard for configuring Dial-Up Networking starts up. Click **Next**.
3. Click the option **Don't detect my modem, I will select it from a list.**
In the next window, select **Standard 9600 bps modem** as the default modem type and enter a COM port in the ensuing window (e.g. COM1).
The modem is installed.
4. Enter the country, prefix and **Tone dialing** as the dialing mode. The modem is configured.
5. Finally, name the new dial-up connection (e.g. "SLIP to HiPath HG 1500") and enter a "1" in the **Phone Number** field in the next window. The new connection is created when you complete the procedure by pressing **Next** and **Finish**.
6. Scripting support must then be installed to enable the definition of SLIP properties. The installation of scripting support depends on the Windows version used:
   Windows 95 A or B Update version:
   Insert the Windows CD in the CD-ROM drive, open Windows Explorer and go to the CD directory "...\Admin\Apptools\DScript\SLIP". Activate "Script support for Dial-Up Networking."Scripting support is downloaded from the CD.
   Windows 95 A or B OEM version:
   Open Windows Explorer and go to the LAN Bridge directory "...\LAN Bridge\SLIP dfue\Neu\" on your hard disk. Right-click the file "Rnaplus.inf" and select **Install**. Click **OK** in the ensuing window and then

enter the same directory as before "...\LAN Bridge\SLIP dfue\Neu\" for the required file "cis.scp."Confirm with OK; scripting support is installed.

7. Define the dial-up connection properties:
Select the new dial-up connection created via **My Computer/Dial-Up Networking/SLIP to** HiPath HG 1500. Use the right mouse button to open the **Properties** option. Click **Server Types** and select **SLIP: Unix Connection.** Deactivate the option **Log on to network**. Click **TCP-/IP Settings** and enter the IP address "1.0.0.2". Deactivate the options **IP header compression** and **Use default gateway on remote network**. Confirm the operation as often as required with OK.

8. Open the window "Dial-Up Adapter Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/Dial-Up Adapter**.
"TCP/IP -> Communications Driver" should only be
marked in the **Bindings** tab.

9. Open the window "TCP/IP Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/TCP/IP**. The option **Obtain an IP address automatically** must be marked in the **IP Address** tab. Otherwise, the default settings can be retained.

10. Restart Windows.
If you initiate the dial-up connection by double-clicking **My Computer/ Dial-Up Networking/SLIP to** HiPath HG 1500, an icon will be created in the task bar when you confirm the logon window and the connection will remain active in the background.

Preparing the Admin PC with WIN 95 Version C

Winsock2 must be updated if Windows 95 is installed. This Windows Socket 2 update is available on the Microsoft homepage.

Check whether Dial-Up Networking is already installed:

Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**. If there is a check mark next to Dial-Up Networking, it is already installed. In this case, you can configure Dial-Up Networking. If it is not marked, it must first be installed.

Installing Dial-Up Networking:

1. Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**.
2. Click **Dial-Up Networking** and confirm with OK.
3. Insert the Windows CD in the CD-ROM drive. Dial-Up Networking is installed.

Dial-Up Networking configuration:

1. Double-click **My Computer/Dial-Up Networking/Make New Connection.**
2. The wizard for configuring Dial-Up Networking starts up.
   Click **Next**.
3. Enter a name for the new dial-up connection (e.g. "SLIP to HiPath HG 1500") and select **Standard 9600 bps modem** as the modem. Confirm with **Next**
4. Enter the prefix, enter "1" in the **Telephone number** field and select the country code. The new connection is set up after you confirm with **Next** and **Finish**.
5. Define the dial-up connection properties:
   Select the new dial-up connection created via **My Computer/Dial-Up Networking/SLIP to** HiPath HG 1500. Use the right mouse button to open the **Properties** option. Click **Server Types** and select **SLIP: Unix Connection.** Deactivate the option **Log on to network**. Click **TCP-/IP Settings** and enter the IP address "1.0.0.2". Deactivate the options **IP header compression** and **Use default gateway on remote network**. Confirm the operation as often as required with OK.
6. Open the window "Dial-Up Adapter Properties" by pressing **Properties under** Start/Settings/Control Panel/Network/Dial-Up Adapter.
   "TCP/IP -> Communications Driver" should only be marked in the **Bindings** tab.

7. Open the window "TCP/IP Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/TCP/IP**. The option **Obtain an IP address automatically** must be marked in the **IP Address** tab. Otherwise, the default settings can be retained.

8. Restart Windows.
   If you initiate the dial-up connection by double-clicking **My Computer/Dial-Up Networking/SLIP to** HiPath HG 1500, an icon will be created in the task bar when you confirm the logon window and the connection will remain active in the background.

Preparing the Admin PC with WIN 98

Check whether Dial-Up Networking is already installed:

Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**. In general, Dial-Up Networking is pre-installed in Windows 98. In this case, you can configure Dial-Up Networking. If it is not marked, it must first be installed.

Installing Dial-Up Networking:

1. Click **Start/Settings/Control Panel/Add/Remove Programs/Windows Setup/Connections/Details**.
2. Click **Dial-Up Networking** and confirm with OK.
3. Insert the Windows CD in the CD-ROM drive. Dial-Up Networking is installed.

Dial-Up Networking configuration:

1. Double-click **My Computer/Dial-Up Networking.**
2. The wizard for configuring Dial-Up Networking starts up.
   Click **Next**.
3. Click the option **Don’t detect my modem, I will select it from a list.** In the next window, select **Standard 9600 bps modem** as the default modem type and enter a COM port in the ensuing window (e.g. COM1).
   The modem is installed.
4. Enter the country, prefix and **Tone dialing** as the dialing mode. The modem is configured.
5. Double-click **Make New Connection**. Give the connection a name, e.g: "SLIP to HiPath HG 1500". Enter the number "1" for the phone number in the next window. The new connection is created when you complete the procedure by pressing **Next** and **Finish**.
6. Define the dial-up connection properties:
   Select the new dial-up connection created via **My Computer/Dial-Up Networking/SLIP to** HiPath HG 1500. Use the right mouse button to

open the Properties option. Click "Server Types" and select **SLIP: Unix Connection**. Deactivate the option **Log on to network**. Click TCP-/IP Settings and enter the IP address "1.0.0.2". Deactivate the options **IP header compression** and **Use default gateway on remote network**. Confirm the operation as often as required with OK.

7. Open the window "Dial-Up Adapter Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/Dial-Up Adapter**. "TCP/IP -> Communications Driver" should only be marked in the **Bindings** tab.

8. Open the window "TCP/IP Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/TCP/IP**. The option **Obtain an IP address automatically** must be marked in the **IP Address** tab. Otherwise, the default settings can be retained.

9. Restart Windows.
   If you initiate the dial-up connection by double-clicking **My Computer/ Dial-Up Networking/SLIP to** HiPath HG 1500, an icon will be created in the task bar when you confirm the logon window and the connection will remain active in the background.

Preparing the Admin PC with NT4.0

Check whether Dial-Up Networking is already installed:

Click the **My Computer** icon on your desktop and check if there is an icon for Dial-Up Networking. In general, Dial-Up Networking is pre-installed in Windows NT. If there is no Dial-Up Networking available, it must be installed.

Installing Dial-Up Networking:

1. Click **Start/Settings/Control Panel/Network/Services**.
2. Insert the **Remote Access Service**.
3. Insert the Windows CD in the CD-ROM drive. Dial-Up Networking is installed.

Dial-Up Networking configuration:

1. Double-click **My Computer/Dial-Up Networking.**
2. The wizard for configuring Dial-Up Networking starts up.
   Click **Install** followed by **Yes**.
3. Click the option **Don’t detect my modem, I will select it from a list.** In the next window, select **Standard 9600 bps modem** as the default modem type and enter a COM port in the ensuing window (e.g. COM1).
   Click **Next**.
4. Enter the country, prefix and **Tone dialing** as the dialing mode. The modem is configured.
5. Click Finish. The default settings in the ensuing windows "Add RAS Device" and "RAS Setup" should be retained. To do this, click **OK** or **Next**.
6. Double-click **My Computer/Dial-Up Networking** once more.
7. Confirm the message "Phonebook empty" with **OK**. The window "New Phonebook Entry Wizard" opens.“
8. Enter a name to the new dial-up connection (e.g. "SLIP to HiPath HG 1500") and activate the third option (**The Non-Windows NT Server...**) in the next window. Enter a "1" in the **Phone Number** field in the next window and activate the options **SLIP (Serial Line Internet Protocol)** and **Use a terminal window**. Confirm with **Next**.
9. The window "Name Server Addresses.“Leave the two IP addresses as "0.0.0.0". The new connection is created when you complete the procedure by pressing **Next** and **Finish.**
10. Define the dial-up connection properties:
    Select the dial-up connection just created by means of **My Computer/ Dial-Up Networking/SLIP to HiPath HG 1500**. Click **Next** and select

Entry and modem properties. Select **SLIP Internet** as the dial-up server and activate the option **TCP/IP**. Click **TCP/IP Settings** and enter the IP address "1.0.0.2" in the ensuing window. Deactivate the options **Force IP header compression** and **Use default gateway on remote network**. Otherwise, the default settings can be retained. Confirm with OK.

11. Open the window "Dial-Up Adapter Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/Dial-Up Adapter**. "TCP/IP -> Communications Driver" should only be marked in the **Bindings** tab.

12. Open the window "TCP/IP Properties" by pressing **Properties** under **Start/Settings/Control Panel/Network/TCP/IP**. The option **Obtain an IP address automatically** must be marked in the **IP Address** tab. Otherwise, the default settings can be retained.

13. Restart Windows.
    If you initiate the "SLIP to HiPath HG 1500" dial-up connection by double-clicking **My Computer/Dial-Up Networking** and you can close the "Connection Complete" window with **OK**. An icon will be created in the task bar when you confirm the logon window and the connection will remain active in the background. You can display information about the current connection by clicking this icon in the task bar.

Preparing the Admin PC with WIN 2000

Check whether the standard 9600bps modem is installed:

1. Click Start/Settings/Control Panel
2. Click Phone and Modem Options
3. If "Standard 9600 bps modem" is not listed, click "Add“
4. Activate the "Detect Modem" and "Next“
5. Select "Standard 9600 bps modem" from the list and click "Next“
6. Select the required COM interface and click "Next" followed by "Finish“

The modem is configured.

Configuring Dial-Up Networking

1. Click Start/Settings/Network and Dial-up Connections/Make New Connection.
2. The network connection wizard opens. Select "Dial-up to private network.“
3. Select the standard 9600 bps modem from the list and click "Next“
4. Enter "1" as the call number, for example, and press "Next“
5. Select "For all users" and "Next“
6. Enter a name, e.g. "SLIP to HiPath HG 1500" and press "Finish“
7. Click "Properties“
8. Select "SLIP: Unix Connection" under "Type of dial-up server I am calling" in the "Network" tab. Activate "TCP/IP" as the protocol and "Properties“
9. Select "Use following IP address" and enter "1.0.0.2".
10. Under "Advanced->General" deactivate the check box for "Use default gateway on remote network" and "Use IP header compression"
11. Confirm all inputs.

The dial-up network is now configured.

For the administration of HiPath HG 1500, you can now set up a connection via the serial interface with the board via "Start/Settings/Network and Dial-up Connections/SLIP to HiPath HG 1500".

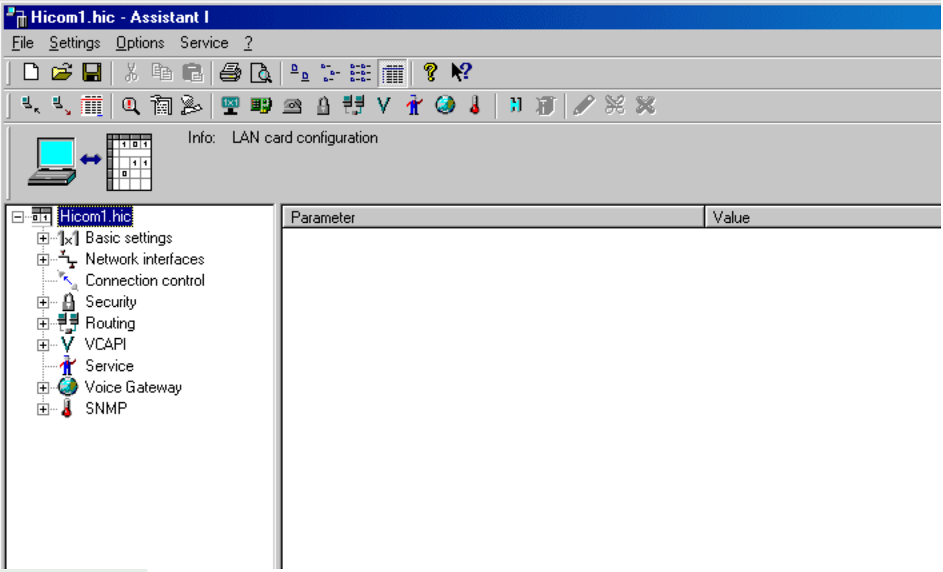
Administration with Assistant I

You can configure HiPath HG 1500 from your PC and modify the configuration settings with the help of the Assistant I administration program. You will find descriptions of the individual steps in the context-sensitive Help which you can open by pressing the F1 key at the relevant location.

Starting Assistant I

Assistant I is started via the start bar in the Windows operating system.

A user name and password are required for starting the Assistant I. The password should only be supplied to HiPath HG 1500 administrators.



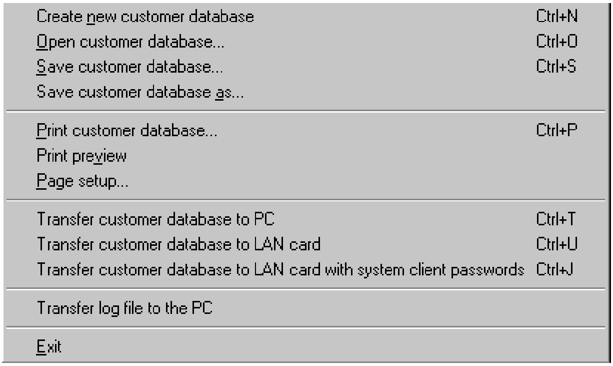
Tool and menu bar

The contents of the menu bar and the meaning of the icons in the toolbar are described below.

Menu bar

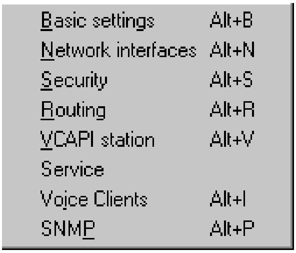
The menu bar comprises a number of commands. Left-clicking one of these main menu commands opens a pull-down menu containing further commands.

"File" menu


Create new customer database Ctrl+N
Open customer database... Ctrl+O
Save customer database... Ctrl+S
Save customer database as...
Print customer database... Ctrl+P
Print preview
Page setup...
Transfer customer database to PC Ctrl+T
Transfer customer database to LAN card Ctrl+U
Transfer customer database to LAN card with system client passwords Ctrl+J
Transfer log file to the PC
Exit

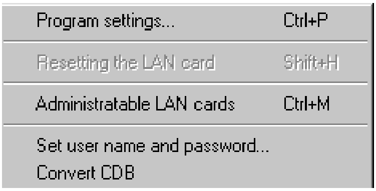
see → 33
see → 33
see → 34
see → 34
see → 34
see → 34
see → 34
see → 34
see → 35
see → 35
see → 35
see → 35

"Settings" menu



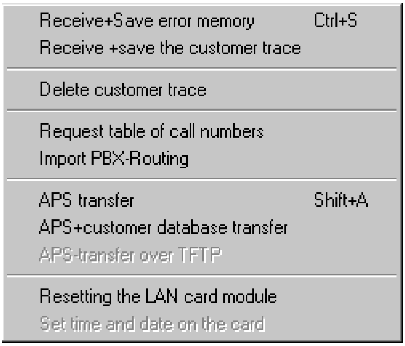
see → 36
see → 40
see → 45
see → 46
see → 49
see → 57
see → 59
see → 62
see → 66

"Options" menu



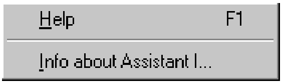
Program settings...	Ctrl+P	see → 68
Resetting the LAN card	Shift+H	see → 68
Administratable LAN cards	Ctrl+M	see → 68
Set user name and password...		see → 68
Convert CDB		see → 68

"Service" menu



Receive+Save error memory	Ctrl+S	see → 69
Receive +save the customer trace		see → 69
Delete customer trace		see → 69
Request table of call numbers		see → 69
Import PBX-Routing		see → 69
APS transfer	Shift+A	see → 69
APS+customer database transfer		see → 69
APS-transfer over TFTP		see → 70
Resetting the LAN card module		see → 70
Set time and date on the card		see → 70

"?" (Help) menu



Help	F1
Info about Assistant I...	

Toolbar

You can use the toolbar to directly activate important functions. These functions are also available in the menu bar but can be activated more quickly from the toolbar. The icons that relate to Assistant I are listed here.

Create new customer database

Open customer database

Save customer database

Print customer database

Print preview

Transfer customer database to PC

Transfer customer database to HiPath HG 1500

Transfer log file to the PC

Receive+Save error memory

Retrieve + Save the customer trace

Delete customer trace

Editing the basic settings

Editing the network interfaces

Editing the connection control

Editing the security parameters

Editing the routing settings

Editing the vCAPI stations

Editing the service settings

Editing the system clients

Editing the SNMP settings

Administrable HiPath HG 1500 cards

Resetting the HiPath HG 1500 module

New

✂ Change

❌ Delete

Initial generation

Prerequisites for initial generation

Date required:

- IP address and sub-network mask for HiPath HG 1500
- IP address and sub-network for the Admin PC
- Call number of the HiPath HG 1500 router
- Station name, IP address and call number of the HiPath HG 1500 client (system clients, H323 clients and vCAPI clients)

In the case of Hicom 150 H, the call numbers used in HiPath HG 1500 must have been assigned in the Hicom (e.g. by the Hicom system administrator) and sorted by system clients and all other stations (S_0 stations, e.g. VCAPI, router, H.323 etc.).
If multiple system networking via IP is activated, then trunks must be configured for this in the Hicom. The B channels reserved for this are then unavailable for other services on the HiPath HG 1500 (routing, system clients, VCAPI, etc.
The upper limit of available B channels is restricted by the two parameters under "Service" see → 59.

- The use of more than two B channels by HiPath HG 1500 means that a license number is required to enable the other channels.

The following settings must be made beforehand in HiPath HG 1500 to allow the data to be loaded from Assistant I:

1. Start Assistant I.
2. Enter the current Hicom 150 E Office passwords in the "User Name“ and "Password" fields to log onto Assistant I. The user name and password can only be modified in Hicom.
3. Select **Administratable** HiPath HG 1500 cards in the **Options** menu.
4. Select HiPath HG 1500 **peers** in the left column and click the "New" icon in the toolbar.
5. Enter the HiPath HG 1500 name in the next window, for example "LAN", and confirm the entry with **OK**.
6. In the left column, select the entry that you have just made, for example "LAN", and enter the IP address of HiPath HG 1500 in the right column under "➡ IP address:". Enter the IP address that was assigned to the board by the administration PC here, see → 14.
7. Select **Transfer customer database to PC** in the **File** menu.

8. Select the previously defined HiPath HG 1500 name (for example "LAN") in the next window and confirm the selection with **OK**. The default data of HiPath HG 1500 is transferred now to the PC.

As of Hicom 150 H V1.0, the call numbers preset in Hicom can be accessed directly via a selection box whenever an internal Hicom call number must be entered. This table is read out of Hicom every time "Transfer customer database to PC" is selected.
The call numbers that were already assigned in the CDB are no longer displayed here.

Initial generation settings

A customer database containing the default values of HiPath HG 1500 was transferred to Assistant I.

1. Select **Service** in the **Settings** menu. Set the number of B channels purchased with HiPath HG 1500 in the right column under "➡ Licensed B channels:" (only even values are allowed). A license number is required if this value is modified. This is queried when downloading the CDB to HiPath HG 1500.
   The number of B channels actually used can be restricted under "➡ Maximum number of usable B channels" in the same menu. This value can be set in increments of one.
   Select **Basic settings** in the **Settings** menu. Set the number of B channels that can be used simultaneously for routing in the right column under "➡ Number of B channels that can be used by routers".

2. Enter an internal station number in the right column under "➡ HiPath HG 1500 login number:". This internal station number is automatically dialed after the system has been reset or the CDB has been loaded to HiPath HG 1500. You must ensure that there are sufficient unassigned call numbers. The call number of the routing port is displayed in the caller list of the logged on station. If not, the call number is not available in Hicom (check unassigned call numbers in Hicom, call numbers must be entered in the numbering scheme but must not be assigned to boards installed on the hardware side).
   The logon number is used for configuration diagnostics and can be removed once startup has been successfully completed.

3. Double-click **IP address list for configuration** in the left column and configure the IP address of the Admin PC (PC with Assistant I) using the "New" icon in the toolbar.
   Entire networks can be enabled here for administration (e.g. the service center for remote administration).

4. Click **Router call number** in the left column. In the right column under "➡ Router call number:", enter the call number that can be used to dial HiPath HG 1500 from a remote location. All applications that use this router functionality can be remotely accessed under this one DID number. The responsibility for the administration or assignment of the B channels is assumed by HiPath HG 1500.
   This call number is displayed in the device’s caller list after startup with the login number.
   External routing partners that use the protocols V.34 or V.110 must use different call numbers:
   these are configured as **DID numbers** for the **ISDN peers**.

5. Select **Network interfaces** in the **Settings** menu. Double-click **Network interfaces** in the left column and set the active network interfaces (for example LAN and ISDN 1/2/3, but a minimum of LAN).

Enter the IP address (IP address of HiPath HG 1500) and the IP network mask (network class A, B or C) under **LAN** (depends on the customer network).

Enter the IP address on your WAN side under **ISDN1**. The IP address on the WAN side must be located in the same network as the IP address of the ISDN peer (the ISDN settings are only required for a routing, teleworker station, Internet access, remote access).

6. Select Routing in the **Settings** menu. Double-click **ISDN peer** in the left column and configure a new ISDN peer using the "New" icon in the toolbar. Select the **Call number list** command and enter the call number of the ISDN station by means of the "New" icon in the toolbar. Click the call number and define the call direction under "➡ Call direction:" Click the ISDN peer and configure the peer parameters, for example the IP address, the B channels, the protocol (V.34 for analog and V.110 for digital modems) or configure a DID number if required.
7. Select **Security** in the **Settings** menu and check whether the "IP firewall", "MAC verification" and "IPX firewall" parameters are deactivated. Security information: the firewall is deactivated here to simplify startup. Various security settings should be configured and activated when dialing in for the first time to ensure secure operation.
8. Open the **File** menu and select **Transfer customer database to** HiPath HG 1500. Select the previously defined HiPath HG 1500 name (for example "LAN") in the next window and confirm the selection with **OK**. The data is transferred now to HiPath HG 1500. The HiPath HG 1500 performs a board reset when the data has been initially retrieved.
9. Basic board operation can be tested from any computer in the first LAN using the IP protocol with the PING test program and the IP address of HiPath HG 1500.
   As of this point, further configuration can be performed via the first LAN interface irrespective of the access for initial startup (e.g. SLIP). It may be necessary for this to reset the IP address of the Admin PC to the original value.

Explanation of the menu functions

This section provides additional information about the individual commands contained in the menu structure described in the previous section. The information provided partly corresponds to the Assistant I Online Help.

"File" menu

Create new customer database

This command is used to create a new customer database in the main memory of the Admin PC. Since you can only process one CDB at a time, you have the option of saving a previously loaded data record.

A new CDB does not contain any data structures that are dependent on the customer profile. Consequently, no ISDN peers, VCAPI stations, IP/IPX/ MAC firewall, etc. are defined.

User-defined default values, for example, can be entered when these data records are configured (see the "Settings" command). These are saved in the Hlb_Cfg.def configuration file in the application’s HOME directory.

The basic settings (e.g. IP address, first LAN interface) are preconfigured and must be set by the customer to suit the appropriate environment.

A CDB only contains configuration data for a HiPath HG 1500 board. Names and IP addresses where the HiPath HG 1500 board to be administered can be reached are set under "Administratable HiPath HG 1500". These are saved in a separate configuration file in the HiPath HG 1500 application’s HOME directory.

Open customer database

You can use this command to load a preconfigured or saved customer database from the Admin PC hard disk (or from another data medium) to the main memory. Previously processed data records can be saved first. A customer database file has the "hic" extension (for Hicom).

Data consistency is checked during the loading operation.

Save customer database

You can use this command to save an edited customer database to a data medium.

Save customer database as...

This command allows you to save the customer database to a data medium under a selected name and path. The default (and recommended) extension is "*.hic."

Print customer database

You can use this command to print the customer database. A pop-up window in which you can select the printer and print options appears if you select this command.

The CDB printout is protected against unauthorized access.

Print preview

You can use this command to preview the customer database before it is printed. You can also configure the printer, the printer properties and the paper size using this command.

Page setup...

You can use this menu item to open the context menu for operating system printer settings. You can set the printer, its properties and the paper size here.

Transfer customer database to PC

You can use this command to load a customer database from a HiPath HG 1500 to the Admin PC. A Hicom configuration already stored in the PC main memory can be saved first. This must be followed by the selection of a HiPath HG 1500 peer (configurable under "Administratable HiPath HG 1500") from a list. The name is only queried when the board is accessed for the first time. This selection remains active until the temporarily used HiPath HG 1500 is reset. The name of the currently used HiPath HG 1500 is displayed in the status line of the program window. The consistency of the board configuration data is checked once the load operation has been completed.

Transfer customer database to HiPath HG 1500

You can use this command to transfer an edited or newly created customer database to HiPath HG 1500. If a board has already been selected (e.g. by previously loading a customer database from the board to the Admin PC), this is accepted as a destination for the current CDB transfer.

Transfer the customer database to HiPath HG 1500 with system client passwords

You can use this command to transfer an edited or newly created customer database to HiPath HG 1500. If a board has already been selected (e.g. by previously loading a customer database from the board to the Admin PC), this is accepted as a destination for the current CDB transfer. All system client passwords are also transferred to HiPath HG 1500.

All system client users can change their password via the client. The system client passwords are a component of the CDB, but are only overwritten on HiPath HG 1500 if this option is used or if individual passwords were specifically modified with Assistant I. The passwords can be set to a defined value with this option. The client users must be informed of this.

Transfer log file to the PC

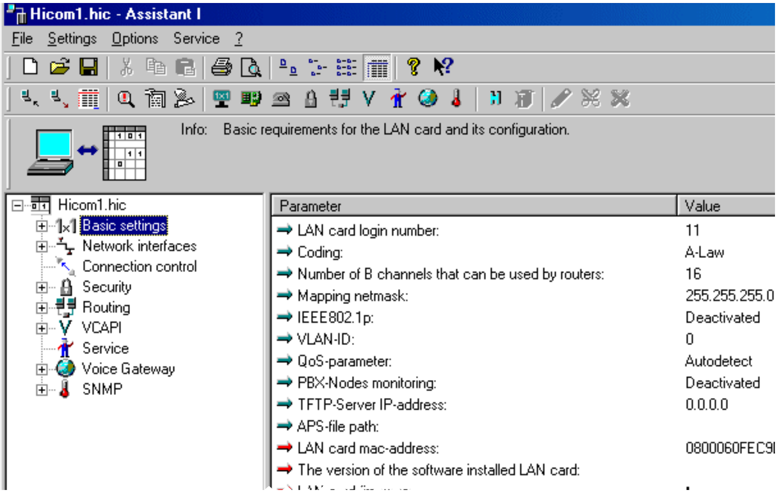
This command loads the log file to the PC and saves the loaded log file.

Exit

This command terminates Assistant I and, where applicable, prompts you to save any unsaved data.

"Settings" menu

Basic settings



Info: Basic requirements for the LAN card and its configuration.

Parameter	Value
LAN card login number:	11
Coding:	A-Law
Number of B channels that can be used by routers:	16
Mapping netmask:	255.255.255.0
IEEE802.1p:	Deactivated
VLAN-ID:	0
QoS-parameter:	Autodetect
PBX-Nodes monitoring:	Deactivated
TFTP-Server IP-address:	0.0.0.0
APS-file path:	
LAN card mac-address:	0800060FEC9
The version of the software installed LAN card:	

This command configures the basic settings. This data only exists once within the CDB. The following parameters are assigned directly to the "Basic settings" category:

➡ HiPath HG 1500 login number:

An internal station number is entered here. This station is automatically called every time a VCAPI client is started up or restarted during initial startup and after every HiPath HG 1500 reset. The caller list contains the router number, call numbers or station names of the VCAPI client successfully logged in. This service is used for configuration diagnostics and can be removed once startup has been successfully completed.

➡ Coding:

This button affects the language coding on the ISDN side.

➡ Number of B channels that can be used by routers:

HiPath HG 1500 can use a maximum of 16 B channels. A customer can license a certain number of B channels. A certain number of these channels, in turn, can be used for routing. This is particularly useful, for example, if a minimum number of B channels must always be available for HiPath HG 1500 clients (VCAPI, H.323, system clients, etc.). Four channels can be assigned to the router, for example, if six channels are licensed. This ensures that two channels are always available to HiPath HG 1500 clients.

➡ Mapping Netmask

Specifies the network mask that defines the host part for address mapping, see → 106 IP address mapping.

➡ IEEE802.1p

The Ethernet format can be set with this parameter. The parameter only works on packets that are sent from the board (deactivated by default).
Automatic detection is active for all packets that are sent to the board, see → 83, QoS.

➡ VLAN ID

Whenever 802.1p is used, VLAN ID 0 is transmitted in the header. This ID causes problems with a certain number of switches (e.g. Cisco). This is why the VLAN ID can be administered

Default value: 0

Value range: 0 ... 4094 (0xFFE)

➡ QoS procedures

Defines the Quality of Service procedure used by HiPath HG 1500 to set precedence for IP packets on the basis of the IP header information (ToS field, Type of Service).
The values available are DiffServ, IP precedence or Autodetect (default). If the setting "Autodetect" is selected, DiffServ and IP precedence are accepted and duly evaluated for routing, see → 83 QoS.

➡ PBX node monitoring

For HG1500 V1.x:
This parameter activates monitoring between networked PBX/HiPath nodes.
Warning: this parameter must be set identically in all nodes.

In HG1500 V2.0 and later, this parameter is set on a node-specific basis under Voice Gateway->PBX Node.

➡ IP address of the TFTP server

Specifies the IP address of the TFTP server.

➡ Path and file name of the APS file

Specifies the path and file name of the APS file on the TFTP server.

➡ MAC address of the board

The MAC address of the board (LAN interface) is displayed here.

➡ LAN board software (HiPath HG 1500):

The current version of the software loaded in HiPath HG 1500 is displayed here.

➡ LAN board firmware:

Specifies the current firmware

IP address list for configuration

Up to 10 IP addresses (including network addresses) can be defined under this category. These specify the Admin PCs that can be used for configuring HiPath HG 1500.
Entire networks can be enabled here for administration (e.g. the service center for remote administration).

> This list must always be kept up-to-date and should only contain necessary entries.

Router call number

➡ Router call number:

The Hicom DID number at which HiPath HG 1500 can be contacted from an external terminal is specified here. All applications that use the router functionality can be accessed remotely using this one DID number. The responsibility for the administration or the assignment of the B channels is assumed by HiPath HG 1500.

This call number should be displayed in the caller list of the logged on station once initial startup has been concluded.

Script processing

A logon script must be processed for accessing some Internet providers. PAP or CHAP is usually required (see → 50, "Settings - Routing - ISDN peer" command).

This step involves various parameters, such as USER,
LOGIN, HOST and PASSWORD.

The mask is structured in such a way that the necessary characters must be entered in the parameter fields.

Processing can be deactivated. This script is available once in the customer data memory and is valid for all ISDN peers who have activated script processing.

Example:

Requested script:

HOST: ERT005

USER: KJUMBERT

PASSWORD: 34lk98UF5

The following characters must now be entered in the mask:

- ID 1: HOST:ERT005
- ID 2: USER:KJUMBERT
- Password: PASSWORD 34lk98uF5

QoS order of priority

The HiPath HG 1500 uses four priority classes to assign levels of precedence (descending) to its own IP data traffic. The values can be set here. In general, the default values do not need to be changed, see → 83 QoS.

- Voice Payload:
  H.323 packets which contain voice information.
- Call Signaling:
  are needed for connection setup (e.g.H.323).
- Fax Modem Payload:
  e.g. for fax data for IP networking.
- Network Control:
  e.g. SNMP traps.

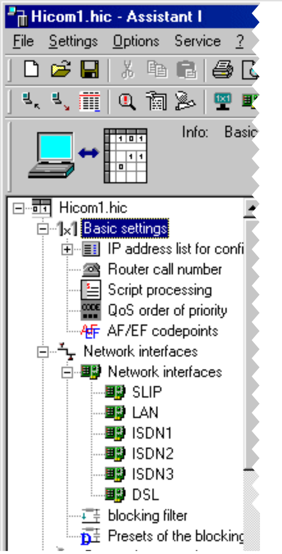
The values for the individual classes are selected from the list of "AE/EF codepoints".

AE/EF codepoints

The values that define the various priorities are defined here. The hex value to be entered corresponds to the ToS field (Type of Service) in the IP header. The two lower bits are always zero; consequently, not all values are permitted here (only the upper 6 bits are evaluated). In general, the default values do not need to be changed, see → 83 QoS.

The value "0" is permitted, but means that all "normal" unmarked packets (ToS field=0) are transported in the corresponding class.

Network interfaces



HiPath HG 1500 has a maximum of six network interfaces. These include the first LAN interface (LAN) which is connected to the company network, ISDN interface ISDN1, ISDN interface ISDN2 and ISDN3 interface used to access the Internet with NAT/SUA (ISDN3) and the DSL/LAN2 interface as a fully functional additional 10BT LAN interface, supported by QoS and firewalls in the IP/IPX router. Your Siemens technician must perform the initial startup of HiPath HG 1500 if the SLIP interface is used.

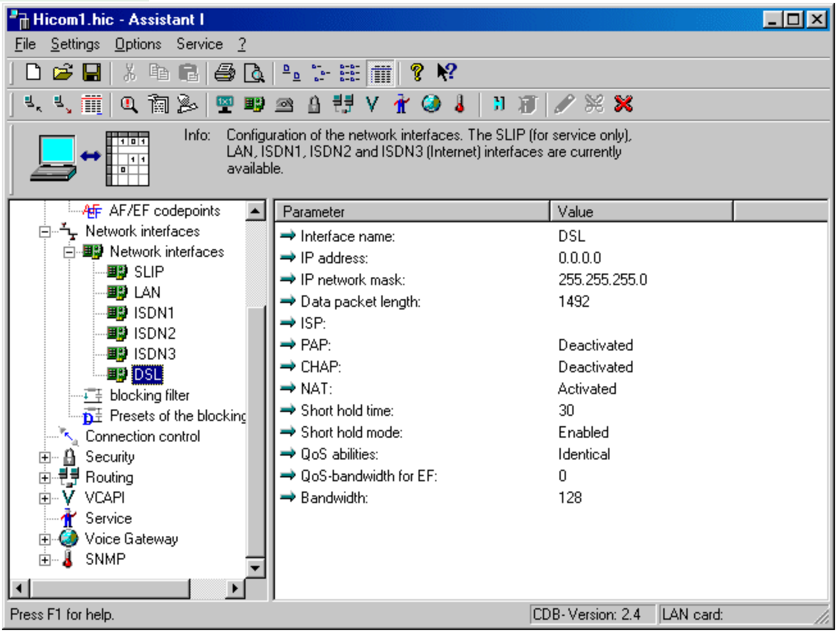
The configuration of a valid protocol address (IP and/or IPX) activates the protocol stack for the interface. The "Network interfaces" main category is only directly assigned the following parameters:

➡ Active network interfaces:

The following five network interfaces:

LAN, ISDN1, ISDN2, ISDN3 and DSL/LAN2

can be activated or deactivated. All options for common activation and deactivation are provided.
LAN2 and DSL interface can be selected via the selection box in the case of LAN2.



Info: Configuration of the network interfaces. The SLIP (for service only), LAN, ISDN1, ISDN2 and ISDN3 (Internet) interfaces are currently available.

Parameter	Value
Interface name:	DSL
IP address:	0.0.0.0
IP network mask:	255.255.255.0
Data packet length:	1492
ISP:	
PAP:	Deactivated
CHAP:	Deactivated
NAT:	Activated
Short hold time:	30
Short hold mode:	Enabled
QoS abilities:	Identical
QoS-bandwidth for EF:	0
Bandwidth:	128

Press F1 for help. CDB- Version: 2.4 LAN card:

Example for the configuration of a second LAN interface

Network interfaces

➡ SLIP:

The SLIP interface may be required by your service technician for the initial startup of HiPath HG 1500.

ISDN1, ISDN2, LAN and DSL/LAN2 have the following parameters:

➡ Interface name:

Two options are available under LAN2, namely DSL and LAN2. DSL is set by default.

➡ IP address:

This is the IP address of the interface. Only addresses from class A, B or C networks are permitted. Addresses must be unique both within the three interfaces and also with regard to the IP addresses of the ISDN peer.

Class A networks:
nnnnnnn . hhhhhhhh . hhhhhhhh . hhhhhhhh
Standard network mask: 255.0.0.0

Class B networks:
nnnnnn . nnnnnnnn . hhhhhhhh . hhhhhhhh
Standard network mask: 255.255.0.0

Class C networks:
nnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh
Standard network mask: 255.255.255.0

The following applies: n = network, h = host

➡ IP network mask:

The network mask is used for creating subnetworks (see → 162). In this way, a class B address in which bits 2 to 15 normally identify the network and bits 16 to 31 identify the workstation, can use network mask 255.255.240.0 to lead to a number of subnetworks that are only recognized within the company network structure. The above network mask shifts the separation between network bits and host bits to the third byte so that bits 16 to 19 are now also used for the network ID, while only bits 20 to 31 now describe the workstation. This procedure offers the advantage of clearly structuring a company network and simplifying maintenance. Smaller companies often only have a class C address (assigned by the IEFT or authorized national institutes).
If the company comprises a number of locally separate offices, these must be linked by WAN connections (wide area network). This type of task is performed by a router but router technology is based on the connection of different networks. A sub-network mask can be used to divide up the C class address into a sub-network to provide every com-

pany branch with a separate IP network (despite only one official IP address). This redistribution of bits only applies in internal company networks. The company still only has one Internet access class C network.

➡ Data packet length:

This describes the maximum packet length in bytes for both the IP as well as the IPX protocol. The value can be within the range of 500 to 1500.
Only 1492 bytes are permitted in DSL mode.

➡ IPX network number:

An IPX address comprises an eight-digit hexadecimal number for the network ID and a 12-digit hexadecimal number which references the workstation (the digit specification must be observed). The network number may not accept the values 0x00000000 or 0xFFFFFFFF. In addition, the network numbers of the three network interfaces must be different.

➡ IPX node:

This part of the IPX address characterizes the workstation within an IPX network. A node consists of a 12-digit (exactly) hexadecimal number. The values 0x000000000000 and 0xFFFFFFFFFFFF are not permitted.

ISDN3 is used exclusively for Internet access. NAT/SUA is used on this interface, see → 105. This interface is not designed for use of the IPX protocol.

The definition value of a new CDB is 1.1.1.1 for the IP address with the network mask 255.0.0.0. This value can be manually modified by entering another address. The use of IP address 0.0.0.0 with the network mask 255.255.255.248 is recommended when using ISDN3 interfaces.
A ping cannot be sent to an IP address via the ISDN3
interface.

NAT/SUA = Network Address Translation / Single User Access, i.e. the entire network with all released PCs is mapped to the Internet by means of an IP address that is provided by the Internet provider once the connection has been set up.

DSL/LAN2

The following additional submenus are available for DSL or LAN2 under the "Network interfaces" menu item:

➡ Provider name (for DSL):

Name of the provider

➡ PAP (for DSL):

see → 53

➡ CHAP (for DSL):

see → 54

➡ NAT (for DSL):

This parameter is used to activate or deactivate the "NAT" interface. For information on the function see → 105

➡ Short hold time (for DSL):

see → 50

➡ Short hold mode (for DSL):

see → 51

➡ QoS capabilities:

see → 53

➡ QoS bandwidth for EF:

This parameter can be used to reserve a specific percentage of the available bandwidth (configured under "Throughput rate") for the EF codepoint (EF), see → 83 QoS.

➡ Throughput rate (for DSL):

The throughput rate parameter defines the outgoing bandwidth on this interface in kBit/s necessary for using QoS rules.

The NAT flag (Network Address Translation) can be activated for the second LAN and for the DSL interface.

Blocking filter

The blocking filter allows certain services to be enabled or blocked for every network interface of individual Novell servers in a LAN with an IPX protocol.
Up to 30 entries can be created. An individual filter entry has the following parameters:

➡ Server name:

The name of the Novell server can contain up to 48 characters. A wildcard (precisely one "*") indicates all available servers. If a wildcard was selected, then the entry "All" cannot be selected under "Service". Several filters can be created for a server but the combination of server name and service must be unique.

➡ Service:

The IPX service which is to be enabled or blocked for a server. The associated server name may not be a wildcard if the entry "All" is selected.

➡ LAN filter mode

➡ ISDN1 filter mode:

➡ ISDN2 filter mode:

These parameters enable or block the IPX service for the specified Novell server(s). The default entry is "enabled" for LAN and "blocked" for ISDN1/ISDN2.

Presets of the blocking filter

➡ LAN filter mode

➡ ISDN1 filter mode:

➡ ISDN2 filter mode:

The above settings for the three filter modes are used as default values for a newly created blocking filter.

Connection control

The following parameters are used for connection control:

➡ Number redial:

Specifies the maximum number of redials prior to a successful connection setup.

➡ Pause:

Specifies the pause (in seconds) between redials.

➡ Upper threshold:

Channel bundling procedures are specific to channel capacity levels if several B channels have been enabled for the connection to an ISDN peer (without static channel bundling). This is determined by averaging the data throughput over a variable period of time. If the data throughput rate exceeds or is less than a certain limit value (which is also variable), a B channel is either additionally activated or deactivated.
The upper threshold specifies the channel capacity percentage value above which an additional B channel is activated. This value can vary between 66% and 100%. The value should always be greater than the value above the "lower threshold".

➡ Deviation duration:

This is the average time interval in seconds in which the upper threshold must be exceeded (see above) for the B channel to be activated. The parameter value can be between 3 and 20 seconds.

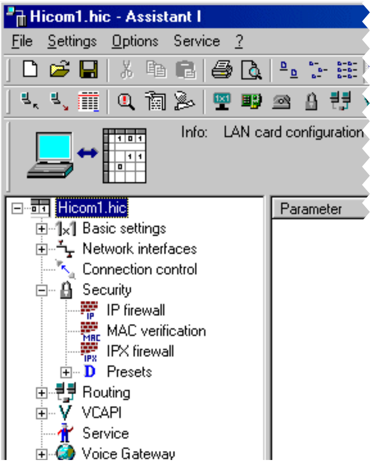
➡ Lower threshold:

Channel bundling procedures are specific to channel capacity levels if several B channels have been enabled for the connection to an ISDN peer. This is determined by averaging the data throughput over a variable period of time. If the data throughput rate exceeds or is less than a certain limit value (which is also variable), a B channel is either additionally activated or deactivated. The lower threshold specifies the channel capacity percentage value under which a B channel is deactivated. The value can be between 30 and 70% but must always be below the upper threshold (see above).

- Deviation period:

This is the average time interval in seconds in which the lower threshold must be exceeded (see above) for the B channel to be deactivated. The parameter value can be between 3 and 20 seconds.

Security



Four different security mechanisms are provided for protecting the network against unauthorized users.

- Call number verification
- IP firewall
- MAC verification
- IPX firewall

These mechanisms can be activated or deactivated with the help of the parameters named above. The mechanisms are described below.

The configuration of the firewall is not required for the ISDN3 interface. These entries are created dynamically during outgoing traffic (see → 55 "Settings - Routing - Internet for remote requests“).

➡ Call number verification:

Call number verification only checks the central call number of the router (under "Basic settings - Router call number“). It is a global function, i.e. if it is activated, calls are only answered if an ISDN peer is defined for the incoming call number (cf Routing). Calls that are transferred without the identification of the call number are rejected.
If a routing partner calls the DID number of the ISDN peer, the routing partner is identified and call number verification is not performed.

IP firewall

This category can contain up to 305 entries. This firewall affects the routing behavior of HiPath HG 1500. The table defines whether a LAN PC is permitted to send IP frames to another network via HiPath HG 1500 or whether an external computer or external network has access to the local LAN (authorization firewall). This also permits or prevents routing to the ISDN and, consequently, to remote networks.

An IP firewall entry comprises the parameters:

➡ IP address:

The IP address to which the firewall should react. The closest entry is always evaluated in the case of source and destination IP addresses: this can be a network address or an individual host. The IP routing table is used for evaluating the network mask. The address type of the entry (network or host) is transferred if a routing entry exists for an IP address.

All IP addresses are blocked by default if the IP firewall is activated.

Addresses that can be accessed from the Internet via ISDN3 must not be entered in the IP firewall. The selection is performed via the menu item: Routing->Internet.

IP addresses/networks to be transferred via ISDN3 from the HiPath HG 1500 network to the Internet must, however, be entered.

Only outgoing connections are monitored for the ISDN3 interface. Incoming packets are monitored by an automatically activated firewall (see → 55, "Settings - Routing - Internet" command).

➡ IP address of destination:

The network or the host to which a connection can be set up are specified by the destination IP address. The value "0.0.0.0" permits a connection to any IP address.

➡ IP protocol:

This setting allows the protocol of the IP package for which the firewall is to be activated to be more precisely defined. Individual port numbers can be configured for the various protocols (port firewall). The following protocols are distinguished:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- ICMP (Internet Control Message Protocol)

Security information:
The route that was enabled by the firewall can then pass through. The reverse direction is then enabled for a few minutes so that response packets can pass through the firewall. If you want initial setup to take place at the remote station, an entry must also be made for this.

Technical information:
TCP/UDP ports are used dynamically in the case of H.323 telephony (Voice over IP). It is therefore difficult to configure a static IP port firewall.

MAC verification

Up to 100 entries are permitted. Each PC in the LAN has a MAC address and an IP address as a unique feature. The combination of both is maintained in a table. The entry of this combination into a table allows the PC to set up an IP connection to HiPath HG 1500. A connection to HiPath HG 1500 cannot be set up if this combination is not available. This prevents the deceptive action of manually altering the IP address (IP address<->MAC address combination is no longer correct). The MAC firewall applies to both LAN interfaces.

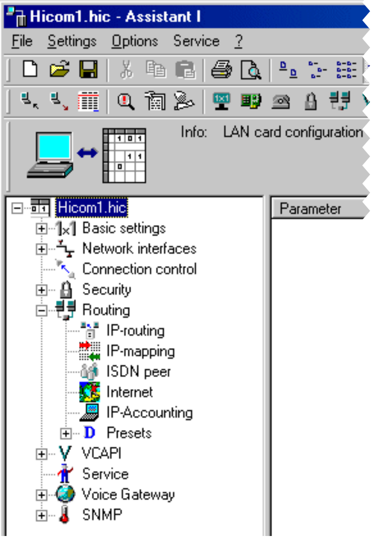
IPX firewall

Up to 100 entries are permissible under this parameter. This firewall only affects incoming or outgoing IPX packages. An incoming IPX packet comprises the node address and the network number. This combination in a table is used to verify the authorization of a peer. This packet is rejected if one of the two parameters in this combination is incorrect.

Presets for IP firewall and IPX firewall

The specified presets are transferred if a corresponding firewall entry is newly created. The routing authorizations can be preset for the IP firewall and the network number can be preset for the IPX firewall.

Routing



IP-routing

Up to 100 entries can be made under this parameter category. This category is used to define which IP network or which individual IP computer is reached via which gateway. The networks (LAN, ISDN1, ISDN2, DSL/LAN2) directly connected to the HiPath HG 1500 are recognized by the internal router. No routing entries are evaluated, therefore, for these networks. An entry contains the following parameters:

➨ IP address:

This is the IP address of the destination system or network.

➨ IP Network mask:

see → 42 and see → 162

If the network mask is assigned the value 255.255.255.255, the associated IP address is interpreted as a single system. Otherwise it is interpreted as an entire network. The IP address can be assigned the value 0.0.0.0 in this case and the gateway (see below) becomes the default gateway.

➨ Gateway:

The gateway is the next computer/router via which the desired target (described by the IP address) can be reached. If the target address describes a network (i.e. the network mask is not equal to 255.255.255.255), the gateway with the IP address 0.0.0.0 becomes the default gateway. This is necessary for all destinations that are not explicitly listed in the routing table. The values 0.0.0.0 or 255.255.255.255 are otherwise not permissible for gateways.

IP mapping

Up to 20 IP address pairs can be entered here. Based on these entries, the IP address is exchanged between the internal LAN and the (external) ISDN side in the case of routing with appropriately parameterized ISDN peers (IP mapping activated).
As a result, multiple IP networks with the same addresses, for example, can be reached if these networks are accessed via a HiPath HG 1500, see → 53, IP address mapping. The entry consists of two values:

➡ Internal IP address:

This is the IP address on the LAN side.

➡ External IP address:

This is the IP address which can be used to access the internal address from outside.

ISDN peer

Up to 70 peers can be configured. This data structure describes an ISDN peer that dials into the company network via the Hicom. The parameters directly included in this category are

➡ Name:

The name of the ISDN peer may contain up to 14 characters of any kind and must be unique.

➡ IP address:

This is the IP address of the ISDN partner. The IP address "0.0.0.0" is not permissible. The value "255.255.255.255" is used in special cases. This activates the IP protocol for this peer. The address must also be unique. In other words, it may not be used by the other peers or HiPath HG 1500 network interfaces.

➡ Node address:

This is the IPX node address of the ISDN partner. This part of the entire IPX address characterizes the workstation within an IPX network. A node consists of a 12-digit (exactly) hexadecimal number. The value 0x000000000000 is not permissible while node address 0xFFFFFFFFFFFF deactivates the IPX protocol for this peer.

➡ Short hold time:

The short-hold parameter describes the duration in seconds following which a connection is disconnected if the data transfer process inactive. The connection is set up again (visibly displayed for the user) if new data packets are transferred. This mechanism is also called background connection setup and disconnection. Costs are only incurred if the line is actually used.

➡ Short hold mode:

Activating and deactivating short-hold mode.

➡ Short hold charge pulse analysis

If this switch is activated, short hold mode is optimally controlled with regard to charge pulse analysis.

➡ B channels:

HiPath HG 1500 has a maximum of 16 B channels (licenses must be obtained for the enabling of B channels). A certain number of B channels can be reserved for routing purposes. This enables a sufficient number of B channels for other applications (for example CTI).

The B channels are assigned by means of the "Basic settings - Maximum number of B channels" parameter. It may be necessary to set the number of B channels available to a particular peer to a maximum number again. This can be performed here.

➡ System start behavior:

The option of setting up an automatic connection to a particular ISDN peer when the system is started up is available. This is done by setting the value to "Automatic connection". Connections are set up to the partners, provided that B channels are free. If too many automatic connections are defined, some of the connections may not be set up. It is, therefore, recommended not to define more autostart peers than available B channels.
This automatic system start facility is particularly useful for IPX routing since it allows data to be exchanged with remote routers.

➡ Callback:

A calling peer must transfer its call number to the ISDN connection in the D channel. If the callback feature is activated, the connection is refused by HiPath HG 1500 and the peer is called back immediately after this. This feature prevents an unauthorized peer from dialing into the network. The activation of the callback function means that the initial incoming call does not result in a connection setup. Costs are only incurred, therefore, by the calling back party.
Callback should only be programmed at both of the relevant sides to avoid loops.

➡ Script processing:

The parameters entered under the Basic settings -> Script processing menu are activated for the ISDN peer here.

The script is only executed once and is valid for the entire system.

➡ Multilink:

The Multilink protocol can be activated or deactivated here for channel bundling in the PPP protocol. The channels are implemented either dynamically or statically (see below "Static Channel Bundling"), depending on the data volume.
Multilink can only be used if the peer supports this
protocol.

➡ Segmentation:

The segmentation option can be activated to distribute the capacity utilization of the B channels as evenly as possible when multilink is used. The segmentation process divides data packets into sub-units and transfers them by means of the available channels.

The remote station must also support this feature.

➡ IP header compression:

TCP header compression can be activated here. UDP and RTP headers are always compressed (if possible). This setting is **deactivated** by default.

➡ MTU size fragmentation:

This parameter can be used to enforce packet fragmentation (in 256 byte fragments) to ensure that voice transmission is not affected by long data packets. This setting is **deactivated** by default.

➡ PPP default header:

Send can be activated here for partners who need the default PPP header. This setting is **deactivated** by default.

➡ V.34 peer:

Activated in the case of a V.34 peer (e.g. analog modem).

➡ V.110 peer:

Activated in the case of a V.110 peer (GSM or Digital).

➡ Suppress IP addresses:

This parameter is activated if use of a transit network is not required. The remote station must also support this feature.

➡ Static channel bundling:

If this item is activated, HiPath HG 1500 attempts to set up all B channels administered for the peers
when setting up the connection for the first time.

➡ DID number:

This DID number is used to identify the caller when a call number is not transmitted (e.g. analog modem). Dialing this DID number instead of the HiPath HG 1500 router call number enables identification.
A DID number must be configured if the partner does not transfer a call number. This DID number must then be dialed by the partner.

➡ IP address mapping:

The parameter is set to "yes" if you want the IP addresses to be exchanged with this routing partner according to the IP mapping rules, see → 106.

➡ QoS capabilities:

Describes the Quality of Service capabilities of the ISDN peer or interface, see → 83. The default value is "identical", i.e. the same capabilities as used by HiPath HG 1500 are assumed: the partner can process the same values in the ToS field (Type of Service) in the IP header as HiPath HG 1500.

– DiffServ: the partner prefers to work with DiffServ; a reevaluation to DiffServ is performed, where applicable, by HiPath HG 1500.

– IP precedence: the partner prefers to work with an evaluation of the IP precedence fields (3 bits); the board consequently remaps the ToS field, where applicable.

➡ QoS bandwidth for EF:

This parameter can be used to reserve a specific percentage of the available bandwidth for the EF codepoint (EF), see → 83 QoS.

➡ PAP:

PAP must be activated at this point and the following parameters must be configured to allow the PAP security mechanism to be used within the PPP protocol:

– HOST:
This item defines whether the remote station (CLIENT) or the board (HOST) is to start the authentication procedure.

Host activated means: the board must be authenticated at the peer.

Host deactivated means: the peer must be authenticated at the board. "Host deactivated" is not generally used in conjunction with providers.

– User ID:

The PAP ID or corresponding user ID for the service provider is entered here.

– Password:

The corresponding PAP password is entered here.

➡ CHAP:

CHAP offers a different (safer) authenticating method as an alternative to PAP. The method should only used for CHAP.

- HOST:
  If this button is deactivated, HiPath HG 1500 awaits a command to authenticate (challenge). This is answered (response) and the HiPath HG 1500 is authenticated by the other.
  This setting is often needed when selecting the Internet.
  If the button is activated, HiPath HG 1500 sends a command to the authorizer and awaits a reply.
- User ID:
  At this point, a CHAP ID or corresponding user ID for the service provider is entered.
- Password:
  The corresponding CHAP password is entered here

The menu item "ISDN peer" contains the following submenus:

Call number list

➡ Call number

This is the ISDN call number at which a peer can be reached. It must be unique within the entire configuration and can comprise up to 22 decimal digits (0-9). A hyphen for separating the required trunk seizure codes can also be inserted.

➡ Call direction:

This parameter specifies the type of connection that can be set up under the call number. The following values are available:

- Blocked
  The number cannot be used.
- Incoming
  The peer may make calls but may not be called.
- Outgoing
  The peer may be called but may not make calls.
- Incoming and outgoing:
  The peer can make calls and be called.

IPX reconnect filter

Certain IPX packet types can be filtered to avoid unnecessary data traffic and the ensuing high communication charges. The filters can be activated or deactivated for every ISDN peer under this parameter category. If a filter is set, the system simulates packet exchange with the server. Double-clicking on a filter entry opens a window where "On" or "Off" can be selected. If the filter and short-hold mode are activated, the packets in question do not cause a connection to be reestablished. Nevertheless, if a connection is reestablished, these packets are transferred.

The following packet types can be filtered:

- Diagnostic packets
- Ping packets
- NDS packets
- NetBios packets
- SNMP packets
- SNMP packets
- NCP exchange time
- Interserver packets
- RIP/SAP modifications

Internet

To provide computers with Web pages or other services for the Internet, and in order to comply with the security mechanisms of the firewall, up to 20 computers can be specified on the basis of their IP address, service or protocol. In this way, the services enabled here are available via the Internet as soon as a connection is established with the Internet provider.

The following parameters apply:

- IP address: e.g. 135.34.12.178 (e.g. Web server in the home LAN)
- PC port: e.g. 80 (HTTP protocol, Web server)
- HiPath HG 1500 port: e.g. 80
- Protocol: TCP

With this entry, a Web server that was assigned by the provider for individual Internet access can be reached via the IP address.

The command only affects the ISDN3 interface and the DSL/LAN2 interface when NAT is activated (see → 105).

The PC and HiPath HG 1500 ports are normally identical.

IP Accounting

The parameters for using an accounting application are entered here. An accounting application with valid user name and password can access the accounting data records

➡ IP address application client:

IP address of the client PC. Data records can only be queried from this IP address. If the dummy IP address 0.0.0.0 is entered here, all PCs can query data, authorization is based exclusively on the user name and password.

➡ User name:

Login name for the accounting application. This name must be used by the accounting application for registration.

➡ Password:

Password for the accounting application. This password must be used by the accounting application for registration.

Presets

IP-routing

The network mask and gateway are assigned these presets when an IP-routing entry is newly created.

➡ Network mask:

A default value for the network mask can be specified here.

➡ Gateway:

A default value for the gateway can be specified here.

ISDN peer

The parameters short hold time and Callback are assigned these presets when an ISDN peer is newly created.

➡ Short hold time:

A default value for the short hold time can be specified here.

➡ Callback:

A default value for the callback can be specified here.

The menu item "ISDN peer" contains the following submenus:

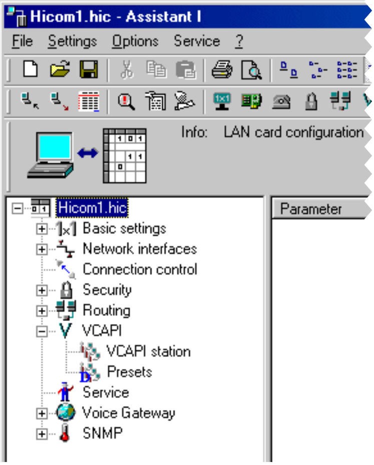
Call number

A default value for the call direction can be specified here.

IPX reconnect filter

Default values for the IPX reconnect filter can be specified here.

vCAPI



vCAPI station

With HiPath HG 1500 and vCAPI software (virtual CAPI), the PC behaves like a PC with a separate ISDN card. The CAPI interface provides applications with a standard method for interchanging data via ISDN. A "virtual CAPI” (vCAPI) must be installed since not every workstation within a LAN has access to a separate ISDN connection. A vCAPI client that provides a CAPI interface to the applications is required on the workstations. This communicates with the vCAPI server located on the HiPath HG 1500 with the help of the TCP/IP protocol. The vCAPI server distributes data to the relevant clients. Before configuring vCAPI clients in the administration program, you must define the IP addresses of the client PCs in question.

Up to 100 vCAPI stations that contain the following parameters can be configured:

➡ Call number (internal):

This parameter specifies the DID number at which a vCAPI station can be reached. A station can have more than one number (e.g. one for fax, one for Eurofile transfer, etc.), each containing up to 15 decimal digits (0-9) without special characters. The number must also be unique. The call numbers available can be determined on the basis of the call number list and simply assigned vCAPI functionality (see → 69).

➡ IP address:

The IP address is the characteristic value for a vCAPI station. The vCAPI client can be reached by the vCAPI server (HiPath HG 1500) at this address. More than one call number can be assigned to an IP address.

➡ Fax group 3:

The fax service option can be enabled or blocked for a call number using this parameter.

➡ Voice:

Voice can be enabled or disabled for a call number here.

➡ Digital data:

The "digital data" service can be enabled or disabled for a call number here.

Only fax group 3 or voice can be activated for a call number.

Presets

vCAPI station

➡ IP address:

A default value for the IP address can be specified here.

➡ Fax group 3:

Fax group 3 can be activated or deactivated by default here.

Service

➡ Licensed B channels:

The number of licensed B channels is stored here. If this parameter is changed, the license code number is queried following a customer database transfer.

➡ Maximum number of usable B channels:

The number of licensed B channels which HiPath HG 1500 may use is configured here.

Trace groups

The following data is output in the specified trace level.

➡ TG 112 (customer trace PPP)

Data concerning PPP setup is output here.

- Level 0

The partner station does not support CHAP

- Level 1
  - Connection setup rejection with output of
  - the reason and
  - the calling number
  - PPP over Ethernet active/session is closed
  - PPP, CHAP and PAP timeout
- Level 3
  - Connection setup by router with information on
  - the ISDN partner,
  - the calling number and
  - the called number
  - Progress of PPP handling until PPP connect message
- Level 4
  - IP/IPX packet which establishes the connection and specifies the
  - source and destination IP
  - protocol specifying the used ports
  - type of DNS query
  - inclusion of an additional B channel in the case of Multilink

    - Delayed CONN_CONF message with current state output
    - PPP over Ethernet Session open

➡ TG 113 (customer trace DSS1)

D channel ISDN messages are logged here.

- Level 2
    - Message Type with Causes and Channel ID
- Level 3
    - Call number (called and calling number)
    - Service (CIP)

➡ TG114 (customer trace CAPI)

VCAPI messages are output here.

- Level 1
    - Error entry: IP address cannot be configured as a VCAPI partner
- Level 3
    - Open/close an IP connection by specifying the IP address of the VCAPI client
    - Connection setup with
called number, calling number and channel ID (plci) for incoming connection
called number and channel ID for outgoing connection
    - Connection setup rejection with reason

Connection cleardown with reason
The reason is purely numeric and corresponds in part to the CAPI 2.0 specification,

➡ TG115 (customer trace H.323 stack)

No data has yet been output with this trace.

➡ TG 116 (customer trace virt. Optiset)

Messages to the virtual Optiset are output here.

- Level 1
    - Client login error
      Incorrect call no.
      Time difference between PC and Hicom too large
      Incorrect password during authentication
      Double license available
- Level 2

  - H.323 connection setup
    H.323 connection is assigned a channel
    H.323 connection could not be assigned a channel
    H.323 connection is through-connected
    H.323 connection could not be through-connected
    H.323 connection should be enabled
    H.323 connection was enabled
- Level 3
  - LAN connection to IP address set up/ended
    LAN connection to IP address set up (before login)
    LAN connection to IP address ended
- Level 4
  - Client login at Hicom (during system startup)
  - Client login status
    Client wants to log in
    Client successfully logged in
    Client wants to log out

➡ TG 117 (customer trace security)

Firewall messages are output here.

- Level 2
  - ISDN access firewall violation, rejection of call setup
    Unconfigured caller number
    Incorrect PAP/CHAP
  - MAC address used twice; output of relevant MAC address
  - IP firewall violated; output of source and destination IP
- Level 3
  - MAC firewall violated; output of IP and MAC address
  - NAT firewall violated (for ISDN3 interface only); output of source IP and port used

➡ TG118 (customer trace PBX routing)

The following messages are output in the case of PBX routing:

- Level 1
  - Message Type (incoming)
- Level 2
  - Causes, Channel Ident, Called and Calling Party Number
- Level 3
  - Call number (Called and Calling Number)
- Level 4

– Outgoing messages

Trace groups 119 to 121 are not used.

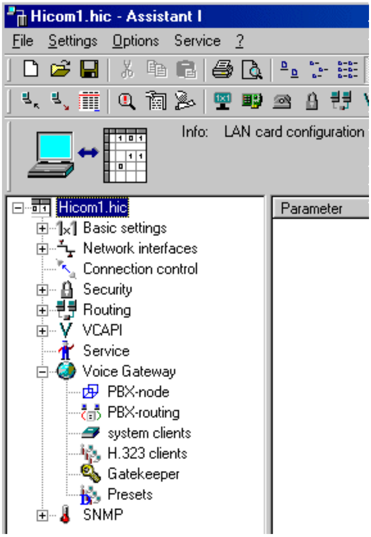
Trace level

- Level 0: deactivates the trace groups.
- Level 1-4: trace information details are reduced per level (1 = lowest level, 4 = highest level with the most information)

Should a trace memory overflow occur, reduce the trace level accordingly from 4 to a lower level.

Activated trace groups have a detrimental effect on performance. This is why they should only be activated for fault correction, and should be set to 0 during normal operation.

Voice Gateway



With Voice over IP, HiPath HG 1500 allows you to implement HiPath HG 1500 client features using Hicom.
In particular, you can implement this on a Teleworking PC.

H.323 clients can also be used for NetMeeting, for example.

Basic settings which are described by the following parameters apply for both clients:

Echo:

You can define here how echo compensation is to be implemented for Voice over IP.

➡ Traffic statistics:

This where you define whether traffic statistics should be compiled for clients, which can then be evaluated via SNMP.

➡ Coding:

This switch affects voice coding to the ISDN side.

➡ Max. number of simultaneous calls:

A specific number of the licensed B channels can be provided for Voice over IP. This is particularly useful if a minimum number of B channels is always to be available for routing. If six channels have been licensed, for example, four of these can be assigned to Voice over IP. This ensures that 2 B channels are always accessible for routing.

➡ Audio-Codecs for Voice Clients:

This parameter can be used to set the sequence of the audiocodecs which are used for handling. G.723 compresses the language, G.711 is uncompressed.

➡ AudioCodecs for Voice Clients

This entry defines the audiocodecs for connections to the clients and the sequence of their use.

PBX-node (Hicom 150 H V1.0 and later)

The IP addresses of your HiPath HG 1500 boards are configured here for each node (Hicom system), identified by a number from 1-64. Up to three HiPath HG 1500s can be configured per node, see → 76.

➡ AudioCodecs:

This entry defines the audiocodecs for connections between the PBX nodes and the sequence of their use.

➡ PBX node monitoring

As described under Basic Settings – ?????? Which settings????????

➡ Packeting:

This parameter is used to set the number of frames per RTP packet. A high value means a better relationship from user data to packet overhead but also a higher delay. A value between 1 and 3 can be set here. 1 is set by default.

PBX-routing (Hicom 150 H V1.0 and later)

Up to 2000 call numbers (including prefixes) can be entered here with the associated services that can be reached in another Hicom system via IP networking. The required service is configured for the call num-

ber: this can be voice, modem or fax.
PBX-node specifies the Hicom system in which this call number should be reached, see → 76,

System clients

"C55 optiClient" (new name: optiPoint 130) and "optiPoint IPadapter" (V1.0 Hicom 150 H and later) belong to the system clients.

➡ Internal call number of the system client:

The internal Hicom call number already defined is assigned here to the corresponding HiPath HG 1500 client.

➡ Authentication:

You can define whether the client must identify itself to HiPath HG 1500 in order to be used. This is particularly useful for clients which do not belong to the internal LAN and have to dial in externally.

➡ Password:

You can enable a selectable password for this client for authentication. This parameter is only active when authentication is set to "Yes".

➡ Status message transfer:

The transfer of status messages (e.g. display messages and LED information) can be activated or deactivated here. This parameter should be set to "Off" for remote clients. Otherwise short-hold is not possible for this connection.

H.323 clients

Voice and data services which are also available via Internet are provided by a H.323 client on the network PC. No Hicom features are supported here. When using the
as a gateway for H.323 clients, HiPath HG 1500only voice functions are available.

Before configuring H.323 clients in the administration program, you must define the IP addresses of the client PCs in question.

➡ Internal call number of the H.323 client:

Enter the internal Hicom call number provided for this station here. The call numbers available can be determined on the basis of the call number list and simply assigned H.323 functionality (see → 69).

➡ IP address:

This is where the IP address which was also assigned to the client PC for networking is entered. The IP address 255.255.255.255 must be entered if gatekeeper support is required for a client.

Gatekeeper

The gatekeeper registers the H.323 clients and administers their rights and services. It converts client call numbers into logical names or IP addresses and vice versa. In addition, it registers the gateways and can be networked with neighboring gatekeepers.

H.323 clients with gatekeeper link must be configured with the IP address "255.255.255.255".

➡ IP address:

Enter the PC’s IP address with the gatekeeper.

➡ Using gatekeeper:

You can activate gatekeeper support here.

➡ Prefix:

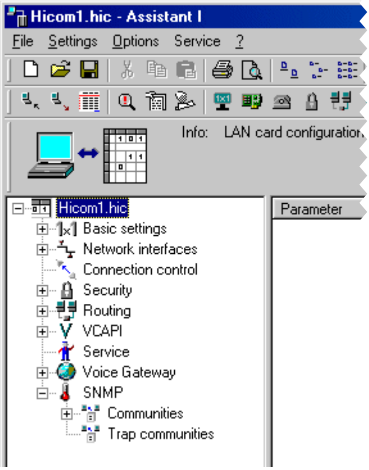
Enter the code which the station registered at the gatekeeper can use to reach a station connected directly to the Hicom.

Presets

➡ IP address:

A default value for the IP address can be specified here.

SNMP



The Simple Network Management Protocol is a standard which enables the transfer of data in the network concerning the status of HiPath HG 1500. HiPath HG 1500 enables data to be provided for evaluation using a standard SNMP program.

The following parameters can be set for this purpose:

- Minimum severity for general traps
- Minimum severity for voice traps
- Minimum severity for data traps
- Minimum severity for security traps
- Contact (MIB-2)
- Name of managed node (MIB-2)
- Location of managed node (MIB-2)

The possible severity values are warning, minor, major and critical.

Traps are only generated if a trap community is set up.

Communities

Communities can be defined here for SNMP agents. The parameters for a community are:

➡ Community name:

Freely assignable name (ASCII character string).

➡ Label (e.g. IP address):

The IP address of the manager who uses this community. If no value is specified or if 0.0.0.0 is entered, then this community can be used by every manager.

➡ Authorization:

Describes the type of access for this community, which can either be read-only or read/write.

Trap communities

Defines a community to which traps are to be transferred.
The parameters for a trap community are:

➡ Trap community name:

Freely assignable name (ASCII character string).

➡ Label (e.g. IP address):

The IP address of the recipient

"Options" menu

Program settings...

This menu allows the user to select the language.

Resetting the HiPath HG 1500

If a new HiPath HG 1500 board is to be administrated, the old connection established using this command must be reset.

Administratable HiPath HG 1500 cards

A HiPath HG 1500 board to be administered is entered here with a name and IP address. The required HiPath HG 1500 peer can be selected from a list if data is to be exchanged.

Set user name and password...

The user name/password combination can be changed here, e.g. to administer another HiPath HG 1500. User names and passwords are managed in Hicom and can also only be administered there.

Convert CDB

This option can be used to convert the current CDB. This can be necessary in the case of feature hubs in the board software (APS change with modified CDB layout). The current CDB version is shown in the status bar.

"Service" menu

Receive+Save error memory

Receives and saves the HiPath HG 1500 error messages in a file.

Receive+save the customer trace

Receives and saves the trace messages of the trace group previously activated under Service in a file.

Delete customer trace

Deletes the customer trace memory in the module.

Request table of call numbers

The call numbers (MSN) configured in the Hicom 150 E system can be requested here for the administration of HiPath HG 1500. The call numbers in this list can be
directly assigned VCAPI or H.323 functionality.

Import PBX-Routing

A file that simplifies the configuration of call numbers for PBX routing can be read in here, see → 76,

APS transfer

Enables the HiPath HG 1500 software to be updated.

APS+customer database transfer

Enables the HiPath HG 1500 software to be updated.
The customer database is also transferred. This is useful when the customer database structure has altered following several HiPath HG 1500 releases. In this way, the customer database can be converted at a remote workstation and then transferred together with the APS to HiPath HG 1500.
Proceed as follows to perform an APS transfer with CDB hub:

1. Read out the CDB from the HiPath HG 1500.
2. Select "Options -> Convert CDB" to update the CDB format.
3. Select "Save customer database as..." to save the CDB to the hard disk.
4. Activate "APS+customer database transfer": enter the new APS file in the file selection box then specify the converted CDB.

Both files are now transferred to the HiPath HG 1500 and permanently saved in the flash. A reset is then performed and the board starts up with the new APS and the converted CDB.

APS transfer via TFTP

Enables the HiPath HG 1500 software to be updated via TFTP. The IP address of the TFTP server and the directory and file name of the APS file must be configured.

Resetting the HiPath HG 1500 module

HiPath HG 1500 can be reset via Assistant I.

Transfer date and time to board

This function is used to transfer the date and time from the PC to the HiPath 500 board.

Applications

Voice over IP

Voice over IP is just one of the amazing features of HiPath HG 1500. Together with the clients connected to the LAN, the board offers options for using not only Voice over IP but also the telephony features of the system. You can avail of teleworking, i.e. full Voice over IP functionality is provided at the Teleworking PC. H.323 clients (e.g. NetMeeting) can also be used.

General parameters for Voice over IP

Before configuring HiPath HG 1500 clients and H.323 clients, you must configure the valid parameters for both variants:

➡ Echo:

You can define here how echo compensation is to be implemented for Voice over IP.

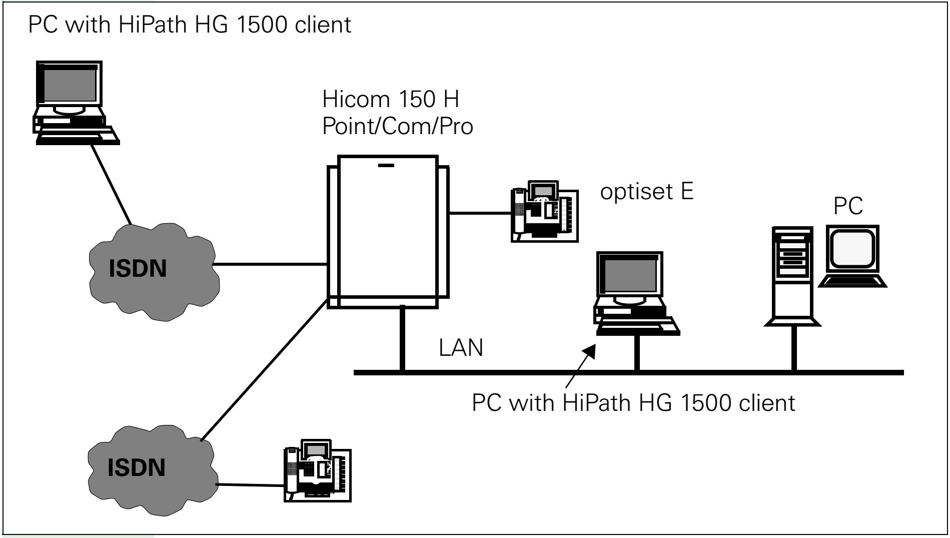
➡ Traffic statistics:

This is where you define whether traffic statistics should be stored, which can then be queried via SNMP.

➡ Coding:

The parameter is used to select the voice coding to be implemented.

HiPath HG 1500 client



Configuring a system client

To configure a system client in the Assistant I administration program, double-click with the left mouse button on "Voice Gateway" and then on "System Clients."You can then enter the call number of a new client by pressing "New". Repeat this step until you have defined all the required clients.

You can request a list of the possible call numbers with the menu item "Service/Request table of call numbers".

Once the client has been created, the following parameters must be modified:

➡ Internal call number of the system client:

This is an MSN configured for HiPath HG 1500.

➡ Authentication:

You can define whether this client must identify itself to HiPath HG 1500 with a password when starting the software. This is particularly useful for clients which do not belong to the internal LAN and have to dial in externally.

- Password:

  You can enable a selectable password for this client for authentication. This parameter is only active when authentication is set to "Yes".

- Status message transfer:

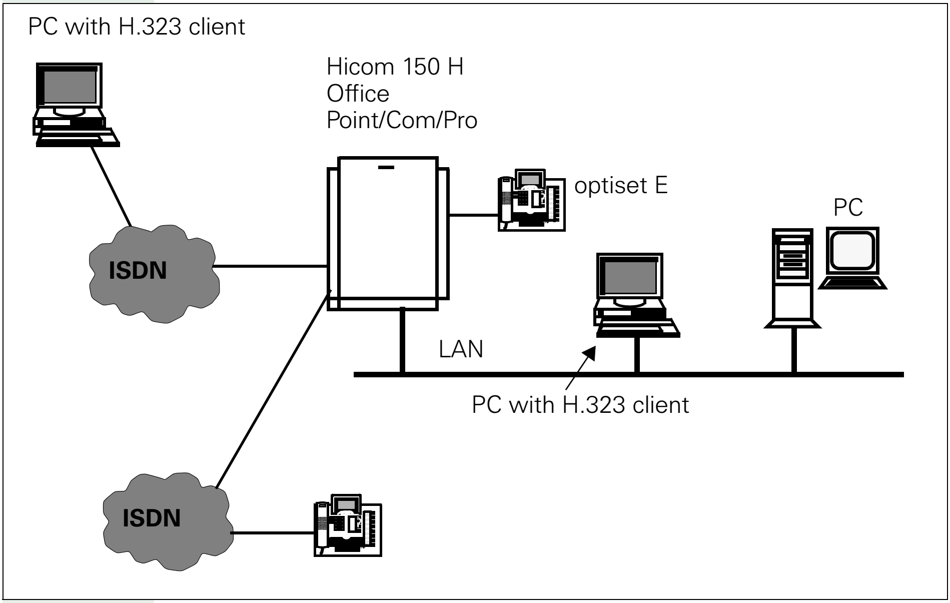
  With this selection you define whether client status messages (e.g. status of key LEDs) should be transferred.
  In the case of teleworking workstations, the transfer of status messages may prevent a configured short-hold function from being implemented.

See the operating instructions for more information on the system client.

In order to use a system client, the PC client must be equipped with a sound card offering full duplex functionality.

H.323 client

Voice services which are also available via Internet are provided by a H.323 client on the network PC (prerequisite:
fixed IP addresses for all stations and HiPath HG 1500). No Hicom features are supported.



Configuring a H.323 client

To configure a H.323 client in the administration program Assistant I, the IP network address should be saved under "Voice Gateway -> Presets". A list of the possible call numbers can then be determined and assigned under "Service-> Request table of call numbers". Once this has been done, simply edit the host address of the relevant clients.

Once the client has been created, the following parameters must be modified:

➡ Internal call number of the H.323 client:

This is an MSN configured for HiPath HG 1500.

➡ IP address:

A window now opens automatically where you can enter the IP address to be assigned to this call number. This is the IP address which was also assigned to the client PC for networking.

For information on presets, see "Voice Gateway - H.323 client“ (see → 65).

You can now configure the required H.323 clients on the network PC.

The gateway IP address must be entered at each client. This corresponds to the IP address of the LAN interface.

Information on client installation and configuration is contained in the operating instructions or Online Help for the software in question.

Enter 255.255.255.255 as the IP address
if gatekeeper support is to be used. For more information, see → 114.

IP Networking (PBX Routing)

Introduction

In addition to the previous networking options available to Hicom 150 H systems via CorNet-N and QSig, IP networking can now also be used in V1.0 and later (OfficePro, OfficeCom, OfficePoint). The IP Networking feature was enabled by HiPath HG1500.

This can lead to significant call charge savings if an appropriate IP network is available. The user can also avail of telephony features, such as name transmission and callback in the usual way.

The hardware prerequisite for IP networking is that the systems involved must have at least one of the following HiPath HG1500 boards:

- HXGM: max. three boards can be implemented in an OfficePro. 16 IP channels are available for voice connections (Voice over IP) in each HXGM.
- HXGS (wall housing) or HXGSR (19" housing): up to two boards can be implemented in the OfficeCom and one in the OfficePoint. Both boards feature 8 IP channels for voice connections.

The IP-networked systems and the HiPath HG1500 boards are administered via two different tools:

- Hicom Assistant E Office: extend the existing Hicom 150 H CDB to include information for IP networking (page 77 and later)
- Assistant I/HG1500: make HiPath HG1500 board settings (page 80 and later)

Please refer to

- the Hicom 150 H Service Manual and
- the HiPath HG1500 Administration Instructions

for additional information.

Hicom Assistant E Office: Extending the Existing Hicom 150 H CDB to Include Information for IP Networking

The following information refers to Hicom 150 H systems with the central boards CBMOD (OfficePro) and CBPC (OfficeCom, OfficePoint).

The structure of the "Network..." mask ("Settings" menu) is different for systems with CBCPR, CBCC, CBRC, CBCP, CBRP, SBSCS and SBSCO control boards.

Step	Action
1.	Download and save the existing Hicom 150 H CDB using Hicom Assistant E Office.
2.	If necessary, convert CDB to Version 1.0 or 1.2.
3.	Open the "System-wide..." mask in the "System status" menu.
4.	Open the "Cards" tab. • Switch to "SW expansion": insert HiPath HG1500 board(s). • Switch to "Card Config." and open the "HXGM configuration" tab: – Selection: if an OfficePro features more than one HXGM board, the HXGM board to be configured can be selected here. – Trunks: the maximum number of possible trunks (IP channels) to be configured on a HiPath HG1500 board is defined under “new number.”The trunks appear in the corresponding display field once the "setup" button is pressed.
5.	Open the "Lines/networking" mask in the "Settings" menu.
6.	Open the "Trunks" tab. • Route column: trunks used for IP networking must always be assigned route 16. • Param column: double-click this field for the relevant trunk to display the "Parameter" mask with the current protocol set (HXGM/HXGS: Trunk CorNet-N Plus (HiPath AllServe H150).
7.	Open the "Routes" tab. • Route Name: a route can be assigned a name here. The route name is then displayed instead of the default route number entered in the "Routes" list field. • PABX number: the system is identified in the IP network on the basis of this number. The PABX number must not be included in the numbering plan and must be unique within the IP network. No entries should be made for country code and local area code.

Step	Action
8.	Open the "Routing parameters" tab. The following settings are mandatory: • Route optimize active: No • Routing flags: Over. service 3.1 kHz Audio • Analog trunk seizure: no pause • Trunk call pause: Pause 6 s • Type of seizure: linear • Route type: PABX • No. and type, outgoing: Internal • Callnumber type: Internal/DID
9.	Open the "Network..." mask in the "Settings" menu.
10.	Open the "IP parameters" tab. • IP-Access: select HIP Forwarding. The HiPath HG1500 board works in bridging mode, i.e. the HiPath HG1500 board and the Hicom 150 H control board have separate IP addresses which share a physical LAN interface. • Hicom 150 H – IP address: the IP address used by the HiPath HG1500 board for addressing the Hicom 150 H is entered here. – Subnet mask: subnet mask at the interface between Hicom 150 H and the HiPath HG1500 board. – MTU: maximum Ethernet frame length on the link between Hicom 150 H and the HiPath HG1500 board. The preset value should not be modified. • Routing table: all values set here should not be modified.
11.	Open the "AllServe Parameter" tab. • Server IP address: not relevant • Node Node ID: a unique node ID must be set for each system in the IP network. The number used should be in the range 1 - 64 because a node ID is also required on the HiPath HG1500 board and both IDs must be identical (assignment of node ID to IP address). • AllServe access authorization Board column: shows which HiPath boards are inserted in which slot in the system. The "AllServe access" flag is to be set for the boards intended for IP networking.
12.	Open the "Least cost routing..." mask in the "Settings" menu. Note: the unit numbering of all IP-networked systems must be set before system generation in order to guarantee the uniqueness of all call numbers and codes (trunks, internal accesses, groups, etc.) in the network. One way of doing this is by assigning a defined call number range to each system. For example, one-thousand call numbers (1001 - 1999) for system 1 (node 1), two.thousand call numbers (2000 - 2999) for system 2 (node 2), etc.

Step	Action
13.	Open the “Codes and flags” tab. • LCR - flags: set the “Activate LCR" flag to activate automatic least cost routing. • Digit transmission: mark en-bloc sending. Dialled digits are buffered by the system. The number is only dialing when a timeout activated by entering the last digit or the end-of-dialing code "#" expires.
14.	Open the "Dial plan" tab. • Dialed digits column: the digits for accessing the IP-networked system are set here. • Route table column: the route table entered here specifies the connection setup. Example: dialed digits = –2XXX, route table assigned = 1. Connections are set up for all dialed call numbers from 2000 - 2999 on the basis of route table 1.
15.	Open the "Dialing rules table" tab. • Rule name column: a freely selected name containing up to 16 ASCII characters can be entered here. • Rule format column: the rule entered here defines how the digits dialed by the user are to be implemented and dialed by the system. Example: rule format = DxxxE1A, where xxx is the PABX number of the system to be reached (see 7).
16.	Open the “Route table” tab. • Selection field: the route table defined in 14 must be selected here. • Route column: enter the route selected in 6. • Dial rule column: enter the rule defined in 15.
17.	Save CDB and transfer to Hicom 150 H.

Assistant I/HG1500: Making HiPath HG1500 Board Settings

- Start up the HiPath HG1500 board(s)

  For more information, refer to the Chapter Startup in the HiPath HG1500 Administration Instructions.

  The prerequisite for IP networking is that all PBX nodes (Hicom 150 H systems) are located in the same IP network and not networked via IP-routing (e.g. connection via an S0 dedicated line).

- Enter the settings for IP networking

Step	Action
1.	Download and save the existing HiPath HG1500 board CDB using Assistant I/HG1500.
2.	Select "Basic settings" in the "Settings" menu.
3.	Enter the basic settings: • Coding: this parameter is transferred by Hicom 150 H to the HiPath HG1500 board(s) and must not be changed. • Number of B channels that can be used by routers: max. 16 B channels are possible, a minimum number of which should always be available for HiPath HG1500 clients. If, e.g. six B channels are licensed, four of these could be assigned to the router. This would guarantee that two B channels are always free for the HiPath HG1500 client. • IEEE802.1p: parameter for setting the Ethernet format. The available settings are "deactivated" (default) and "activated". The parameter only works on data packets that are sent from the HiPath HG1500 board. All components in the LAN used by HG1500 for exchanging Ethernet data packets must support this format. • QoS procedures: parameters for defining the Quality of Service procedure used to set precedence for incoming IP data packets on HiPath HG1500 board. Default value is "Autodetect". • PBX-node monitoring (in Assistant I/HG1500 SMR15 or later, this setting can be found under "PBX-routing“ in the "Voice Gateway" menu item): Monitoring can be activated here between the IP-networked Hicom 150 H systems (nodes). If "activated" is selected, monitoring messages are sent from node to node every 4 seconds. IP Networking is considered to have crashed if a node does not receive any more monitoring messages. Existing calls are cleared down. The parameter must be set identically in all systems (nodes).

Step	Action
4.	Set the "QoS order of priority". HiPath HG1500 uses four classes to set the order of precedence for incoming IP data traffic: • Voice Payload: H.323 packets which contain voice information. • Call Signaling: needed for connection setup (e.g. H.323). • Fax Modem Payload: e.g. for fax data for IP networking. • Network Control: e.g. SNMP traps. The priority of the individual classes is set via the "AE/EF codepoints". The default values can generally be maintained.
5.	Set "AE/EF codepoints". The values that define the various priorities are defined here (4). The default values are to be maintained.
6.	Select "Voice Clients" in the "Settings" menu. (This option is called "Voice Gateway" in Assistant I/HG1500 SMR15 and higher.)
7.	Enter settings for Voice over IP: • Echo: if "on" is selected, compensation can be made for echos which can occur in the case of connections via the voice gateway to analog telephones. • Traffic statistics: select "one" to generate statistics which can be evaluated via SNMP. • Coding: this parameter is transferred by Hicom 150 H to the HiPath HG1500 board(s) and must not be changed. • Max. number of simultaneous calls: a certain number of the licensed B channels (max. 16 for HXGM, max. 8 for HXGS, HXGSR) can be made available here for Voice over IP. This also depends on the number of HiPath HG1500 clients installed (voice clients). • H.323 client capabilities (in Assistant I/HG1500 SMR15 and later these options can be found under "Audio Codecs for Voice Clients"): the audio standards of the H.323 clients under IP Networking (Voice over IP) are defined here. The following settings must be selected: – Number of entries = 3 – AudioCodec (high priority) = G.723 – AudioCodec (medium priority) = G.711 U-Law – AudioCodec (low priority) = G.711 A-Law Note: G.723 performs compression on approx. 18 - 20 kBit/s. G.711 provides for a fully duplex connection with 180 kBit/s (at the expense of the IP data load). Note on the use of C55-type IP telephones: "AudioCodec = G.723" must be selected for configuration as a "Home client", while "AudioCodec = G.711 U-Law" must be selected for configuration as "Office client".
8.	Select Routing in the Settings menu.

Step	Action
9.	Enter settings under "PBX-node" (in Assistant I/HG1500 SMR15 and later, this setting can be found in the "Voice Gateway" menu item): The connection between the node number (node ID, see 11 on page 78) of the Hicom 150 H system and the IP addresses of the HiPath HG1500 board is set up here. • PBX-node: number from 1-64 which identifies the Hicom 150 H system (node ID, see 11 on page 78). • IP address: up to three HiPath HG1500 boards can be configured per node (Hicom 150 H system) on the basis of their IP addresses.
10.	Enter settings under "PBX-routing" (IP Networking) (in Assistant I/HG1500 SMR15 and later, this setting can be found in the "Voice Gateway" menu item): Up to 2000 call numbers (DID numbers or prefixes) can be entered here with the associated services that can be reached in another Hicom 150 H system via IP networking. • Call number • Service: the services voice, modem and fax are available. • PBX-node: enter the node number (node ID, see 11 on page 78) of the Hicom 150 H system in which this call number is to be reached.
11.	Save CDB and transfer to the HiPath HG1500 board.

Quality of Service (QoS)

Quality of Service encompasses various methods for guaranteeing certain transmission properties in packet-oriented networks (IP).

It is thus important, for example, to ensure a minimum bandwidth for Voice over IP for the entire duration of the transfer operation. If multiple applications with equal rights are operating via IP, then the available bandwidth for the transmission path (e.g. an ISDN B channel, 64kBit/s) is split. In this case, a voice connection may experience packet losses which can reduce voice quality.

The HiPath HG 1500 uses various different procedures to implement Quality of Service.

On layer 2 (according to OSI, Ethernet), an extension (IEEE802.1p) of the standard Ethernet format (DIX V2) can be activated. This extension enhances the Ethernet header to include additional information including a 3-bit data field. The data packet is assigned priority information in this field. For all packets that reach the board from the LAN, both Ethernet formats (IEEE802.1p and DIX V2) are understood; for all packets that are sent from the board to the LAN, the format can be selected via "Basic settings->IEEE802.1p. You should check whether all components in the network support this format before this parameter is activated. Otherwise, it may not be possible to access the HiPath HG 1500 from the LAN anymore.

The Ethernet header is not transported when switching to another transport medium (e.g. ISDN). An IP router (like the HiPath HG 1500's router) can therefore use the information contained in the IP header for prioritization. Straightforward IP routers that connect two network segments, for example, can use the IP level prioritization In the Type of Service field, either 3 bit (IP precedence based on RFC 791, older standard) or 6 bit (Differentiated Services or DiffServ, based on RFC 2474) are evaluated for the creation of various classes. The HiPath HG 1500's IP router provides various bandwidths for these classes, so that, for example, voice packets can be processed first. The procedure adopted by HiPath HG 1500 can be set under "Basic settings->QoS procedures" (Autodetect is set by default).

For the DiffServ parameter, various so-called codepoints ("Basic settings ->AF/EF codepoints") are defined, and based on these codepoints two different procedures are used for processing the payload of different marked data flows:

The Expedited Forwarded (EF) procedure (based on RFC 2598) guarantees a constant bandwidth for data in this class. If this defined value is reached, all packets that exceed this bandwidth are rejected. A separate class is defined for EF on the HiPath HG 1500. For this class, the bandwidth can be defined as a percentage for every ISDN peer (QoS bandwidth for EF).

The Assured Forwarding (AF) procedure (based on RFC 2597) guarantees a minimum bandwidth for the data of one (of many) classes. Lower priority classes share the bandwidth not used by EF or the classes with higher priority. In addition, the speed at which packets are rejected if the system is unable to forward them fast enough can be defined for every class by means of the Dropping Level setting. Nothing is thus to be gained by buffering voice packages for an extended period of time (this only increases the delay). In the case of secure data transfer (e.g. File transfer), on the other hand, a large buffer is advantageous as packets are otherwise sent repeatedly between the two terminals.

Four classes are reserved for AF on the HiPath HG 1500: AF1x (low priority), AF2x, AF3x and AF4x (high priority), where "x" stands for one of three dropping levels: low (1), medium (2) and high (3). In the case of "low", packets are buffered over an extended period, in the case of "high", packets are promptly rejected if they cannot be forwarded. Unmarked IP packets (ToS field=00) are handled in the same way as the codepoint AF11.

If a routing partner can only work with one of the two standards (DiffServ or IP precedence, e.g. an older router that only works with IP precedence), then the HiPath HG 1500 can translate the ToS field accordingly. This can be set for each ISDN peer or DSL/LAN2 interface via "QoS capabilities". When the default value is set ("identical"), nothing is translated; with the values "DiffServ" or "IP precedence", translation is performed on the basis of the table below, if data is not entered in the field in accordance with the standard set.

In the case of IP data traffic, the IP packets that generate the HiPath HG 1500 are split into five groups (e.g. the VCAPI server, H.323 gateway). You can set which codepoint is to be used for marking the packets for four of these groups. This is configured under "Basic settings->QoS order of priority“:

Voice Payload for H.323 telephony (Voice over IP)

Call Signaling for connection setup in H.323

Fax Modem Payload e.g. for IP networking with fax or modem

Network Control e.g. SNMP traps

The remaining data traffic is marked "deactivated", i.e. 00.

The following table shows the relationship between the various codepoints of DiffServ, IP precedence and the "User Priority" field in the Ethernet header.

IP header									**Ethernet header**
DiffServ						vs.	IP precedence		IEEE802.1p
Codepoint	Default (adjustable)		Drop level				Assignment (fixed)		
	binary (bit field)	ToS field (hex)	high	med	low		binary (bit field)	ToS field (hex)	User Priority (binary, bit field)
deactivated	000000	00					000	00	000

IP header									Ethernet header
AF 11	001010	28			x	->	001	20	001
AF 12	001100	30		x		<->	001	20	001
AF 13	001110	38	x			->	001	20	001
AF 21	010010	48			x	->	010	40	010
AF 22	010100	50		x		<->	010	40	010
AF 23	010110	58	x			->	010	40	010
AF 31	011010	68			x	->	011	60	011
AF 32	011100	70		x		<->	011	60	011
AF 33	011110	78	x			->	011	60	011
AF 41	100010	88			x	<->	100	80	100
AF 42	100100	90		x		<->	110	C0	110
AF 43	100110	98	x			<->	111	E0	111
EF	101110	B8				<->	101	A0	101

The "vs." column shows the relationship between the DiffServ and IP precedence standards. Since DiffServ offers more variants, the codepoint is permanently selected when translating IP precedence into DiffServ: the codepoint for the IP precedence "010", for example, becomes "AF22". In the case of packet that leave HiPath HG 1500 in the direction of the LAN, the user priority specified in the last column is set when IEEE802.1p is active.

QoS can be activated for the second LAN or DSL interface as well as for the ISDN peer.
For the DSL interface, the interface is extended by an additional transmission rate limitation. The function of the quality evaluation corresponds to the ISDN peer procedure. The average transmission rate is set in configuration data.

Telematics using a vCAPI client

Principle of virtual or distributed CAPI (vCAPI)

Today all users can access an ISDN card integrated in a network PC or server by installing a "virtual CAPI interface" (vCAPI) in their PCs to emulate the existence of a local ISDN card.
With respect to PC applications, the virtual CAPI interface behaves for the most part like a CAPI interface supplied with an ISDN card. The difference is that the virtual CAPI does not forward the functions activated by the application directly to the card, but rather converts them into a data packet and outputs them to the LAN (client/server principle).
A virtual ISDN card is provided by Hicom150 E Office Point/Com/Pro to save one or more ISDN cards. A virtual CAPI interface with the previously described functionality is installed on all network PCs (CAPI client). The messages sent by the PCs via the virtual CAPI are evaluated on HiPath HG 1500 (CAPI server). This information is subsequently used to set up one or more B channel connections for the required service and to process the selected protocol.
A number of DID numbers (max. 100) must be made available to HiPath HG 1500 for incoming calls. Each of these call numbers must be mapped to a network address to allow an incoming call to be switched specifically to one of the virtual CAPI interfaces. The virtual CAPI reconverts the Ethernet packet into the appropriate CAPI messages.

Identification of the CAPI station

A "vCAPI" interface is installed in the form of a DLL (CAPI20.DLL 16 Bit, CAPI2032.DLL 32 Bit) on each PC that uses telematic functions. Each PC is uniquely identified in the network by means of its IP address and its call numbers.
The call number of the destination station is specified in every outgoing connection setup and, if applicable, checked with the, Hicom150 E Office Point/Com/Pro toll restriction check. The call number is not checked by HiPath HG 1500 at this point.
Unlike router functionality, the security mechanisms (firewalls) described there cannot be used for telematic functionality. For example, it must also be possible to contact a PC with vCAPI via its DID number if the call does not have an ISDN call number (e.g. analog fax machine).

With HiPath HG 1500 and vCAPI software (virtual CAPI), the PC behaves like a PC with a separate ISDN card. This requires:

- TCP/IP as the transport protocol
- WIN 95/98, WIN-NT 4.0 or Windows 2000 as the client operating system

Call numbers are assigned in HiPath HG 1500 by assigning a TCP/IP address to the call number. Up to 100 call numbers can be used for vCAPI functions.

It is sometimes necessary to assign several call numbers to your TCP/IP address so that several services can be used. This is particularly relevant if you wish to use CTI and fax services simultaneously on one PC.

You can request the available internal call numbers via the table of call numbers (see → 69).

Only the CAPI standard Version 2.0 is supported.
(16 and 32-bit Version / CAPI20.dll and CAPI2032.dll)

A CAPI is also installed as a service under Windows NT 4.0 and Windows 2000, e.g. for cFos.

Configuring vCAPI client

In order to use the virtual CAPI function in the network, 2 requirements must be met:

- Configuring the vCAPI station in the administration program
- Configuring the vCAPI client on the network PC.

Before configuring vCAPI clients in the administration program, you must define the IP addresses of the client PCs in question as well as the internal Hicom call numbers to be used.

To configure a vCAPI client in the administration program Assistant I, the IP network address should be saved under "Voice Clients -> Presets". A list of the possible call numbers can then be determined and assigned under "Service-> Request table of call numbers". Once this has been done, simply edit the host address of the relevant clients.
Repeat this step until you have defined all the required clients.

Once the client has been created, the following parameters must be modified:

- Call number (internal):

  This is an MSN configured for HiPath HG 1500.

- IP address:

  A window now opens automatically where you can enter the IP address to be assigned to this call number. This is the IP address which was also assigned to the client PC for networking.

- Fax group 3:

  You can define here whether a vCAPI station is also permitted to use the fax group 3 service. If this flag is enabled and CTI is used at the same time, a second call number must be assigned to this IP address. Otherwise problems may arise during call pickup.

- Voice:

  Voice can be enabled or disabled for a call number here.

- Digital data:

  The "digital data" service can be enabled or disabled for a call number here.

For information on presets, see "vCAPI station“ (see → 58).

Repeat these steps until you have defined all the required stations.

You can request the available internal call numbers via the table of call numbers (see → 69).

Now you can install the vCAPI software delivered with HiPath HG 1500 every PC where vCAPI is to be provided.

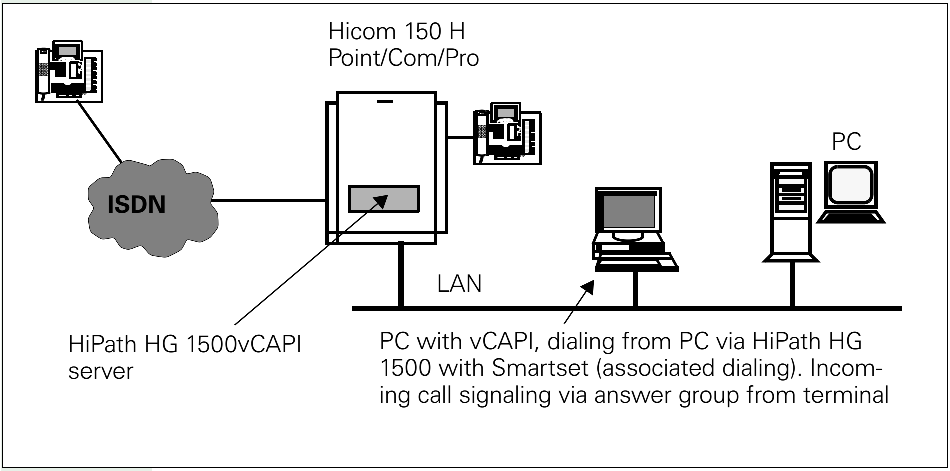
The IP address of the LAN network interface must be entered during installation.

Call charge allocation

When telematic services are used via vCAPI, call charges are assigned to the corresponding PC call number/MSN.

vCAPI and Smartset

Smartset is an optional CTI client which provides your PC with features such as associated dialing from a telephone book, caller identification using the telephone book, answer groups and a caller list. Documents can also be opened automatically for incoming ISDN calls. Smartset exchanges data with your Windows applications using DDE functions.

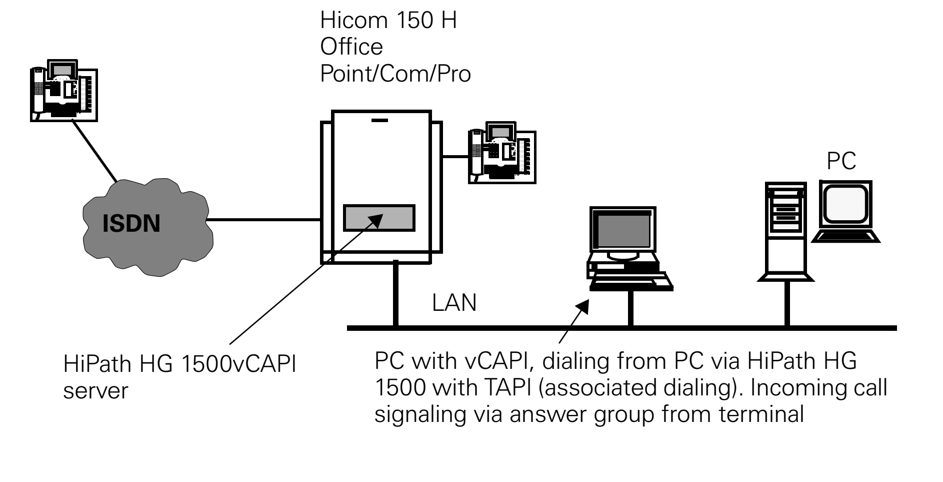

Hicom 150 H
Point/Com/Pro
PC
ISDN
LAN
HiPath HG 1500vCAPI server
PC with vCAPI, dialing from PC via HiPath HG 1500 with Smartset (associated dialing). Incoming call signaling via answer group from terminal

Configuring CTI/Smartset

A vCAPI station must first be configured, if this has not yet been completed (see → 87, Configuring a vCAPI client).

- Hicom: Associated dialing must be enabled in Hicom if Smartset functionality is to be used.
- Smartset: Enter your own call number, the call number of the station for which associated dialing is to be implemented, and the trunk seizure code. (See the operating instructions for more information on Smartset.)
- Answer group: The answer group feature is configured for the vCAPI station telephone. Smartset only displays incoming calls when this is configured.

vCAPI and TAPI


Hicom 150 H
Office
Point/Com/Pro
ISDN
PC
LAN
HiPath HG 1500vCAPI server
PC with vCAPI, dialing from PC via HiPath HG 1500 with TAPI (associated dialing). Incoming call signaling via answer group from terminal

TAPI clients

Automatic dialing can also be implemented using the vCAPI-based TAPI and a TAPI-compatible application. One example of this is dialing one of the call numbers saved in MS Outlook under Contacts.

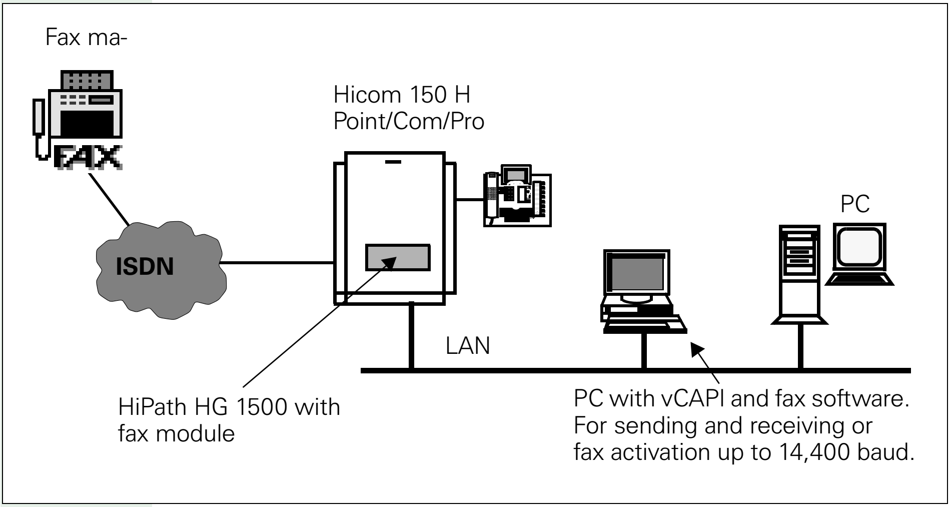
Note that in MS Outlook, call numbers must be specified in the international format, e.g. +49(2302)999420.

Associated dialing must be enabled in Hicom if TAPI functionality is to be used.

The answer group feature must be configured for the TAPI station telephone.

vCAPI and fax

You can send and receive faxes via the HiPath HG 1500 vCAPI. To do this, you need an optional CAPI-based fax software.


Fax ma-
FAX
Hicom 150 H
Point/Com/Pro
PC
ISDN
LAN
HiPath HG 1500 with
fax module
PC with vCAPI and fax software.
For sending and receiving or
fax activation up to 14,400 baud.

Fax services with HiPath HG 1500

- Each PC has a separate fax DID number
- Group 3 fax machines send and receive at a speed of 14,400 bauds
- Fax activation in receive direction
- Fax forwarding possible on no answer and busy to analog fax (e.g. if PC is switched off)
- No B channel reservation (the channel can be used by other applications when no fax is being sent or received).
- Depending on the system type and the number of boards up to 9 simultaneous faxes are possible.

Configuring a fax

A vCAPI station must first be configured, if this has not yet been completed (see → 87, Configuring a vCAPI client)

- Install fax application and enter assigned call number
- Start fax application

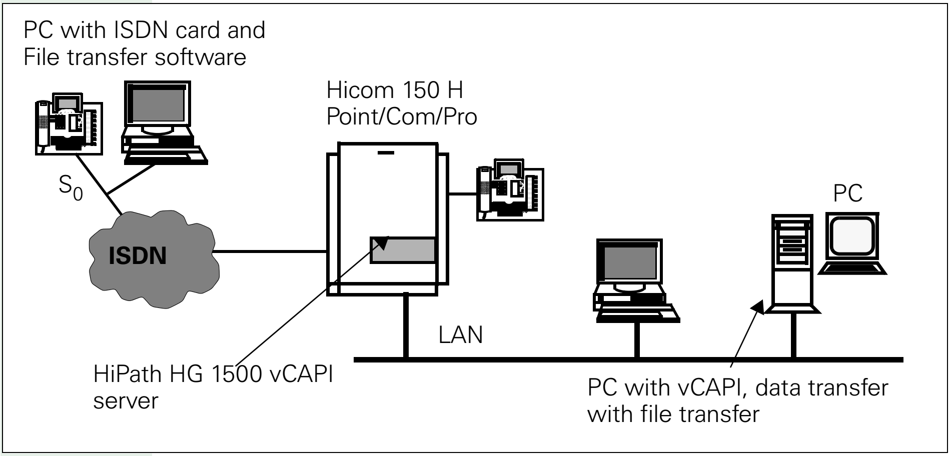
The call number now appears in the caller list of the station logged on.

Refer to the software installation instructions for more information on installation.

If you want to use CTI and fax functions simultaneously at your client PC, an individual call number should be allocated for each service. Otherwise problems could arise during call pickup.

vCAPI and file transfer

File transfer enables direct data exchange with your ISDN peer. This is possible using any software with the EuroFile transfer standard, or using the same proprietary software on both sides.



Configuring file transfer

A vCAPI station must first be configured, if this has not yet been completed (see → 87, Configuring a vCAPI client)

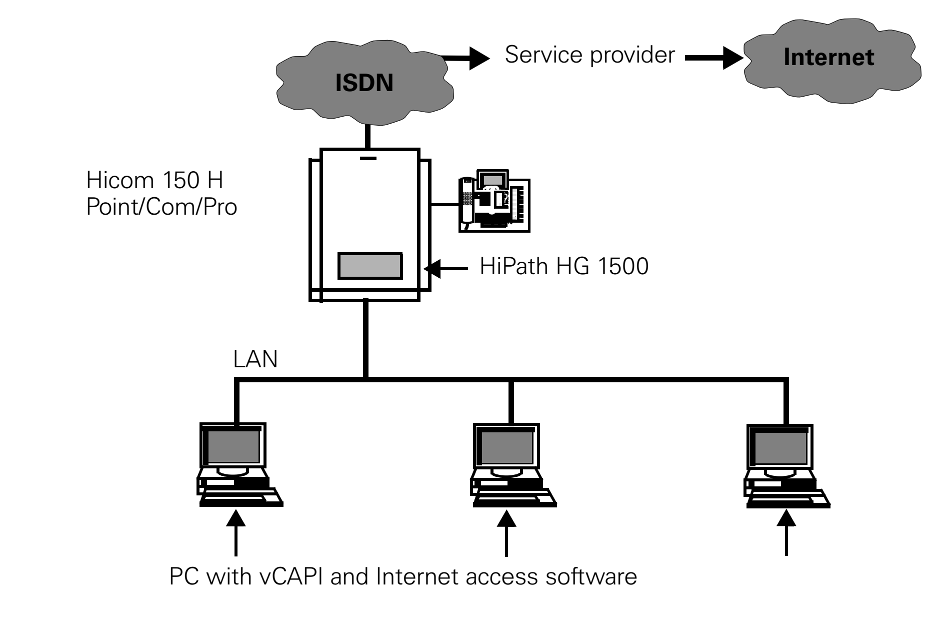
- Install file transfer application and enter call number
- Start file transfer application

The call number now appears in the caller list of the station logged on.

Refer to the software installation instructions for more information on installation.

vCAPI and Internet

Internet access via vCAPI is only necessary if your service provider’s access software requires the CAPI interface.



Internet access is also possible via routing (see → 101,

Configuring Internet access via vCAPI

A vCAPI station must first be configured, if this has not yet been completed (see → 87 Configuring a vCAPI client)

- Install Internet access software

For more information on installation and configuration (IP addresses, gateways, etc.) see the software installation instructions.

Routing

LAN-LAN and Teleworking

LAN-LAN connections, i.e. WAN connections can be established using HiPath HG 1500 to another HiPath HG 1500, Hicom LAN-Bridge 1.x or other routers. Access to Internet providers is also possible via routing.

HiPath HG 1500 offers channel bundling for up to 16 B channels (Hicom Office Point offers a maximum of 8 B channels on the CO-side).
The transport protocols IP or IPX are supported.

In the case of HiPath HG1500 with two LAN interfaces, routing is also possible between the two LAN interfaces,see → 98.

Features

- PPP connections (LAN-LAN connection and teleworking)
- PPP multilink connections (channel bundling)

Firewall mechanisms

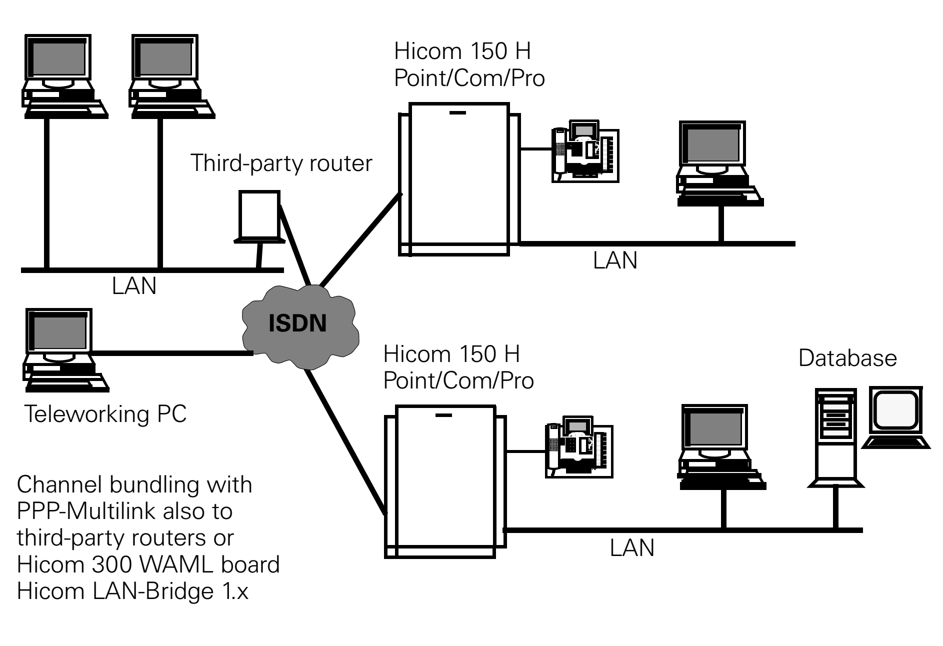
- Verification of MAC, IP or IPX addresses
- TCP, UDP and ICMP port firewall
- Access control using ISDN call numbers
- Automatic callback
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol).

A teleworking station requires an ISDN card with remote access software (e.g. Dial-Up Networking). A network connection to HiPath HG 1500 is established via the ISDN card.

Access to the local networks can be established via the following connections:

- Analog V.34 (max. 33,600 bit/s)
- ISDN DSS1
- GSM V110

Routing with HiPath HG 1500



Configuring LAN-LAN routing via ISDN

The following steps must be completed in the administration program to use HiPath HG 1500 as an ISDN router:

- Identify the IP address of the remote LAN
- Define the IP address of the shared WAN (ISDN)
- For all PCs, enter the IP address of HiPath HG 1500 as the gateway under "Network interface -> Network interfaces -> LAN".

Network interfaces

Network interfaces

➡ ISDN 1 or 2

Enter the IP address defined previously for the WAN here.

Where required, enable the interface to be configured under "Network interfaces".

Routing

IP-routing

With the left mouse button, select "IP-routing" and press "New."In the dialog window, enter the IP address of the LAN and confirm your entry. To reduce the input load, you can enter the values for "Network mask" and "Gateway" under "Presets".

Select the new entry using the mouse.

➡ Network mask:

Specify the network mask of the destination network.

➡ Gateway:

Under Gateway, enter the IP address of the remote ISDN interface.

ISDN peer

With the left mouse button, select "ISDN peer" and press "New."In the dialog window, enter the name of the ISDN peer and confirm your entry.

Select the new entry using the mouse.

➡ IP address:

Enter the IP address of the remote ISDN interface. The same address is entered here as under "Routing - IP-routing - Gateway" (IP address of the remote ISDN interface).

➡ B channels:

Enter the maximum number of B channels for this connection.

Double click on the corresponding ISDN peer.

Call number list

Press "New" to create a new entry and enter the remote call number.

➡ Call direction:

Define the call directions permitted for this peer.

Adapt the other protocol settings in line with the remote side and configure these settings for your HiPath HG 1500.

Finally, test the specified route by transmitting a "Ping" to the peer.

➡ If a correct reply is not received for the Ping, the peer may be incorrectly configured.

For information on further parameters, see → 50.

Configuring LAN-LAN routing between the LAN interfaces

Both LAN interfaces can connect two different networks. The configuration of the LAN2 interface is the same as for the first LAN interface.

No routing entries must be made for the two directly connected networks.

Moreover, the "NAT" parameter can be used to set up address translation vis-à-vis the other interfaces, see → 105.

Special features of Windows networks

Routing and name resolution

For example, when routing from HiPath HG 1500 to HiPath HG 1500 and for peer-to-peer connections (Windows for Workgroup Network for IP routing), you must create an LMHOSTS/HOSTS file on the client PCs. This is stored in the Windows directory under Windows 95, and in the directory WINNT\SYSTEM32\DRIVERS\ETC under Windows NT/2000. The file LMHOSTS.SAM in the directory can be expanded but must not have an extension (LMHOSTS).

Sample entry:

192.168.10.10 HG1500

192.168.10.20 PC1

Do not forget to press Return after the last entry.

Once the LMHOSTS/HOSTS file has been created, a Ping command should be transmitted to the peer with the name (e.g. Ping HG1500). Since browsing is not transferred in the case of routers (broadcast messages), the other PC can only be found by right-clicking the Network Neighborhood and Find Computer icons. The network resources can be accessed when the PC is found. The other PC cannot be accessed by opening the network neighborhood.

Names should contain no more than 8 characters since some operating systems run into problems if there are more than 8 character in the name.
Modifications in LMHOSTS/HOSTS are only effective after the computer has been rebooted. Under Windows 95 and 98 you can also use the command NBTSTAT -R.

Call charge allocation/callback

If HiPath HG 1500 establishes an ISDN trunk call, the charges incurred are allocated to the call number used. As long as this physical connection exists, data can be transferred in both directions. If a connection exists between HiPath HG 1500 A and HiPath HG 1500 B via the trunk, all HiPath HG 1500 A and B devices connected to the LAN can avail of the connection. In this case, the charges are allocated to the call number of the HiPath HG 1500 A board port which established the connection.

As standard with today's routers, call charges can only be allocated to the router call number and not to specific LAN devices or applications.

If the physical connection is cleared down via "short-hold", it is reestablished when new messages are received. If this takes the form of data fromHiPath HG 1500 B to A, i.e. HiPath HG 1500 B initiates connection setup, then call charges are allocated to B.

If the "callback" is activated, charges are allocated to the called party HiPath HG 1500 as the called party rejected the incoming call and actively re-establishes the connection (callback without a connection). Thus, no B channel is established. Identification is implemented via the call number entered in Setup or, in the case of analog stations via the DID number entered under "ISDN peer".

For information on further parameters, see → 50.

In some cases, dial-up connection can be only be manually initiated (e.g. short-hold is deactivated).

Internet access

One or more client PCs can simultaneously access the Internet directly using an Internet browser. The connection from the LAN is set up via ISDN or DSL. In general, access is possible from all PCs. Some providers block this option and access must be specially requested.

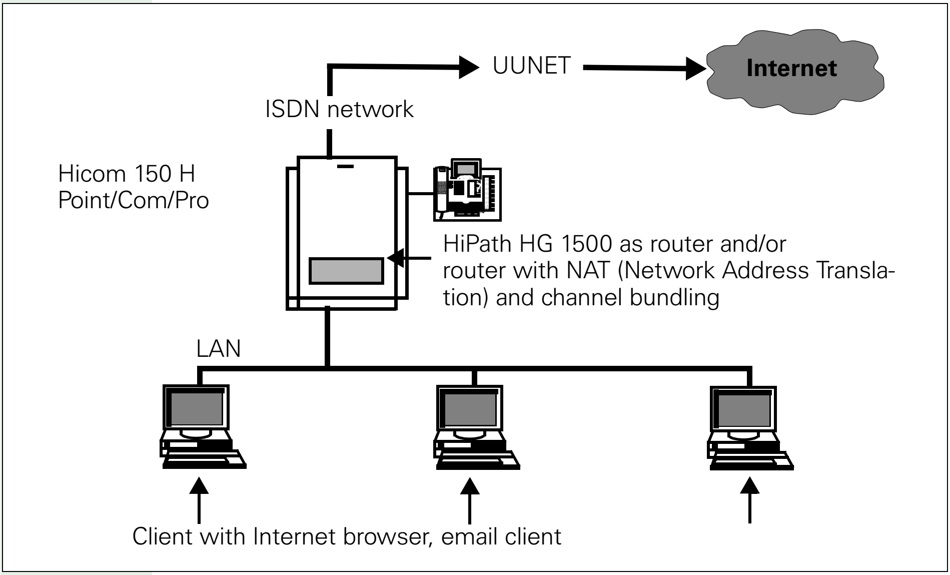
Access to the Internet provider takes place with the IP transport protocol via HiPath HG 1500.

All clients use the same provider.

Features

- Static or dynamic IP addresses
- Routing function with NAT/SUA (Network Address Translation/Single User Access)
- PPP multilink (channel bundling)
- PPPoE (for DSL)
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

HiPath HG 1500 and access to the Internet via a network provider


UUNET
Internet
ISDN network
Hicom 150 H Point/Com/Pro
HiPath HG 1500 as router and/or router with NAT (Network Address Translation) and channel bundling
LAN
Client with Internet browser, email client

Internet access via T-DSL (T-ISDN DSL)

Deutsche Telekom AG launched a new product at the end of 1999 which combines high-speed Internet access with enhanced T-ISDN DSL telephony features (also known as T-DSL).

At 768,000 Bit/s, TDSL users can download data from the Internet 12 times quicker than with a normal ISDN connection. Transmission rates of 128,000 Bit/s are achieved when sending files, i.e. the same as can be achieved by bundling two channels (lines) in a normal ISDN connection.

T-ISDN DSL is first and foremost a normal T-Net or ISDN connection as a multi-device or system connection.

Over and above the functions of the normal T-Net or ISDN connection, the T-DSL interface is a data interface for Internet connection with a speed of 768 kBit/s downstream and 128 KBit/s upstream. A T-Net or ISDN interface channel is not seized when using this data interface.

Function

In contrast to T-ISDN, the NTBA is not connected directly to the main station but rather downstream of a so-called "ISDN splitter" (BBAE). This device can be seen as a DSL-speed distributor between the ISDN interface and data transmission.

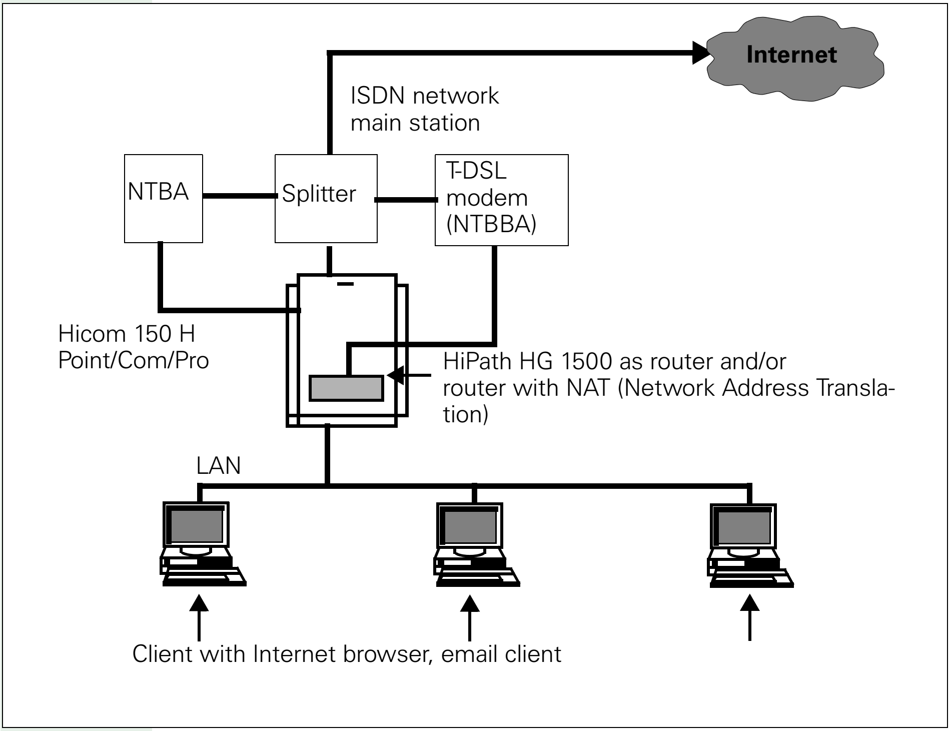
The splitter has a TAE jack to which the NTBA is connected. The connection to the Hicom 150H is set up in the conventional manner.

In addition, the splitter features a port for the "T-DSL MODEM" (NTBBA) which provides the interface for data transmission at T-DSL speed.

The "ISDN splitter", the "NTBA" and the "T-DSL modem" are supplied free of charge by Deutsche Telekom AG with every T-ISDN DSL connection.

The T-DSL modem is connected to the HLB board via a 10BT interface. The PPPoE (Point to Point Protocol over Ethernet) protocol is used for the connection.

Configuration example for T-DSL see → 123.


Internet
ISDN network
main station
NTBA
Splitter
T-DSL
modem
(NTBBA)
Hicom 150 H
Point/Com/Pro
HiPath HG 1500 as router and/or
router with NAT (Network Address Translation)
LAN
Client with Internet browser, email client

Configuring Internet access via PPP and NAT/SUA

A public IP address may not be used. Assign an IP address from the private network area.

Network interfaces

The use of IP address 0.0.0.0 with the network mask 255.255.255.248 is recommended when using ISDN3 interfaces.

Routing

IP-routing

➡ IP address:

The IP address 0.0.0.0 (ISDN3 IP address) is entered as the destination network.

➡ Network mask:

Enter the corresponding network mask.

➡ Gateway:

Enter the IP address from the ISDN3 network as the gateway. (e.g. 0.0.0.1)

ISDN peer

With the left mouse button, select "ISDN peer" and press "New."In the dialog window, enter the name of the provider and confirm your entry.

Select the new entry using the mouse.

➡ IP address:

Enter the IP address. This is the same as the address entered under "Routing - IP-routing", e.g. "0.0.0.1".

➡ B channels:

Enter the maximum number of B channels for this connection. (If there is more than one B channel the provider may encounter problems with password handling).

➡ PAP or CHAP:

For authentication on the provider side, enter the defined password under PAP or CHAP.

Ask your service provider for the other parameters required for successful connection setup. More information on these parameters is contained in the chapter “Administration with Assistant I”.

➡ Once the Internet access has been set up, you should verify that the connection also reverts to short hold mode when no more data traffic is required. If the connection remains open or if it is set up at regular intervals, then a customer trace should be performed, see → 171ff.

Function of NAT/SUA (Network Address Translation)

Non-public IP addresses are masked.

Non-public IP address range	Netmask	(Class)
10.0.0.0	255.0.0.0	A
172.16.0.0 - 172.31.255.255	255.240.0.0	B
192.168.0.0	255.255.255.0	C

Since these addresses are not routed via the Internet, these hosts must use HiPath HG 1500's WAN (ISDN) address that was previously negotiated with the ISP via PPP for exchanging data. As a result, hosts are invisible in the Internet as the data is exchanged completely via the NAT/SUA.

The internal corporate LAN operates on the Internet with only a single IP address, namely the address assigned by the provider for the dial-in time. This address and various port numbers are used to access the Internet from this LAN. This setting blocks all IP connection attempts (incl. attacks) to access the corporate LAN via the Internet, unless these were explicitly configured under "Routing->Internet“ (see → 55).

Configuring the PCs for Internet access

When using the Internet access directly via the board, two configurations must be performed on the PCs:

1. The board must be set as the default gateway from the PC perspective: The board's IP address is configured for the PCs under "Default Gateway" in Network Settings->TCP/IP.
2. A DNS server must be configured on the PCs for name resolution: Enter Network Settings->TCP/IP DNS server, e.g. a DNS server from T-Online: 194.25.2.129.

IP address mapping

As a result of Internet expansion, it has become common practice to use the short but globally unique IP addresses exclusively for the Internet and to use the so-called private (not public, see → 105) IP addresses for IP networks within companies.

Consequently, addresses from the same IP network can frequently be used in many companies.

The "IP address mapping" feature was developed to enable users to reach these addresses via a unique routing entry despite the multiplicity of entries.

For routing with specific partners defined during configuration, the HiPath HG 1500 exchanges the private IP addresses used in its own network for other IP addresses and can be contacted by external users via these IP addresses.

The following example explains this:

A service provider would like to provide server support for two different customers (A+B). Both of the customers selected 192.168.1.0 as the IP network address and each has a HiPath HG 1500. To ensure that the service provider can reach both customer networks, IP address mapping is activated in at least one customer network, or in this example, in both customer networks.

To round off the example, the service provider should only be able to access two IP addresses in the customer B's LAN.

The service provider (own network:192.168.100.0) configures the following routing:

Customer A: IP network address: 10.1.1.0, network mask 255.255.255.0

Customer B: IP network address: 10.1.2.0, network mask 255.255.255.0

The following is configured for customer A:

Basic settings->Mapping netmask: 255.255.255.0

ISDN peer "Service provider"->IP address 192.168.100.254, IP address mapping: yes

Routing->IP-routing->IP address: 192.168.100.0, network mask 255.255.255.0, gateway: 192.168.100.254

IP-mapping->external IP address: 10.1.1.0, internal IP address: 192.168.1.0

The service provider can now access the IP address 10.1.1.1 in customer A's system, e.g. via the IP address 192.168.1.1.

The following is configured for customer B:

Basic settings->Mapping netmask: 255.255.255.0

ISDN peer "Service provider"->IP address 192.168.100.254, IP address mapping: yes

Routing->IP-routing->IP address: 192.168.100.0, network mask 255.255.255.0, gateway: 192.168.100.254

IP-mapping->external IP address: 10.1.2.1, internal IP address: 192.168.1.200

IP-mapping->external IP address: 10.1.2.2, internal IP address: 192.168.1.201

The service provider can now access exactly two addresses in the customer's system:

the service provider can access the IP address 192.168.1.200 in customer B's system via the IP address 10.1.2.1,

the service provider can access the IP address 192.168.1.201 in customer B's system via the IP address 10.1.2.2.

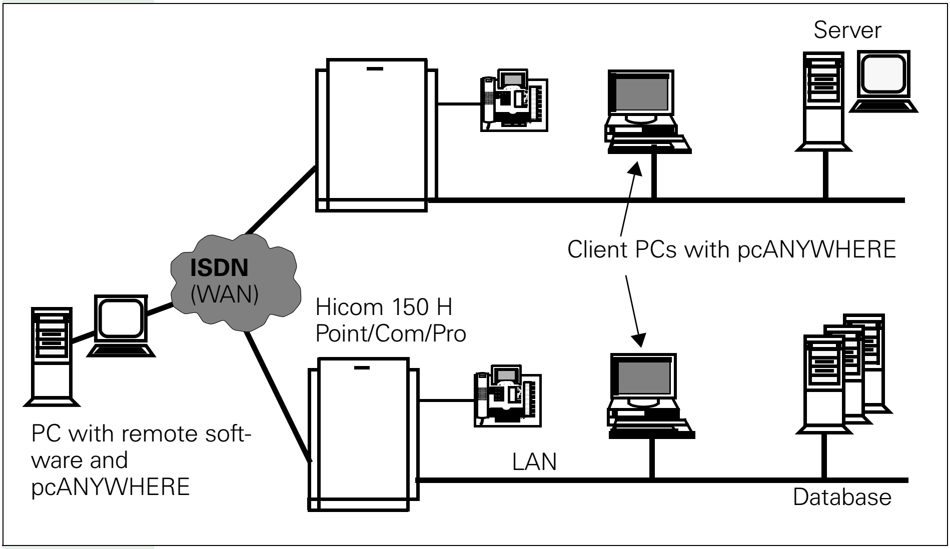
No other addresses in customer B's LAN can be accessed by the service provider.

The following applies both for NAT/SUA via ISDN3 and IP address mapping:
IP addresses are only exchanged in the IP header. This mechanism does not work if the IP addresses are exchanged on higher protocol layers, e.g. between the applications. This should be taken into consideration in the event of malfunctions which do not occur when this mechanism is not used (e.g. in the case of direct access via an ISDN card).

Remote control

Solution pcANYWHERE

Teleworking with HiPath HG 1500 and pcANYWHERE


Server
Client PCs with pcANYWHERE
ISDN
(WAN)
Hicom 150 H
Point/Com/Pro
PC with remote software and pcANYWHERE
LAN
Database

You can operate a PC in the network from an external PC with Symantec's pcANYWHERE software.

Prerequisite:

- Windows 95, Windows 98, Windows NT 4.0 or Windows 2000 as the operating system
- Connection setup with the IP or IPX transport protocol
- PC is operational (if applicable, screen is dark)

Safety mechanisms ("Security")

General information

An access authorization is required for the routing function to control access via HiPath HG 1500 from the internal LAN to the ISDN and vice versa.

A "firewall" is not practical for telematic functions. Rules (e.g. trunk access) can be saved in Hicom for these functions and their call numbers.

The following information is intended specifically for the router (HiPath HG 1500).

Call number verification (incoming only)

Verification of the call number of the calling station (station authentication, configurable) and the IP or IPX address to prevent unauthorized external connections via ISDN.

Verification of the IP or IPX address (configurable) of internal LAN subscribers.

IP firewall (authorization firewall)

An IP firewall comprises the following two steps:

- IP routing authorization
  The IP routing authorization procedure checks and, where applicable, rejects packages on the basis of the source and destination IP address and the ports used. The IP addresses can be network addresses or individual hosts.

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

IPX firewall

IPX packets are only valid if the specified network number/node address combination corresponds to that of the sender.

Firewall

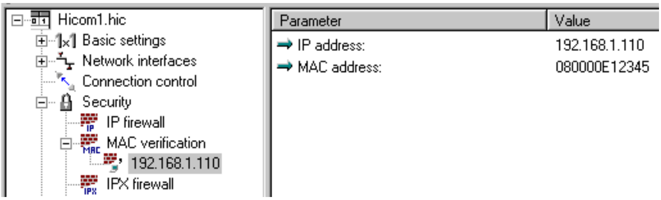
A firewall is a barrier which protects against unauthorized access. In this case, the internal LAN (LAN1), for example, should be protected against external access (e.g. Internet-based access via DSL).

The objective of a firewall configuration is to allow individual, specified computers to access an non-secure network (e.g. Internet). The firewall should prevent 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 question is a so-called authorization firewall. In other words, as soon as the firewall is activated, only configured components can access board services. Each board service is automatically rejected for all unentered LAN components.

WARNING: the activation/deactivation of firewall parameters can cause dramatic restrictions in terms of board functionality (e.g. LAN-based administration may not be possible any more) or enable access to sensitive data.

Configuring a MAC firewall



Parameter	Value
IP address:	192.168.1.110
MAC address:	080000E12345

A MAC firewall is responsible for authorizing access to board services for specific MAC/IP address combinations only. The protection offered here lies in the "non-configurabilty" of a MAC address. A restriction of the available Internet services has **not** yet been achieved

To configure MAC verification, you need a list of the MAC and IP address combinations of the installed LAN cards which should have access to the board services. You will find the MAC addresses in the documentation provided by your Ethernet card manufacturer.

Proceed as follows for configuration:

Expand the firewall menu in the menu tree (click the plus sign in front of Security) and confirm the warning with OK. The click the MAC verification menu entry and press the "INS" key. You are then asked to enter an IP address which will be included in the verification. After confirmation with OK you must enter and confirm the associated MAC address.

Then repeat this procedure for each individual MAC/IP address combination.

To correct MAC/IP address combinations, you can select the entry to be corrected by expanding the list of configured combinations (click the plus sign in front of MAC verification) and then select the required IP address. You can now open an edit mask in the right window by double-clicking the required entry and then enter your changes.

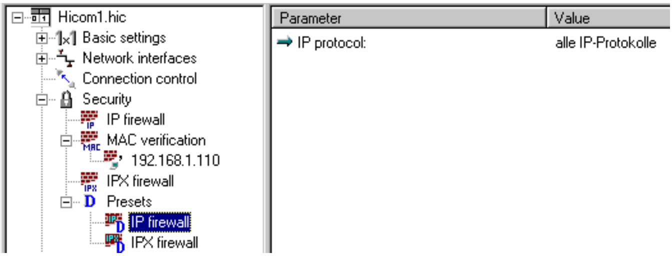
If you want to delete an entry (i.e. the appropriate rights should be withdrawn from the PC), the IP address is simply selected in the expanded menu tree and deleted with "DEL".

Configuring an IP firewall

An IP firewall can grant individual or groups of IP addresses access to specific goals (for the sake of simplicity, this manual assumes one IP address only; however it is also possible to delete entire networks). This is also an authorization list, i.e. only IP addresses that are listed here are assigned access to the defined services. The IP firewall can check IP protocols and the associated services (port numbers).

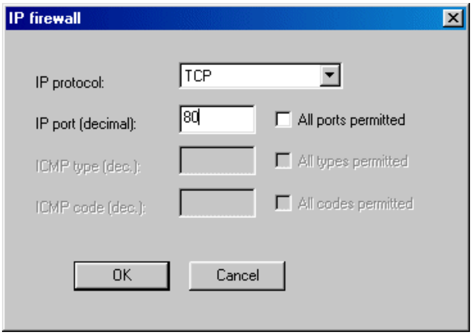
To be able to define an exact selection of the required function, you must, where applicable, know the authorizing protocol and the port number in addition to the IP address of the destination.

Presets



Parameter	Value
IP protocol:	alle IP-Protokolle

"Presets“ are useful when multiple IP addresses are to be configured with the same restrictions. To do this, expand the Presets entry under Security and select IP firewall. Now select "IP protocol" in the edit window and enter the required settings:


IP firewall

IP protocol: TCP

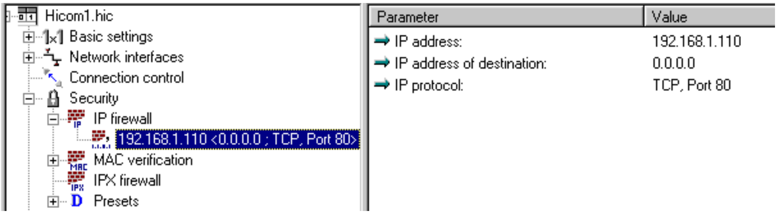
IP port (decimal): 80 ☐ All ports permitted

ICMP type (dec.): ☐ All types permitted

ICMP code (dec.): ☐ All codes permitted

To permit Internet surfing (HTTP protocol), for example, enter the TCP protocol here and set 80 as the "IP port". You can also use the prepared presets; in this case, all protocols are permitted without port filter functions. These configured presets are now used for the IP addresses to be entered.

Configuring IP addresses



Parameter	Value
➡ IP address:	192.168.1.110
➡ IP address of destination:	0.0.0.0
➡ IP protocol:	TCP, Port 80

The required authorizations can then be found under the menu tree item "Security, IPFirewall". As described previously, select IP firewall and press the "INS" key. Enter the IP address which is to be assigned specific access rights. Once you have confirmed the input with OK, you can select the IP address (see fig.) to make additional restrictions or to correct the IP address. If you want to withdraw all rights from this IP address, select the entries and delete them with the "DEL" key.

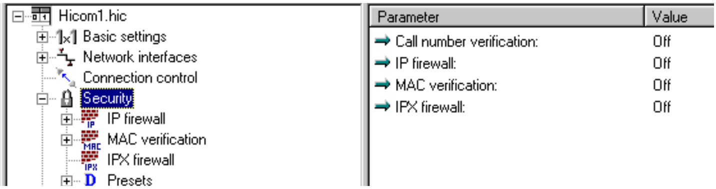
In the presetting, the IP address entered has full authorization and can thus reach all IP addresses and use all services. To make additional restrictions, you must perform the following steps:

For the current settings and restrictions for an IP address, select the IP address (under Security, IP firewall) in the menu tree. The selected IP address as well as the "IP address of destination" which this IP address may contact and the permitted protocol are displayed in the edit window. The entry 0.0.0.0 under IP address of destination applies to all destinations. If the selected IP address is only to be able to communicate with a specific network and host, double-click "IP address of destination". You can now enter the required destination network or the appropriate host in the following input mask.

If you want to enter restrictions for the protocol and/or port, double-click the entry "IP protocol". You can select the required protocol ("all IP protocols", "TCP", "UDP" or "ICMP") in the following mask. Depending on the selected protocol, you can also enter a restriction for the IP port, where applicable, in the form of a decimal number or select "all Ports allowed". Restrictions in the form of "ICMP type" and "ICMP code" can also be entered for the ICMP protocol.

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).

Activating the firewall



Parameter	Value
➡ Call number verification:	Off
➡ IP firewall:	Off
➡ MAC verification:	Off
➡ IPX firewall:	Off

WARNING: the complete firewall is deactivated in the default version. The firewall functionality must therefore be explicitly activated. All previous settings only take effect after this activation.

To activate the firewall, first select Security in the menu tree and then select the required security function (IP firewall or MAC verification). Double-click the security function to switch between "On“ and "Off".

The CDB is transferred to the board once all settings have been made.

Gatekeeper

A gatekeeper performs the following functions in a H.323 network:

- Registers H.323 terminals,
- Administers rights and services,
- Converts call numbers into logical names or IP addresses and vice versa,
- Administers the bandwidths on the network side,
- Registers gateways,
- Registers multi-conference units,
- Can be networked with neighboring gatekeepers (zones).

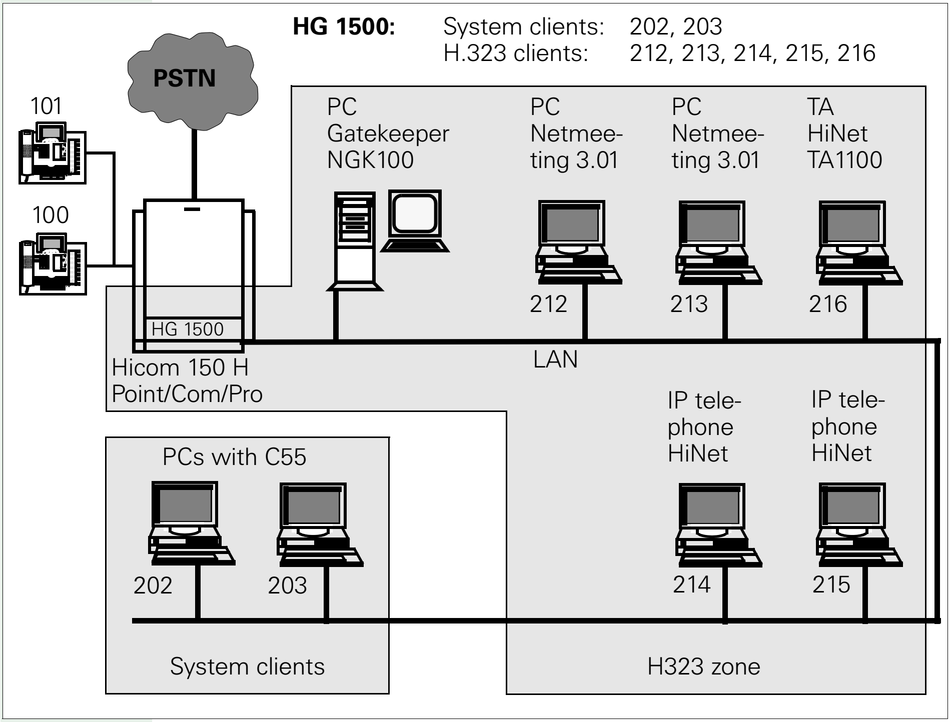
IP telephony can be implemented in H.323 networks even without gatekeepers, if no gateways or multi-conference units are operated. In this case, connections can only be set up via the IP address. Authorizations and bandwidth verification is not possible.
The following is generally applicable: without a gatekeeper, features are not available or seriously restricted.

A distinction is made between the following stations:

- Group 1: stations directly connected to the Hicom (Optisets, POT, CMI, etc.) as well as stations registered at HiPath HG 1500 (system clients or optiClient 130, optiPoint Ipadapter and VCAPI clients) and all line accesses
- Group 2: stations registered at the gatekeeper (H.323 clients such as Netmeeting 3.01, HiNet LP 5100 or optiPoint 300 advance, HiNet TA1100 or HiPath AP1100)

To reach a port (station/line) in group 1, all stations in group 2 must use a code. This code is removed by HiPath HG 1500 in the direction of Hicom and inserted in the opposite direction, i.e. stations in group 1 do not dial the code. The code must be configured as a service in the RADVision gatekeeper NGK100 (see Service Manual) and as a gateway prefix with HiPath HG 1500 in Assistant I (see → 65).

Gatekeeper with a HiPath HG 1500



Different types of H.323 applications can be operated at HiPath HG 1500.

The C55-Opti stations are not registered at the gatekeeper and are configured as “system clients” via Assistant I. Since HiPath HG 1500 is configured for gatekeeper operation, messages are still exchanged during each C55-Opti connection between HiPath HG 1500 and the gatekeeper, as demonstrated at the gatekeeper by the figures and statistics on bandwidth use and call logging. The C55-Opti stations reach the other stations by dialing the internal call number without using a prefix.
If, for example, station 202 calls station 101, one DSP channel is seized.
If station 202 calls station 212, two DSP channels are seized.

The H.323 clients are configured for gatekeeper operation. Together with the gatekeeper and HiPath HG 1500 as the gateway, they form a H.323 zone. These stations must be configured as "system clients" in HiPath HG 1500. The IP address associated with the call number must be configured as "255.255.255.255,"as the gatekeeper assigns the call number and IP address. The stations are mobile (different PCs can be used as workstations, teleworking) as a result of registration at the gatekeeper. The gatekeeper can be operated in the modes "direct routed" and "gatekeeper routed."

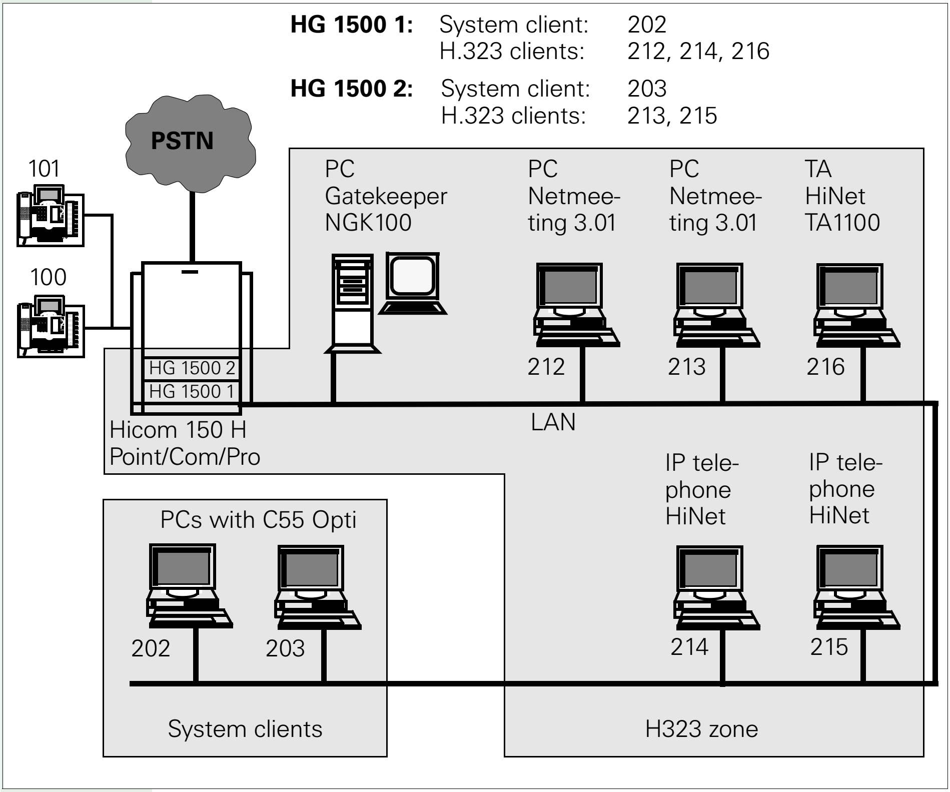
The H.323 clients can only address the HiPath HG 1500 gateway via a "service" that must be configured in the gatekeeper and assigned to the stations. The service code must correspond to the gateway prefix that is configured via Assistant I and registers HiPath HG 1500 at the gatekeeper during startup.

In the example, the gateway prefix in HiPath HG 1500 and service code in the gatekeeper are configured as "0."Multi-digit codes are possible, but the code can only contain digits. HiPath HG 1500 can only be reached via a prefix. The call numbers that are forwarded to the clients are extended to include the prefix so that the call number to be dialed is displayed and dialing from caller lists is possible.

Station 212 can reach station 214 in two ways. If the number "214" is dialed, the call takes place directly on the LAN, if the number"0214"is dialed, the call takes place via the H150E using two DSP channels in HiPath HG 1500. The Optiset and C55-Opti stations can be reached by dialing "0101" or "0203."

H.323 clients that do not support a gatekeeper can also be configured in HiPath HG 1500. To do this, the IP address associated with the call number must be administered under "H.323 clients."The station is not mobile. H.323 clients can be operated in mixed mode with and without gatekeeper link to HiPath HG 1500 when the gatekeeper is operated in "direct routed" mode. Clients that have gatekeeper support must also be operated in this mode if a gatekeeper is implemented.

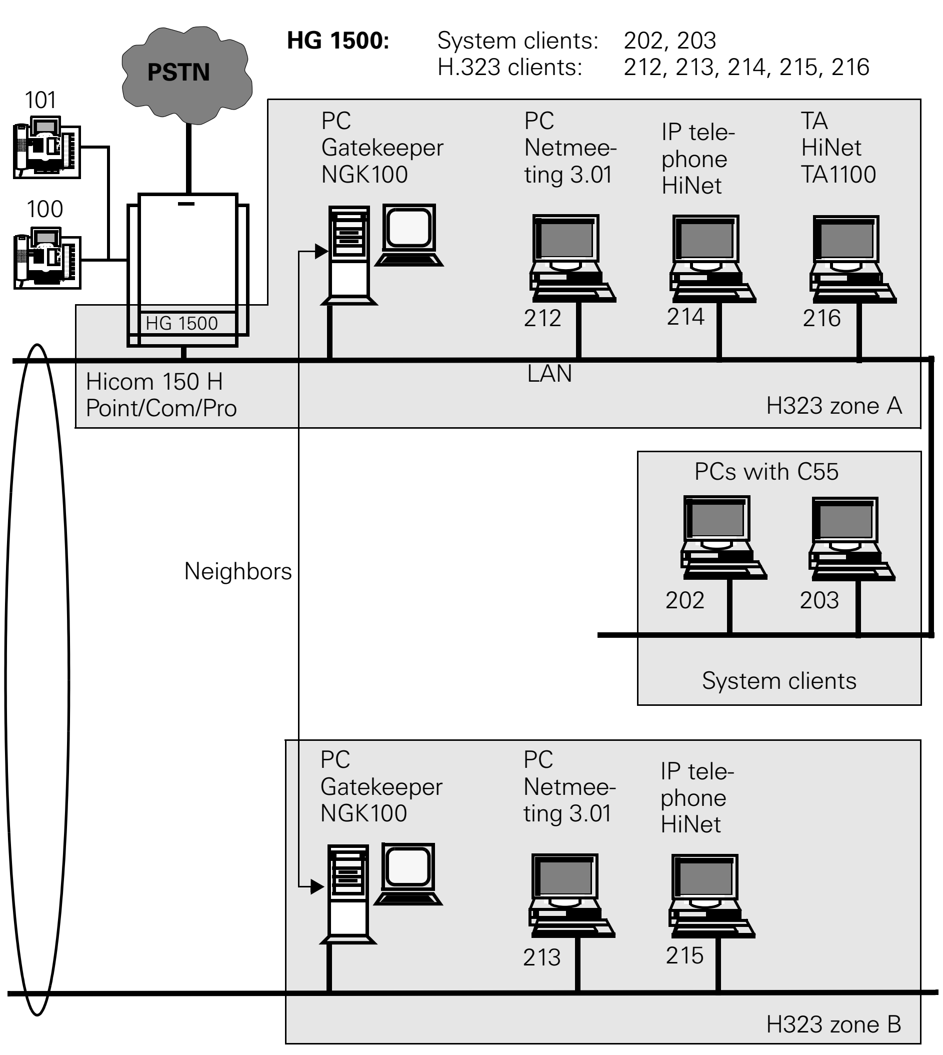
Gatekeeper with multiple HiPath HG 1500s



HG 1500 1:	System client:	202
	H.323 clients:	212, 214, 216
HG 1500 2:	System client:	203
	H.323 clients:	213, 215

Multiple HiPath HG 1500s can be registered at a gatekeeper, e.g. in order to administer a large number of stations. The stations must be distributed on HiPath HG 1500 as depicted above. The stations always conduct calls via the HiPath HG 1500 at which they are logged in. Load balancing is not performed, i.e. if there is no DSP resource free on the home HiPath HG 1500, the call is not set up via another HiPath HG 1500 with free DSP channels. The HiPath HG 1500s do not have to be configured with the same gateway prefix/service as in the example.

Multiple gatekeepers with one HiPath HG 1500 and multiple H.323 zones



Multiple H.323 zones can be configured with multiple gatekeepers. The HiPath HG 1500 is registered in H.323 zone A as a gateway. The gatekeepers must be configured as neighbors so that the stations can reach each other. The gatekeeper can be operated in mixed “direct routed” and “gatekeeper routed" mode. The stations in H.323 zones A and B can address the H150E stations by dialing the prefix “0.”

A separate HiPath HG 1500 can also be provided for each H.323 zone. The stations must be distributed on HiPath HG 1500 as depicted above. The HiPath HG 1500 prefixes may be identical or not. Load balancing is not supported by this configuration.

Even if clients without gatekeeper support are operated at HiPath HG 1500, the gatekeeper must be able to reach them via IP in gatekeeper mode, i.e. IP-routing from and to the gatekeeper must be possible from these clients (verification with ping to gatekeeper).

Using SNMP

An MIB browser (available with Hewlett-Packard’s "Network Node Managers") is required for using SNMP functionality (MIB: Management Information Base).

The SNMP functions include:

- With MIB browser and standard MIB (based on RFC1213):
  – querying and modifying standard MIB 2 parameters
- With MIB browser and private MIB:
  – querying and modifying Hicom HiPath HG 1500’s private MIB parameters
- With Assistant I:
  – defining communities of standard parameters (classes of service)
  – defining trap communities and stations to which the traps are sent
  – defining the trap level for various trap groups (error sensitivity)
- With trap receiver:
  – receiving traps

MIBs also contain a brief commentary explaining the meaning of each parameter.

The following is a list of some parameters:

- mgmt->mib-2->system->sysUpTime: time since the last HiPath HG 1500 startup
- HLB2MIB->siemensUnits->pn->hlb2mib->controlGrouphlb20->sysSoftwareVersion: SW release of the module
- mgmt->mib-2->ip->ipRouteTable: HiPath HG 1500 routing table

HiPath HG 1500 sends SNMP traps (diagnostic and error messages) to the stations configured under "SNMP->Trap communities. These messages are transmitted in accordance with the severity levels set under "SNMP".

Examples of traps generated by HiPath HG 1500:

A) Generic traps - cannot be deactivated:

- warm start
- cold start
- authentication failure

B) Enterprise traps - can be configured

- data init (WARNING - forced reinitialization of data)
- memory low (WARNING - memory resources below the threshold)
- duplicate mac (MINOR - duplicated MAC address)
- ip firewall (WARNING - IP firewall violation)
- mac firewall (WARNING - MAC firewall violation)
- isdn access (WARNING - ISDN access verification)

Configuration examples

This chapter describes a variety of standard configurations which make HiPath HG 1500 easier to administrate and prevent certain problems.

Internet provider

The following describes how to set up an Internet connection.

Example: UUNET

Client setting

Protocol IP
IP address 192.168.30.3
Netmask 255.255.255.0
Standard gateway 192.168.30.254
DNS 192.76.144.66

Microsoft Internet Explorer 4 settings

Under Connection

1. Activate Connect using a proxy server.
2. Address of proxy server to use: Port
3. HTTP: www-proxy.de.uu.net: 3128

By navigating

1. Page: home page
2. address: http://www.uunet.de

HiPath HG 1500 setting

Active LAN and ISDN1/2/3 Internet network interfaces

Network interface ISDN3:

- IP address 0.0.0.0
- Network mask 255.255.255.248

IP-routing:

- IP address 0.0.0.0
- Network mask 255.255.255.248
- Gateway 0.0.0.1

ISDN peer:

- IP address 0.0.0.1
- Set B channel to 1
- Tick CHAP: User ID XXX, password XXX
- Call number 00211917822 outgoing

In general, access is possible from all PCs. Some providers block this option and access must be specially requested.

Configuration examples

Example: T-Online/ISDN

The following must be observed when configuring T-Online as a provider:

The authentication protocol PAP must be set for the ISDN peer, the host button must be activated.

The user ID consists of:
<port ID><T-Online no.>#<user ID>

Example:

- Port ID: 000123456789
- T-Online number: 02302666555
- User ID: 1

The user ID is then: 00012345678902302666555#0001

The password is the personal ID.

Example: T-Online/T-DSL

This data is supplied by T-Online

- Port ID: 000123456789
- T-Online number: 02302666555
- User ID: 1

Proceed as follows to perform configuration:

PAP is set as the authentication protocol. The host button must be activated.

The user ID consists of:
<port ID><T-Online no.>#<user ID>

The user ID is then: 00012345678902302666555#0001

The password is the personal ID.

Accordingly, enter the following menu entries:

Network interfaces->Active network interfaces: LAN2/DSL active

IP address: 172.16.16.16 (wildcard for DSL access)

IP network mask: 255.255.255.255

Data packet length: 1492

Provider name: T-Online.de

PAP:

HOST_Button activated
User ID:
comprising:
<Port ID><T-Online no.><#<User/suffix>
@t-online.de:
00012345678902302666555#0001@t-online.de
password:
The password is the personal ID.

CHAP: deactivated
NAT: activated

Short hold time: as required

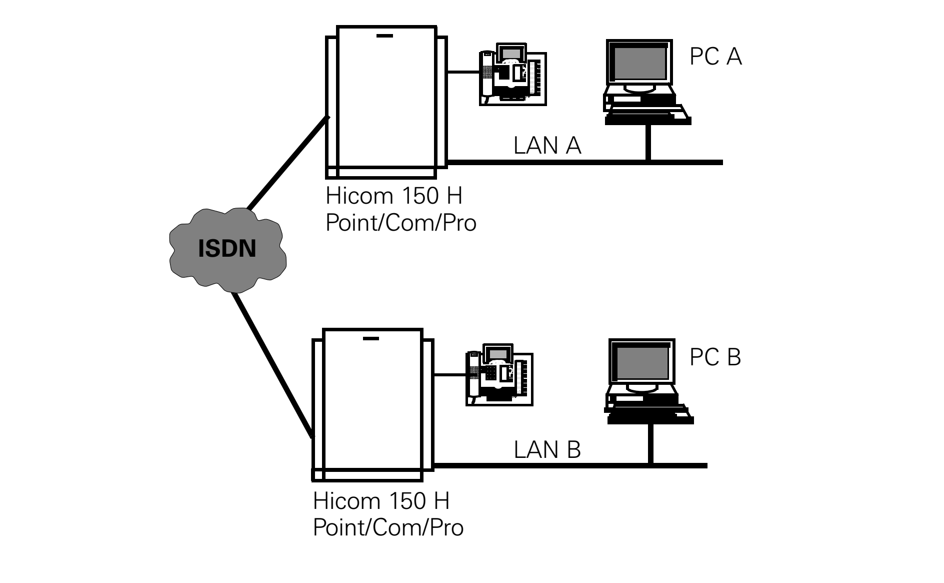
in the case of a flat-rate option
short-hold mode: deactivated
can also be configured
These parameters can be configured as required and on the basis of the applicable tariff structure.

Throughput rate: 128
This corresponds to the data rate in kBit/s which can be sent to the Internet on the DSL interface.

Routing->IP-routing
IP address:0.0.0.0
Network mask: 255.255.255.0
Gateway: 172.16.16.16 (same address here as under Network interfaces->Network interfaces->DSL->IP address) see page 105

Routing HiPath HG 1500 to HiPath HG 1500

LAN-LAN connections, i.e. WAN connections can be established using HiPath HG 1500 via ISDN dial-up lines. The partner in this instance can also be a third-party router. In this case, the configuration of the B-side must be altered in accordance with the third-party manufacturer's configuration instructions.



Configuring HiPath HG 1500 A

- PC A: IP: 218.20.56.181
  Sub-network: 255.255.255.0
  Gateway: 218.20.56.254
- HiPath HG 1500 A
  LAN IP: 218.20.56.254
  Sub-network: 255.255.255.0
- HiPath HG 1500 A
  ISDN1 IP: 218.20.60.1
  Sub-network: 255.255.255.0
- Routing A IP: 218.20.55.0
  Sub-network: 255.255.255.0
  Gateway: 218.20.60.2
- ISDN peer A
  Name: LB2
  IP: 218.20.60.2
- B channel: 1 call number list
  A 0831396809 incoming
  00831396809 outgoing

Configuring HiPath HG 1500 B

- PC B: IP: 218.20.55.181
  Sub-network: 255.255.255.0
  Gateway: 218.20.55.254
- HiPath HG 1500 B
  LAN IP: 218.20.55.254
  Sub-network: 255.255.255.0
- HiPath HG 1500 B
  ISDN1 IP: 218.20.60.2
  Sub-network: 255.255.255.0
- Routing B IP: 218.20.56.0
  Sub-network: 255.255.255.0
  Gateway: 218.20.60.1
- ISDN peer B
  Name: LB2
  IP: 218.20.60.1
- B channel: 1
- Call number list
  A 0831396820 incoming
  00831396820 outgoing

Example: the following test should be performed once the example cited above has been configured:

- PC A Ping to LAN A 218.20.56.254,
- PC A Ping to ISDN1 A 218.20.60.1,
- PC A Ping to ISDN1 B 218.20.60.2,
- PC A Ping to LAN B 218.20.55.254,
- PC A Ping to PC B 218.20.55.181.

Host routing

Host routing / routing without transfer network

A LAN-LAN connection via IP usually involves three IP networks: LAN A, LAN B and an IP transfer network that is configured between the two routers in the WAN (Wide Area Network) (on HiPath HG 1500 via the ISDN interface).

Transfer network configuration is not required in LAN-LAN connections. The partner should support this.

The following example shows the configuration:

- LAN A with the network address 192.168.1.0.
- LAN B with the network address 192.168.2.0.

Each of the LANs contains a HiPath HG 1500.

LAN	NW IP address	Network mask	HiPathHG1500 IP address
A	192.168.1.0	255.255.255.0	192.168.1.254
B	192.168.2.0	255.255.255.0	192.168.2.254

The ISDN1-3 interface of both modules can be configured as required. They are not used for this scenario.

Parameter HiPath HG 1500	LAN A	LAN B
Routing->IP-routing		
IP address	192.168.2.0	192.168.1.0
Network mask	255.255.255.0	255.255.255.0
Gateway	192.168.2.254	192.168.1.254
Routing->ISDN partner		
Name	Partner LAN B	Partner LAN A
IP address	192.168.2.254	192.168.1.254
Suppress IP address	yes	yes

The following entry is necessary for accessing an RAS workstation (remote workstation) from LAN A with the IP address 192.168.50.1:

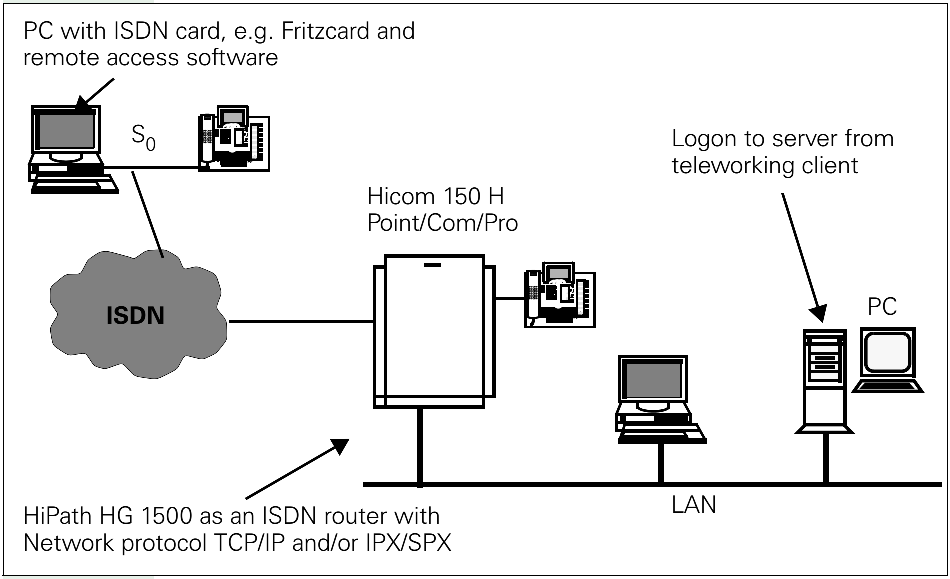
Parameter HiPath HG 1500	LAN A
Routing->ISDN partner	
Name	Partner RAS
IP address	192.168.50.1
Suppress IP address	yes

This example shows that no ISDN interface is configured. The necessary entries in the router are dynamically created and not displayed in the CDB. The negotiation of an IP address in the IP transfer network is deactivated with the switch "Suppress IP address".

According to the procedure described above, up to eight entries can be used.

Remote Access Service (RAS)

Teleworking with HiPath HG 1500


PC with ISDN card, e.g. Fritzcard and remote access software
S_0
ISDN
Hicom 150 H Point/Com/Pro
Logon to server from teleworking client
PC
LAN
HiPath HG 1500 as an ISDN router with Network protocol TCP/IP and/or IPX/SPX

Settings with HiPath HG 1500

To use a PC for teleworking with HiPath HG 1500 via ISDN, the following steps must be completed in the administration program:

First define the IP address of the RAS/teleworking PC (must be in WAN (ISDN)).

Routing

ISDN peer

With the left mouse button, select "ISDN peer" and press "New.“In the dialog window, enter the name of the ISDN peer and confirm your entry.

Select the new entry using the mouse.

➡ IP address:

Enter the IP address of ISDN-RAS/teleworking.

➡ B channels:

Enter the maximum number of B channels for this connection.

The following software can be implemented:

Dial-Up Networking

You can install Dial-Up Networking under Windows 95/98, NT 4.0 and Windows 2000. An ISDN card is required for this purpose e.g.: AVM Fritzcard with CAPI port driver.

Disadvantage of Dial-Up Networking (depending on the Windows version)

- Only a single-channel connection is possible in the standard version of Dial-Up Networking.
- When accessing network resources, the connection must be set up manually.
- The connection must be reactivated manually after connection clear-down with short-hold.
- IPX connection to Novell servers is not possible.
- Dial-Up Networking does not support callback without connection.
- With Windows 95, a dual-channel connection is only possible with Dial-Up Networking Version 1.3 or with the expansion file Demsisdn.exe (see the Microsoft home page on the Internet).

Configuring Dial-Up Networking

Before you can configure Dial-Up Networking, the NDIS-WAN driver must be installed under Network Properties. TCP/IP is provided as the protocol. IP addresses do not have to be entered in the Network properties. Next, you can install the components necessary for Dial-Up Networking by selecting the My Computer icon followed by Dial-Up Networking.
The IP addresses are entered in connection control after the installation of Dial-Up Networking, i.e. a different IP address can be used for each connection. The IP address of the ISDN side of HiPath HG 1500 is specified as a gateway.

The connection can be set up via the My Computer icon and Dial-Up Networking.
If the PC is configured in Network Properties as a member of a domain, the option Logon using Dial-Up Networking can be used in the logon window when starting up the system.

One disadvantage of Dial-Up Networking is that after each clear down, the connection (short-hold) must be reestablished, or the logon screen appears.

ITK Columbus Client Pro

You can install ITK Columbus Client Pro (ITK ix1 connect ws) under Windows 95/98 and NT 4.0. Connections with 1 or 2 channels are possible. The advantage of this compared to Dial-Up Networking is that callback and automatic connection setup are possible when accessing network resources. You can also access Novell networks and create connections with 1 or 2 channels.

Advantage compared to Dial-Up Networking:

- Callback and automatic connection setup possible when accessing network resources.
- Logon and access to Novell networks possible with IPX.

Configuring ITK clients

An ISDN card must be installed with the associated CAPI interface.

The ITK client is installed via the ISDN card using the diskettes supplied.

A new adapter is added under Network properties during installation. The option "No support for Netware" can be selected if this is not necessary. TCP/IP is then the only protocol selected.

The IP address and the gateway (IP address of the ISDN side of HiPath HG 1500) are entered in Network properties for the ITK adapter during installation.

The appropriate connection to HiPath HG 1500 is configured via the program connection control. Multilink (two-channel connection) and callback can be configured here under PPP Options.

If you want the PC to log on to a domain when it starts up, you can specify this in the general settings. A connection is then automatically set up when the PC is started up and the user can log on to the domain as if he/she were connected locally to the network.

The connection is cleared down in the background while the user is working on the PC (short-hold). The ITK client automatically re-establishes the connection as soon as the user accesses any network resources.

AVM Netways (as of Version 3.0 Revision 3)

(The configuration examples given here are valid for Version 3.0.)
You can implement AVM Netways under Windows 95 and NT. Connections are only possible with one channel, and Netways only operates with AVM cards.

Advantage compared to Dial-Up Networking:

- Callback and automatic connection setup possible when accessing network resources.
- Logon and access to Novell networks possible with IPX.

Configuring the AVM client

An AVM-ISDN card must be installed in the associated CAPI interface.

Installation is performed via a setup menu. Queries include whether or not System Service is to be activated. In general, this is only required if the customer wants to log on to a domain. (If this is activated, Netways is always started up and cannot be closed.)

A new adapter is added under Network properties during installation. The IP address of the client and the gateway (ISDN side of HiPath HG 1500) is set here.

When you have finished making entries under Network properties, do not restart the PC but wait for Netways to be activated for the first time - this action will automatically restart the PC.

The IP address is entered once more under Addresses in Netways during configuration.

A new connection is configured under Targets for the connection of HiPath HG 1500. The protocol is set to PPP. The option Netbios via IP filter under the advanced settings for IP must be deactivated. IPX is also deactivated in this case (RAS client for NT network only).

Multilink (multichannel connection) is only available as of Version 4.

If callback is used, this is set to Remote under the advanced settings for COSO.

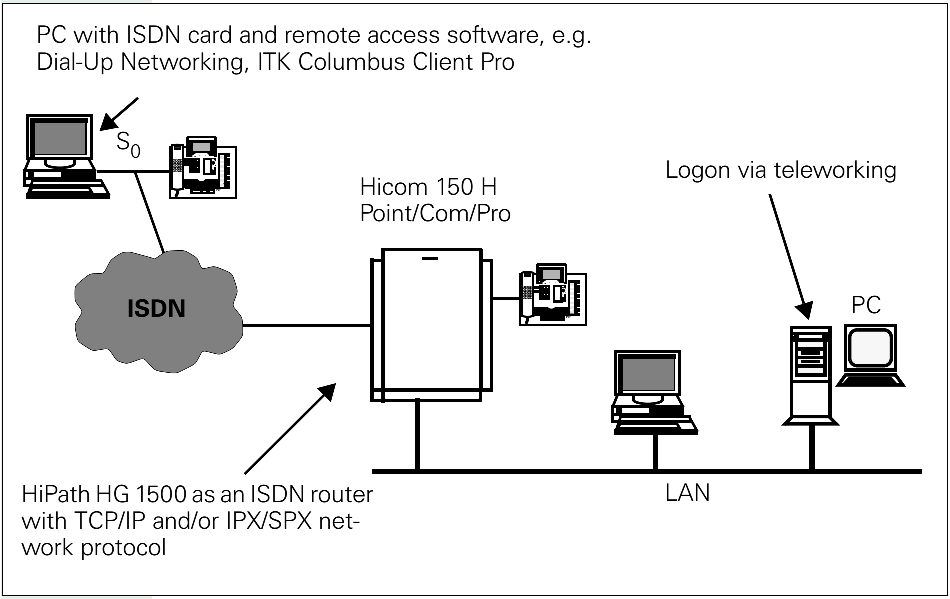
If you want to log on to a domain from the NT workstation when starting up the system, you can change the setting to "Dial" under "Operation Mode for Autoconnect" in the configuration in Netways, and the system searches for a connection to HiPath HG 1500. System Service must be set to Enable under Netways ISDN Service Setup.

A connection to HiPath HG 1500 is now automatically set up when you start up the PC and you can log on to the domain as if you were connected locally to the networked PC.

The connection is cleared down in the background while the user is working on the PC (short-hold). The AVM client automatically re-establishes the connection as soon as the user accesses any network resources.

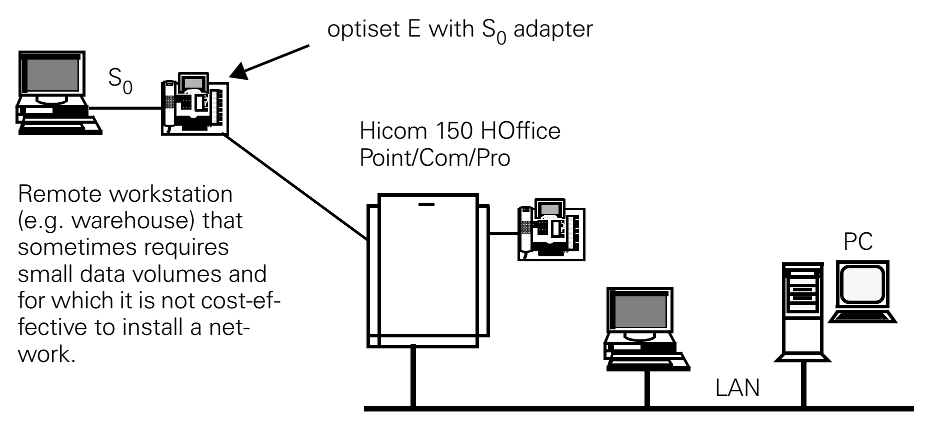
Solution: I-View under Windows 95

Teleworking with HiPath HG 1500 and I-View


PC with ISDN card and remote access software, e.g.
Dial-Up Networking, ITK Columbus Client Pro
S_0
ISDN
Hicom 150 H
Point/Com/Pro
Logon via teleworking
PC
LAN
HiPath HG 1500 as an ISDN router with TCP/IP and/or IPX/SPX network protocol

Solution via S_0 adapter at optiset E

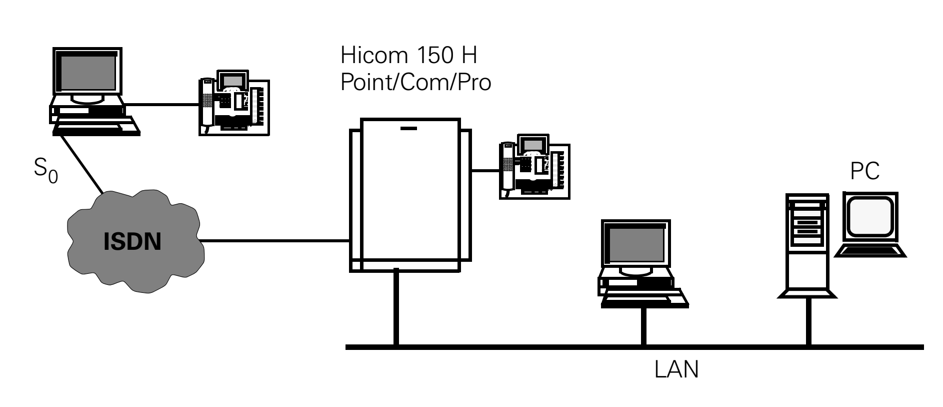
Teleworking with HiPath HG 1500 and optiset E



Remote workstation (e.g. warehouse) that sometimes requires small data volumes and for which it is not cost-effective to install a network.

Solution with Hicom Integrated

Teleworking with HiPath HG 1500 and S_0 telephone



Communication console with optiset E
Integrated software for CTI, call charge recording.

For administering the system PC with ISDN card and remote access software, e.g. I-View with Dial-Up Networking/ITK Columbus Client Pro.

Windows NT 4.0 Workstation with teleworking / RAS

HiPath HG 1500 can also be installed in a Windows NT network as an ISDN RAS router, for example. This means that the user can also access the network remotely via ISDN and can, where applicable, log on to a domain with a Windows NT workstation.

For this purpose, HiPath HG 1500 must only be configured as a router in the network and the appropriate remote peer must be entered.

The remote peers (in this case Windows NT workstation) require an ISDN card and the corresponding software.

Windows Dial-Up Networking can be used as the software. A suitable driver (e.g. in the case of AVM the AVM NDIS WAN CAPI driver) must be available for use as an adapter.

There is also special software available which facilitates RAS access. ITK Columbus Client Pro (ITK ix1 connect/WS for Windows NT 4.0) and AVM Netways for Windows NT are described here.

Advantage compared to Dial-Up Networking:

- Multilink (2 ISDN channels, ITK only),
- Short-hold (automatic call setup/cleardown when accessing the network) and
- Callback can be used.

Teleworking with logon at NT domains

You must first create an LMHOSTS file containing the names and IP addresses of the domain and server.
The user name used for logon on at the workstation must have an account at the domain.

Example for LMHOST entry

192.168.150.1 NTSRV1 #DOM:NTDOM1

First, configure the network as a member of a workgroup only, where the name of the workgroup is identical to the name of the domain.

You can enter the network as a member of a domain in Network properties once the connection has been set up (via ISDN) to the network or domain.

You can then use the dial-up client, ITK client and AVM client to automatically log on to the domain when the workstation is started up via ISDN.

You can access computers and servers directly in the network environment by logging on to the domain. You do not need to use the function "Find computer..." to establish network connections to other computers.

HiPath HG 1500, IPX routing and teleworking with Novell

IPX routing (Novell NetWare) and teleworking on the Novell server

Prerequisite:

The Ethernet_II frame type must be connected on the Novell server to enable IPX routing and teleworking on the Novell server via HiPath HG 1500. You can bind this frame type in addition to the existing frame types, however the network address for the connected Ethernet_II frame type of HiPath HG 1500 must be used. (These settings are normally made by the system administrator.)

HiPath HG 1500 settings:

In order to activate IPX in HiPath HG 1500, the IPX network number of the LAN (see above) must be entered in the "LAN" network interface. The IPX node (MAC address) is preset in HiPath HG 1500 and cannot be changed.

In order to activate IPX for this interface as well, the IPX network number and the IPX node for the ISDN side must be entered in the "ISDN1" network interface (see above).

ISDN/IPX network number = network number for the virtual "ISDN network segment". This must be identical for routing peers (HiPath HG 1500 / router) which are to work together.

ISDN/IPX node = this is the address which identifies each peer/user. It must be unique to each peer. (In the LAN, this is preset by the network card where it is normally not enabled). When this number is assigned, the first 2 digits from the left should be 02, so that it is obvious that the number has been allocated.

(Once these settings have been completed, the "Display networks" command on the server console can be used to determine whether the IPX protocol has been correctly configured. The IPX address of the ISDN network should now also appear.)

Under Routing, the remote stations for IPX routing and the teleworking PCs must be entered for "ISDN peer".

IPX routing peer:

For IPX, the "Node address" must be specified in the peer entry. This is the address which the peer entered as "IPX node" in his "ISDN1 interface". (Similar options are available from third-party routers)

If no additional IP-routing is activated, "System start behavior" must be set to "Automatic connection" so that a connection is established to the peer after the customer database is loaded. This also enables IPX routing information to be exchanged between both networks.

If additional IP-routing is activated, the connection can be set up via a Ping to the peer.

The short-hold should be increased to 60 (seconds), so that all IPX routing information can be exchanged.

The other settings (multilink, B channels, callback, etc.) correspond to the IP-routing settings.

Peer for teleworking:

A "Node address" must also be entered here. This must be the same node address (MAC address) entered in the teleworking software.

The other data corresponds to that of teleworking with IP, whereby both are possible together here.

Note on using IP and IPX:

The following should generally be observed when using IP and IPX:

If IPX and IP are enabled in HiPath HG 1500 A for the peer B, HiPath HG 1500 B must also enable these for peer A. If IPX (or IP) only is enabled in HiPath HG 1500 A for peer B, HiPath HG 1500 B may also only enable IPX (or IP) for peer A. The same applies for teleworking PCs (note teleworking PC settings).

Note for teleworking

A special software is required for the client PC for teleworking under Novell. This is because access via Microsoft Dial-Up Networking is not possible (a node address cannot be entered).

The software Netways from AVM facilitates logon onto a Novell server and is also certified. As this can only be operated with an AVM card, the software packages from ITK, WS Connect and Columbus Client have also been successfully tested with Novell and HiPath HG 1500.

To use the software with Novell, the IPX protocol must be connected with the corresponding NDIS-WAN (ISDN) adapter in Network Properties. Frame type Ethernet_II must be reset here under the advanced settings as the frame type. The node (MAC) address is entered in the settings for the software in question.

Generally, logon to the Novell server follows connection with the software via Network Neighborhood. The Novell server now appears and you can log on by double-clicking and entering your user name.

Routing and callback using Cisco routers

Callback in the D channel with the caller ID (calling number) is now possible using Cisco routers and SW release 12.0. The calling number is generally used as the callback number. Wildcards (in the form of Xs) can also be used should problems occur with call number transfer.

Network interfaces:

LAN = 192.168.40.254

ISDN1 = 192.168.100.31

Connection control:

Number redial = 0

Routing:

IP address = 192.168.70.0

Network mask = 255.255.255.0

Gateway = 192.168.100.15

ISDN peer (Cisco):

IP address = 192.168.100.15

B channels = 2

Callback = No

Cisco router:

```
isdn switch-type basic-net3
!
!!
interface Ethernet0
   ip address 192.168.70.128 255.255.255.0
   no ip directed-broadcast
   no mop enabled
!
interface BRI0
   ip address 192.168.100.15 255.255.255.0
   no ip directed-broadcast
   encapsulation ppp
   dialer map ip 192.168.100.31 002112345678
   dialer-group 1
   isdn switch-type basic-net3
   isdn caller xx2112345678 callback!!!!
   isdn calling-number 168
   hold-queue 75 in
!
```

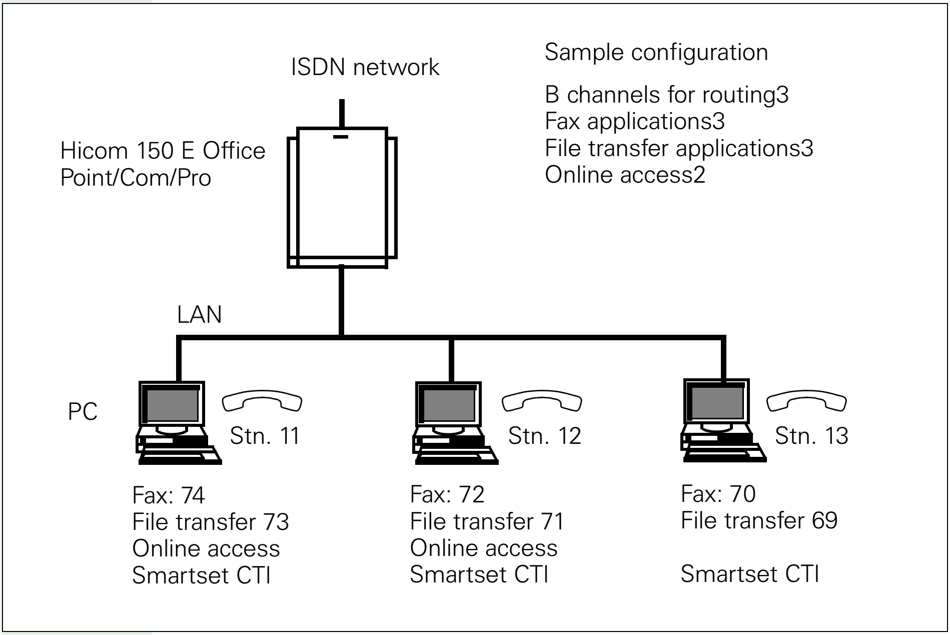
```
ip classless
ip route 192.168.30.0 255.255.255.0 192.168.100.31
ip route 192.168.40.0 255.255.255.0 192.168.100.31
!
dialer-list 1 protocol ip permit
!
```

Telematics

Call number assignment with telematics

All telematic functions that are to be reached by incoming calls require a DID number. The appropriate call numbers thus have to be configured for HiPath HG 1500 for each fax terminal and file transfer application. These call numbers must not conflict with the system numbering scheme. Call numbers are configured for the telematic station by the application program administration component.
Assistant I can be used to administer call forwarding from one fax application to one or more fax applications.

Example for call number assignment



Associated dialing must be enabled for the CTI applications (Smartset) 73, 71, 69. If call evaluation is to be performed on the PC, then an answer group must be configured from terminals 11, 12, 13 to the respective PCs 73, 71, 69.

Restrictions in telematics

Hicom 150 E Office Com and Point supports only two faxes at a time per module whereas Hicom 150 E Office Pro supports three at a time.

vCAPI for clients in the network

With HiPath HG 1500 and vCAPI software (virtual CAPI), the PC behaves like a PC with a separate ISDN card. Prerequisite:

- TCP/IP as the transport protocol
- WIN 95, WIN 98, WIN NT 4.0 or Windows 2000 as the client operating system

Call numbers are assigned in HiPath HG 1500 by assigning the IP address to the call number (max. 100 call numbers).

Thus several call numbers may have to be assigned to one IP address.

FRITZ!vox/fon

The modules are supported with the exception of the following functions:

- Supplementary services, e.g. toggle, consultation

FRITZ!fax and call forwarding

If the PC is deactivated or the fax application is not started in the background, the incoming fax caller hears the ring tone. Forwarding to the customer fax machine can be configured in the Hicom system. The disadvantage/advantage is that while a client with FRITZ!Fax receives or sends a fax, incoming fax calls also for other clients are forwarded. Forwarding can only be set up or changed with the Hicom Assistant.

Appendix

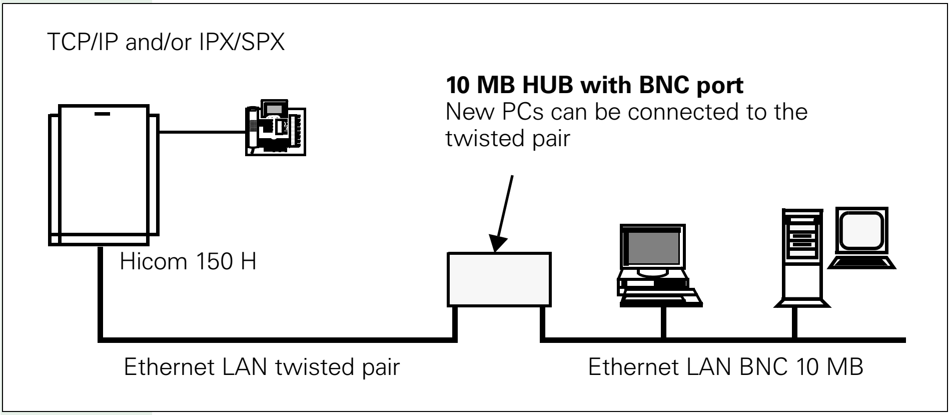
The administration of linked networks in the WAN/LAN is a highly technical procedure. As part of this task, the network administrator will always find configuration problems which should be corrected quickly and efficiently. This appendix should be useful in this regard.

Suggested LAN solutions

BNC network at a twisted pair

Extension of BNC network segment (max. 185 m) by 100 m with twisted pair.

10 MB Ethernet HUB with BNC port


TCP/IP and/or IPX/SPX
10 MB HUB with BNC port
New PCs can be connected to the twisted pair
Hicom 150 H
Ethernet LAN twisted pair
Ethernet LAN BNC 10 MB

Connection of BNC network at twisted pair to HiPath HG 1500

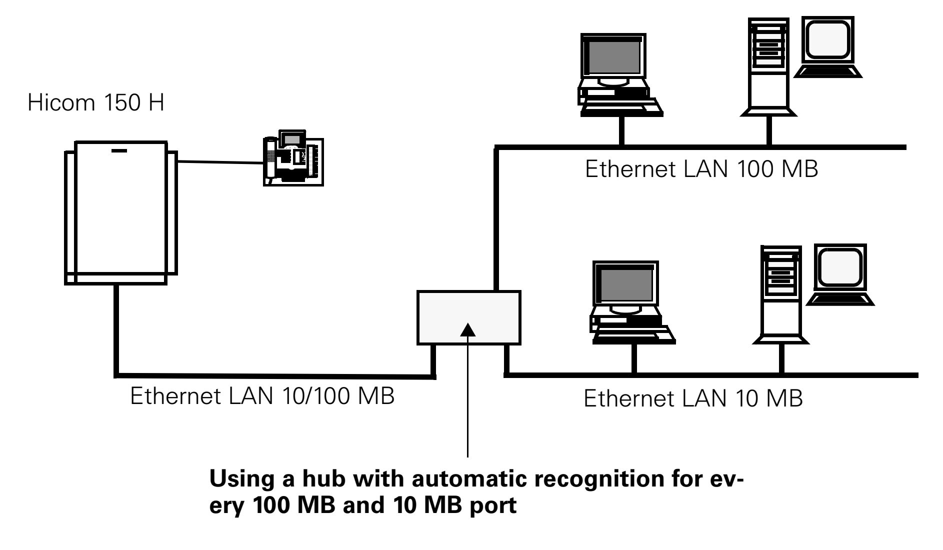
Advantage:

- Simple expansion of BNC network, e.g. 3COM OfficeConnect
- Hub TP 4 Combo (4xRJ-45, 1xAUI, 1xBNC, unmanaged hub)
- Hub 8/TPC (8xRJ-45, 1xBNC, unmanaged hub)
- Hub TP16C (16xRJ-45, 1xBNC, unmanaged hub)

3COM Dual Speed hub

HiPath HG 1500 in 100 MB networks

3COM Dual Speed hub solution


Hicom 150 H
Ethernet LAN 100 MB
Ethernet LAN 10/100 MB
Ethernet LAN 10 MB
Using a hub with automatic recognition for every 100 MB and 10 MB port

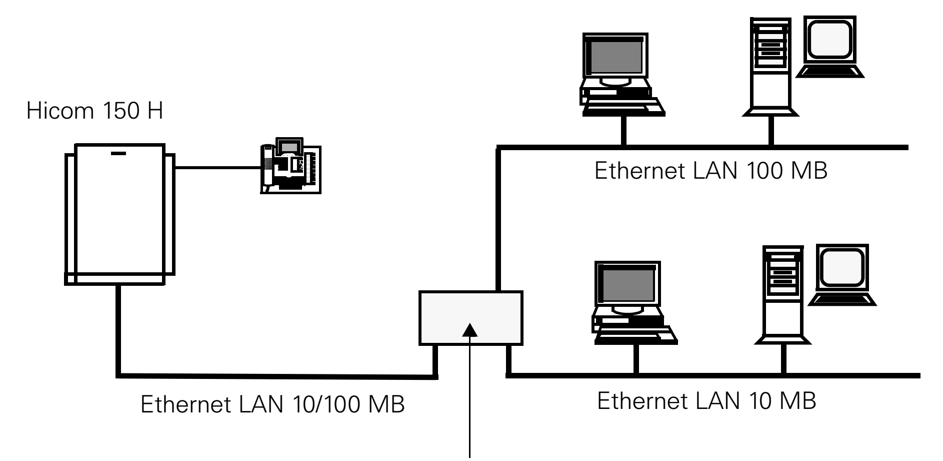
Example: 3COM SuperStack II Dual Speed

- Hub 500 TP 12 port (12 RJ-45, stackable, manageable)
- Hub 500 TP 24 port (12 RJ-45, stackable, manageable)

Solution with a switch

HiPath HG 1500 in 100 MB networks

Solution with switch



Using a switch with 100MB and 10MB ports

Example: Siemens HiNet

- WS 4100 (12 port 10MB, 2 port 100MB)
- WS 4400 (24 port 10MB, 2 port 100MB, managed)
- WS 4700 (24 port Autosense 10/100MB)

or 3COM OfficeConnect

- Switch 140M (4x10/100 BaseT, 1x100BASE-TX) DCF:3C16730-ME
- Switch 280 (8x10/100 BaseT, 2x100BASE-TX) DCF:3C16732-ME

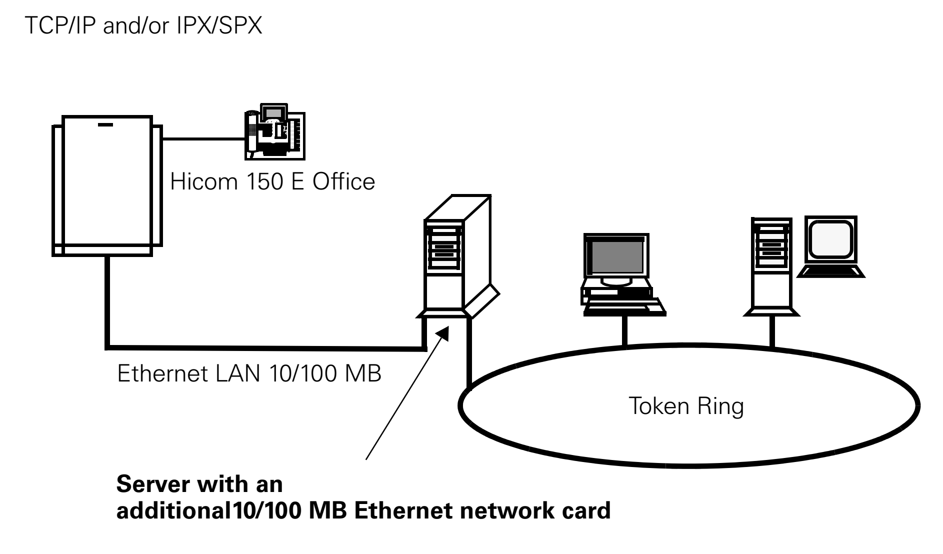
In general, we recommend using switches for Voice over IP connections to keep voice connection interference by other data loads in the LAN to a minimum.
We recommend implementing switches that support Quality of Service: this ensures the necessary prioritization of voice packets with regard to data and improves the quality of voice connections, see → 83 QoS.

HiPath HG 1500 in Token Ring networks

Routing via network server (Token Ring > Ethernet 10/100 MB)

Use of an additional 10/100 MB Ethernet network card in the server. (NT Server 3.51/ 4.0, Netware Server 3.12 / 4.X).

Token Ring network card solution



Utility programs for TCP/IP diagnostics

Each operating system provides tools suitable for finding faults in a TCP/IP environment which do not have an obvious explanation. As each operating system includes its own tools and corresponding command parameters, only the main Microsoft operating system functions are described here. Other tools for UNIX-based operating systems are described in detail in RFC 1147. Special parameters are contained in the Help for the corresponding operating system and can normally be queried by entering <Command> -?.

ping

The tool most often used is the PING command. This command allows you to check whether a computer can be reached in the network, i.e whether communication with the computer is possible. An ICMP ECHO message is sent to the computer and then returned to the sender. If the answer returns to the sending computer, communication is possible with the computer specified. Most variants of the PING command produce connection statistics.

Syntax for Windows 95/98/NT:

```
ping <Host> [<Parameter>]
```

<Host> Contains the destination address or the host name of the destination computer

<Parameter>

-t Uninterrupted transfer of test packets to the computer. Normally 4 test packets are transferred.

-a IP addresses are resolved to host names.

-n <number> Sends <Number> test packets to the computer.

-l <size> Sends test packets with <Size> bytes

-i <TTL> Time in milliseconds valid for a packet. If the computer receives a packet after the time has elapsed, this packet is ignored.

-w <timeout> Timeout in milliseconds to wait for each reply. If this duration elapses, a timeout message appears. This value is set to 1000 (1s) as standard. It is advisable to set this value to 5000 (5s) or 10000 (10s) in the case of slow connections, e.g. via modem or GSM. If the reply takes more than 1 second, a timeout message is received, although a connection is possible.

Example:

Check connection to local computer. The local computer can normally be reached under the loopback address "127.0.0.1" and the name "localhost".

```
C:\>ping localhost
PING is executed for the local host [127.0.0.1] with 32
bytes of data:
Reply from 127.0.0.1: bytes=32 time<10MS TTL=128
Reply from 127.0.0.1: bytes=32 time<10MS TTL=128
Reply from 127.0.0.1: bytes=32 time<10MS TTL=128
Reply from 127.0.0.1: bytes=32 time<10MS TTL=128
```

Messages:

If the remote computer does not reply, the error can be deduced from the messages.

- Invalid IP address (unknown host):
  The host name could not be converted to a valid IP address. This message is generated when the DNS server cannot be reached or is out of service. This message is only output when the host is addressed using a name.
- Destination host not available (network unreachable):
  There are no valid routes to the destination system. The destination address could not be reached, as a gateway is out of service or not correctly specified.
- Request timeout:
  The computer has a route to the destination computer but a response is not forthcoming. The message reaches the destination host, but cannot be returned. This error is caused by in correct destination computer routing.

ipconfig

The "ipconfig" program is a quick way of querying the TCP/IP network configuration. In this way you can display IP addresses, netmasks, gateways and network card statistics. DHCP also enables assigned IP addresses to be enabled or renewed.

Syntax for Windows 98/NT:

ipconfig [<Parameter>]

<Parameter>

/all
Shows detailed information on network configuration. This contains the host name, DNS server used, MAC addresses of each network adapter and DHCP information.

/release [Adapter]
Enables the IP address assigned via DHCP at the adapter.

/renew [Adapter]
Assigns a new IP address to the adapter via DHCP.

If the adapter is not specified under the parameters "release" and "renew", all IP addresses at all adapters assigned via DHCP are enabled or newly assigned.

Example:

Detailed query of current configuration

```
C:\>ipconfig /all


Windows NT IP Configuration
   Host Name ................:  myhost.Siemens.de
   DNS Server................:  192.168.50.23
                               192.168.50.160
   Node Type ................:  Broadcast
   NetBIOS Scope ID .....:
   IP Routing Enabled.....:    No
   WINS Proxy Enabled.....:    No
   NetBIOS Resolution Uses     Yes
   DNS:
```

```
Ethernet adapter El90x2:
   Description..............:  3Com 3C90x Ethernet
                               adapter
   Physical Address.........:  00-10-5A-DD-56-55
   DHCP Enabled.............:  No
   IP Address...............:  192.168.129.1
   Netmask..................:  255.255.255.0
   Default Gateway..........:

Ethernet adapter El90x1:
   Description..............:  3Com 3C90x Ethernet
                               adapter
   Physical Address.........:  00-10-5A-37-26-B1
   DHCP Enabled.............:  Yes
   IP Address...............:  192.168.14.6
   Netmask..................:  255.255.255.0
   Default Gateway..........:  192.168.14.1
   DHCP Server..............:  192.168.11.103
   Lease Supplied....... ...:  Tue, 17.08.1999
                               08:43:30
   Lease Expires............:  Tue, 19.01.2038
                               04:14:07
```

nslookup

An IP address can be assigned via a host name. This assignment of name and IP address is stored in the DNS server (DNS = Domain Name Server). The command "nslookup" can be used to query data that was saved for a specific host in the DNS server. By entering the command "nslookup" in the MSDOS input prompt, the program tries contact the DNS server saved in the network. If a name is queried, the corresponding IP address is returned. If, on the other hand, an IP address is queried, the host name is returned. If neither the IP address nor the host name are stored in the DNS server, a corresponding error message is output.

The Ping command message "Invalid IP address" indicates that the host name specified cannot be converted to an IP address. This occurs when the DNS server is out of service or the entry does not exist. This requires that DNS servers are entered in the network configuration and can be addressed via network.

"nslookup" can be used to query various entries (records) on the DNS server. Once the program has been started, the following entries can be used to query the corresponding data.

set Type=<Type>

<Type>

a	Address entries
any	All entries
mx	Mail Exchanger entries
ns	Name Server entries
soa	Start of Authority entries
hinfo	Host Info entries
axfr	All entries in a single area
txt	Text entries

Syntax for Windows 98/NT:

nslookup <Host>

<Host> Contains the destination address or the host name of the destination computer

Example:

```
C:\>nslookup localhost
Server: ns.domain.com
Address: 192.168.0.1

Name: localhost
Address: 127.0.0.1
```

The host "localhost" has the IP address "127.0.0.1".

hostname

The command "hostname" returns the name of the local computer. Unlike other operating systems, in Microsoft operating systems the host name cannot be changed using this command.

Example:

```
C:\>hostname
localhost
```

netstat

The command "netstat" is used to check existing connections and configured routes, and returns detailed statistics and information on individual network interfaces. Besides the routing table, the most frequently used "netstat" function is the query feature, which ascertains which connections exist at the local computer as well as the status of these connections.

Syntax for Windows 95/98/NT:

netstat [<Parameter>] [<Interval>]

<Parameter>	
-a	Displays all connections, i.e. listening applications are also displayed, e.g. a Telnet server.
-e	Displays Ethernet statistics
-n	Displays IP addresses instead of host names
-p <Proto>	Displays connections established via the <Proto> protocol
-r	Displays the routing table which is also displayed using "route print.
-s	Displays statistics for each protocol
<Interval>	Repeats the display after <Interval> seconds

Example:

Queries all connections in IP address format (abbreviated)

```
C:\>netstat -a -n

Active Connections

Proto  Local address        Remote address       Status
....
....
TCP    0.0.0.0:25           0.0.0.0:0            LISTENING
TCP    0.0.0.0:80           0.0.0.0:0            LISTENING
....
....
TCP    192.168.129.3:110    192.168.129.1:1037   ESTABLISHED
TCP    192.168.129.3:23     192.168.129.2:1038   ESTABLISHED
TCP    192.168.129.3:1031   192.168.129.1:80     ESTABLISHED
....
....
UDP    0.0.0.0:25           *:*
UDP    0.0.0.0:80           *:*
....
```

IP connections and their states can be displayed using this table. Before explaining this example in greater detail, we will first discuss briefly the variables.

<Proto> Indicates the protocol used for the communication. In this case, Windows only distinguishes between TCP and UDP. Unfortunately, certain servers which only operate via a single protocol are displayed both as TCP and as UDP servers. This prevents accurate determination of the actual protocol in use.

<Local Address> This indicates the local address which has established a connection or is listening for a connection. The local address and the foreign address are displayed in the format
<IP address>:<Port number>.

<Remote Address> This indicates the remote address which has established a connection or to which a connection has been established.

<Status>

Shows the current state of the connections:

ESTABLISHED The local computer set up a connection to a server. In this case the local computer is a client.

LISTENING The local computer is ready to accept a connection. In this case the local computer is a server.

SYN_SENT The local computer signals to the server that it would like to establish a connection.

SYN_RECEIVED The local computer where the server is running has received a "SYN_SENT" signal, i.e. the client would like a connection to be established.

FIN_WAIT_1 The local computer would like to clear down the connection to the server.

TIME_WAIT The local computer is waiting for server confirmation that the connection is to be terminated.

CLOSE_WAIT The local computer where the server is running has received a "FIN_WAIT_1" signal, i.e. the client would like a connection to be cleared down.

FIN_WAIT_2 The local computer has received confirmation from the server to clear down the connection.

LAST_ACK The server has sent confirmation that the connection is to be cleared down.

CLOSED The server has received client confirmation that the connection has been cleared down.

A computer can be both a client and a server at the same time. This is the case, for example, where the local computer is connected to its own server. This is possible using the loopback interface "127.0.0.1". If, for example, a Telnet server is running on the local computer, a Telnet session can be opened on the local computer using the command "telnet localhost".

In order to determine which data can be collated using the above example, we will now explain the procedure step by step.

```
Proto   Local address   Remote address  Status


TCP      0.0.0.0:80     0.0.0.0:0       LISTENING
TCP      0.0.0.0:25     0.0.0.0:0       LISTENING
```

The first 2 entries are in the "LISTENING" state, i.e. 2 programs (servers) have been started on the local computer, both of which are waiting for a client to establish a connection with them. Both are connected to the IP address "0.0.0.0". This IP address indicates that the server is connected to all available network interfaces. Even if only one network card is installed, this already has 192 interfaces, i.e the local network card (168.129.3.127) and the loopback interface "0.0.1.1" which is installed as standard by Windows. In this example, a HTTP server (Port 80) and an SMTP server (Port 25) are running on the local computer. In order to determine whether the network card is working correctly, send a test Ping from the local computer, e.g 192.168.129.3". Each error message triggered by this test indicates an incorrectly configured network. If you wish to test the connection to the local HTTP server for example, simply use your Web browser and enter the URL "http://127.0.0.1" or http://192.168.129.3.“Entering "telnet localhost 25" or "telnet 192.168.129.3 25" allows a connection to be established to the local SMTP server. In this case, the port (the application) is specified using "25".

The next three entries are all active connections. These can be established either from the local to the remote computer, or from the remote to the local computer.

```
Proto  Local address       Remote address      Status


TCP    192.168.129.3:1037  192.168.129.1:110   ESTABLISHED

TCP    192.168.129.3:1038  192.168.129.2:23    ESTABLISHED

TCP    192.168.129.3:80    192.168.129.1:1039  ESTABLISHED
```

In order to distinguish between an incoming and an outgoing connection, the entries contained in the "LISTENING" state (server) are required. To do this, you need to check whether the port specified for the local computer is running on the local computer itself. The first line shows port "1037". This port is not running as a server (LISTENING) on the local computer (192.168.129.3). Thus this must be a connection from the local computer to a remote computer (192.168.129.1) with the port "110" (POP3). In other words, the local computer is in the process of downloading its emails from the POP3 server.

The second entry must also be an outgoing connection, as it is also not in the "LISTENING" state on the local computer. The local computer set up a connection to the computer "192.168.129.2" and port "23" (Telnet) This means that the local computer opened a Telnet session on the remote PC.

In the third entry, the local port "80" (HTTP) corresponds to that of a server. Thus the remote computer "192.168.129.1" is in the process of opening Web pages on the local computer.

nbtstat

This utility program allows connections which use the "NetBIOS over TCP/IP protocol" (WINS-Client(TCP/IP)) to be tested. With the "NetBIOS over TCP/IP protocol", the NetBIOS packet is packaged in a in a TCP/IP packet and then unpacked again on the remote side. This is necessary because NetBIOS cannot be rerouted like TCP/IP. As Windows drives can only be enabled via NetBIOS, these must be packaged in TCP/IP if transport to other physical networks is required. For this purpose, Windows creates a NetBIOS name cache which can also be created manually. IP addresses are resolved in a table as computer names for this procedure. This file is called "lmhosts" and is available in every operating system either in the System directory, or in a System subdirectory.

Win95/98:	%systemroot%
WinNT:	%systemroot%\system32\drivers\etc

In these directories, Windows provides various test files which can be used as samples. The structure of each test file is explained. These files have the extension "sam."In this case, the file is called "lmhosts.sam."If this "lmhosts" file does not already exist, it can simply be copied to "lmhosts" and edited.

Syntax for Windows 95/98/NT:

nbtstat [<Parameter>]

<Parameter>	
-a <Host Name>	Returns the name table for the computer specified under <Host Name>
-A<IP address>	Returns the name table for the computer specified under <IP Address>
-c	The NetBIOS Name Cache is listed with NetBIOS names and corresponding IP addresses
-n	Lists all local NetBIOS names used
-R	Deletes the NetBIOS Name Cache and reloads the file "LMHOST"
-r	Lists the names which have been resolved for the Windows networks
-S	Shows client and server connections as IP addresses.
-s	Shows client and server connections and resolves the IP addresses to names.

route

In order to connect several TCP/IP networks together, routing must be configured. Without routing, it is impossible to leave the local network. For routing, note that the gateway which connects the local network to other networks must be located in the same TCP/IP network as the local computer.

Syntax for Windows 95/98/NT:

route <Command> <Destination> <Netmask> <Gateway> [metric <Hops>] [<Parameter>]

<Command>	
print	Displays the current routing table
add	Adds a new route
delete	Deletes an existing route
change	Modifies an existing route
<Destination>	Indicates the destination host or destination network reachable via the <Gateway>.
<Subnet>	Specifies the subnet mask.
<Gateway>	Indicates the IP address of the gateway via which the IP address specified under <Destination> can be reached.
<Hops>	Indicates the number of gateways located between the sender and the destination. This parameter is only relevant when several routes exist for one destination. Certain routes can be assigned priority using this parameter. However, since only one gateway usually exists, the value "1" can be set here.
<Parameter>	
-f	Deletes all routing entries in the routing table
-p	Creates a permanent entry. This parameter can only be specified using the command "add". Normally routes are only set statically with the "route" command. This means that following a system reboot, routes set in this way are deleted. The parameter "-p" sets the entry permanently, so that it is not deleted by a system reboot.

Example 1:

Adding a permanent default route

```
C:\cmd>route add 0.0.0.0 mask 0.0.0.0 192.168.0.199 -p
```

Example 2:

Querying a routing table

```
C:\>route print
Active Routes:

Network Address Netmask         Gateway Address Interface:     Number
0.0.0.0         0.0.0.0         192.168.128.1   192.168.128.14 1
10.2.0.0        255.255.0.0     192.168.128.1   192.168.128.14 1
127.0.0.0       255.0.0.0       127.0.0.1       127.0.0.1      1
192.168.128.14  255.255.255.255 127.0.0.1       127.0.0.1      1
192.168.128.255 255.255.255.255 192.168.128.14  192.168.128.14 1
224.0.0.0       224.0.0.0       192.168.128.14  192.168.128.14 1
255.255.255.255 255.255.255.255 192.168.128.14  192.168.128.14 1
```

The last 2 entries are Multicast or Broadcast entries which will not be described in detail here.

tracert

Tracert (trace route) is used to trace the route from the local computer to the destination host. It indicates all gateways located on the route to the destination host.

Syntax for Windows 98/NT:

racert <Host> [<Parameter>]

<Host>	Contains the destination address or the host name of the destination computer
<Parameter>	
-d	IP addresses are not resolved to host names
-h <number>	Indicates the maximum number of gateways to the destination host
-j <list>	Suggests a gateway route
-w <timeout>	Wait <Timeout> milliseconds for each reply

Example:

```
C:\cmd>tracert localhost
Tracing route to localhost [127.0.0.1] over a maximum
of 30 hops:
1   <10 ms   <10 ms   <10 ms  localhost [127.0.0.1]
Trace complete.
```

arp

Before a packet is sent from one host to another, the hardware address (MAC address) of the destination host’s network card must be determined. For this purpose, each computer which communicates via the TCP/ IP protocol has an ARP table. "ARP" (Address Resolution Protocol) is used for resolving the IP address to the hardware address (MAC address). Before a connection is established, the ARP table is searched for the required destination host. If the host is not contained in the table, an ARP request with the IP address of the destination host is sent via the network. If the destination host receives this request, it send its hardware address to the requesting computer. This hardware address is then entered to the local ARP table. The next time this connection is set up, the hardware address can simply be applied as normal. If a hardware address located outside of the logical TCP/IP network is required, only the router hardware address, via which the destination host can be reached, is necessary.

Syntax for Windows 95/96/NT:

arp <Parameter>

<Parameter>

a	Displays the ARP table
-d	Deletes an entry from the ARP table
-s	Adds a host entry to the ARP table

Example 1:

Entering a new MAC address to the ARP table

```
C:\>arp -s 192.168.0.199 02-60-8c-f1-3e-6b
```

Example 2:

Querying the ARP table

```
C:\>arp -a
Interface: 192.168.0.1 on Interface 1

 Internet Address     Physical Address     Type
 192.168.0.1          00-00-5a-42-66-60    dynamic
 192.168.0.10         00-60-70-cd-59-22    dynamic
 192.168.0.199        02-60-8c-f1-3e-6b    static
```

Telnet

Telnet enables the user to log onto a remote computer. The program uses port "23" as standard for this procedure. If you wish to log onto a computer with another port, you must specify the port number.

Syntax for Windows 95/96/NT:

telnet [<Host> [<Port>]]

<Host> Contains the destination address or the host name of the destination computer

<Port> Port number which identifies the application on the destination computer

Example:

```
C:\>telnet localhost 110
```

IP addressing: Sub-networks

This system offers the "sub-netting" procedure which can be used to circumvent the scarcity of official IP addresses and to divide an IP network in to separate sub-networks.

For the allocation of official IP addresses, for example, sub-netting enables the generation of additional independent IP networks using existing Class A, B and C network addresses.

For networks, various classes and standard network masks have been agreed upon:

Class	Netmask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Division into independent sub-networks also offers the considerable advantage that local network traffic remains in the corresponding sub-network. Access to third-party networks is only possible via a router.

The basic functionality of sub-netting is relatively simple and is based on the "Netmask."Using this mask, bits are defined which represent either the network or the host segment within an IP address. Set bits (1) represent the network segment, while deleted bits (0) represent the host segment.

The best way to analyze a netmask is in binary format. The Class C standard network mask "255.255.255.0" is a good example.

	Network			Host
Bytes	1st byte	2nd byte	3rd byte	4th byte
Netmask	255	255	255	0
Binary format	1111 1111	1111 1111	1111 1111	0000 0000

In netmask "255.255.255.0", the first 3 bytes represent the network segment (all bits 1) and the last byte represents the host segment (all bits 0).

The host (router, workstation, etc.) uses this netmask to determine whether the IP address being addressed is located in the local network. If the destination host is not located in the same network, packets are sent to this address via the corresponding routing mechanisms stored.

To create customized sub-networks, the number of sub-networks to be established within a class-based network (Class A, B, C) must be determined. When a network is divided, 2^n sub-networks are always created as a result. An example will explain this more clearly.

The Class C network "192.168.1.0" is to be divided into 4 sub-networks. A Class C network has the default netmask "255.255.255.0". The following table indicates the interdependency between the bit number and the number of networks.

Bits	Combinations	Bits	Combinations
1	2^1 = 2	17	2^{17} = 131072
2	2^2 = 4	18	2^{18} = 262144
3	2^3 = 8	19	2^{19} = 524288
4	2^4 = 16	20	2^{20} = 1048576
5	2^5 = 32	21	2^{21} = 2097152
6	2^6 = 64	22	2^{22} = 4194304
7	2^7 = 128	23	2^{23} = 8388608
8	2^8 = 256	24	2^{24} = 16777216
9	2^9 = 512	25	2^{25} = 33554432
10	2^{10} = 1024	26	2^{26} = 67108864
11	2^{11} = 2048	27	2^{27} = 134217728
12	2^{12} = 4096	28	2^{28} = 268435456
13	2^{13} = 8192	29	2^{29} = 536870912
14	2^{14} = 16384	30	2^{30} = 1073741824
15	2^{15} = 32768	31	2^{31} = 2147483648
16	2^{16} = 65536	32	2^{32} = 4294967296

So that no gaps are left in the address range, additional 1s are added from left to right to the existing 1s of the netmask.

Class C	**Network**			**Host**
Bytes	1st byte	2nd byte	3rd byte	4th byte
Netmask	255	255	255	0
Binary format	1111 1111	1111 1111	1111 1111	0000 0000
New	**Network**			**Host**
Bytes	1st byte	2nd byte	3rd byte	4th byte

Class C	Network			Host	
Binary format	1111 1111	1111 1111	1111 1111	**11**	00 0000
Netmask	255	255	255	192	

If the new Sub-network is converted from binary to decimal form, the result is the netmask "255.255.255.192". Now 26 bits are available for the network segment and 6 for the host segment. Computers with a network segment with the same bit pattern can communicate directly in a physical network. Other networks can only be reached via a gateway. If the modified 4th byte is viewed in terms of the 2 new network bits (25 and 26), the newly created sub-networks can now be calculated.

4th byte	Decimal	New network	Broadcast address	Host addresses
0000 0000	0	192.168.1.0	192.168.1.63	1 - 62
0100 0000	64	192.168.1.64	192.168.1.127	65 - 126
1000 0000	128	192.168.1.128	192.168.1.191	129 - 190
1100 0000	192	192.168.1.192	192.168.1.255	193 - 254

Thus sub-netting essentially involves the extension of the network segment of an IP address by reducing the host segment. The number of available sub-networks and hosts depends on the following conditions:

The number of available host addresses depends largely on the length of the host segment of the IP address. Viewed mathematically, a 6-bit host segment provides for 64 addresses. However, as each IP network and thus each individual sub-network has 2 reserved addresses, the maximum number of addresses is reduced by 2. These are the host addresses which contain either zeros or ones. The former is used for addressing a network, while the latter is used for broadcasts in the network in question.

As mentioned above, the new network segment bits are added from left to right to the existing bits. The reasons for this are described below. For example, if you use netmask "255.255.255.3" for the network "192.168.1.0", the host segment is located in the middle of the network segment.

	Network			Host	Network
Bytes	1st byte	2nd byte	3rd byte	4th byte	
Netmask	255	255	255	3	
Binary format	1111 1111	1111 1111	1111 1111	0000 00	**11**

No associated IP address areas are provided for by this sub-network as only the hosts which have set the last 2 bits are located in a network. The resulting addresses are listed in the following table.

4th byte	Decimal	New network	Broadcast address	Host addresses
0000 00**00**	0	192.168.1.0	192.168.1.252	4,8,12,16,20,...,248
0000 00**01**	1	192.168.1.1	192.168.1.253	5,9,13,17,21,...,249
0000 00**10**	2	192.168.1.2	192.168.1.254	6,10,14,18,22,...,250
0000 00**11**	3	192.168.1.3	192.168.1.255	7,11,12,19,23,...,251

The host addresses indicate that the individual hosts are not located in associated areas. This type of sub-netting makes it difficult to maintain an overview for administration. This is why this type of sub-netting should not be used.

Up to now we have described how sub-networks are created. We will now explain how the IP addresses of computers are assigned to the relevant sub-network.

The following table shows 4 IP addresses for a network (Class C) as well as their connection to the netmask being used ("255.255.255.224").

	Network	Host
255.255.255.224	11111111.11111111.11111111.111	00000
193.98.44.33	11000001.01100010.00101100.001	00001
193.98.44.101	11000001.01100010.00101100.011	00101
193.98.44.129	11000001.01100010.00101100.100	00001
193.98.44.61	11000001.01100010.00101100.001	11101

The binary illustration of masks and addresses shows quite clearly which sub-network the IP addresses in question belong to. Addresses 1 and 4 are in sub-network ".32" (00100000), address 2 belongs to sub-network ".96" (01100000) and address 3 is located in sub-network ".128" (10000000).

If the example is based on the standard mask "255.255.255.0" of a Class C network, the length of the network segment is 24 bits, while the host segment is 8 bits long. Based on netmask "255.255.255.224" the network segment of an IP address in the network is exactly 27 bits long. Accordingly the host segment is just 5 bits long.

The following overview provides the most commonly-used Class C masks as a reference, together with the corresponding network and host allocations.

Netmask	Number of networks	Hosts per sub-network	Sub-network	Broadcast address	Hosts
255.255.255.0	1	253	0	255	1 – 254

Netmask	Number of net-works	Hosts per sub-net-work	Sub-net-work	Broadcast address	Hosts
255.255.255.128	2	126	0	127	1 – 126
			128	255	129 – 254
255.255.255.192	4	62	0	63	1 – 62
			64	127	65 – 126
			128	191	129 – 190
			192	255	193 – 254
255.255.255.224	8	30	0	31	1 – 30
			32	63	33 – 62
			64	95	65 – 94
			96	127	97 – 126
			128	159	129 – 158
			160	191	161 – 190
			192	223	193 – 222
			224	255	225 – 254
255.255.255.240	16	16	0	15	1 – 14
			16	31	17 – 30
			32	47	33 – 46
			48	63	47 – 62
			64	79	65 – 78
			80	95	81 – 94
			96	111	97 – 110
			112	127	113 – 126
			128	143	129 – 142
			144	159	145 – 158
			160	175	161 – 174
			176	191	177 – 190
			192	207	193 – 206
			208	223	209 – 222
			224	239	225 – 238
			240	255	241 – 254

Example:

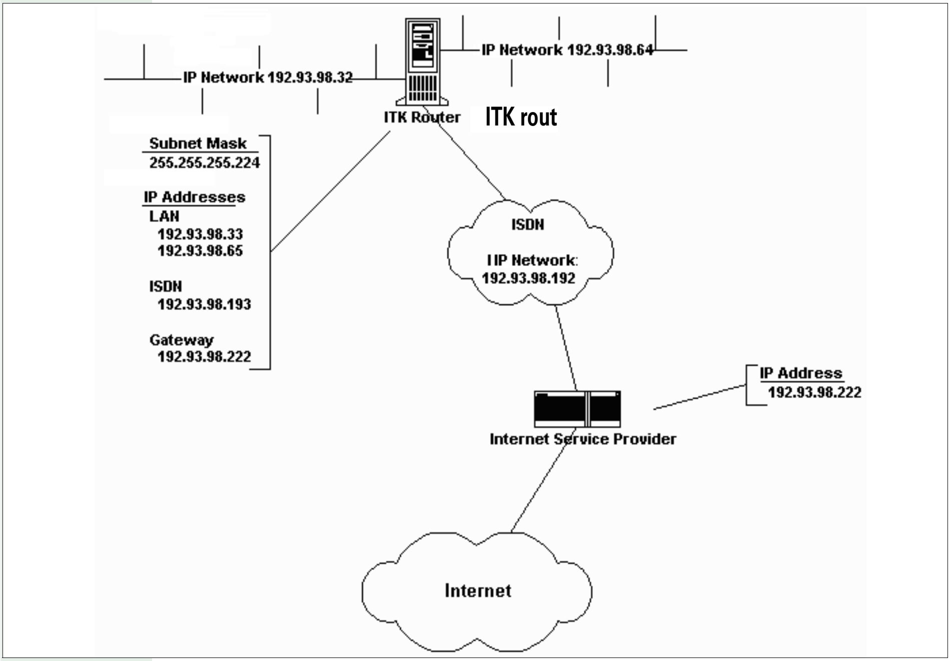
A LAN with 2 Ethernet networks is to be connected to the Internet via ISDN access. All stations in the local Ethernet should have Internet access as well as being directly available via the Internet. Based on the corresponding structures of a Class C address, a complete Class C network should normally be provided for each of the 2 Ethernet networks and for the ISDN network. However, as the maximum number of stations in a Thin Ethernet segment is limited to 30, 223 host addresses per network are lost here alone.

This is where sub-netting is of particular significance: With a corresponding netmask, just one Class C network is required to achieve a complete LAN connection, without the loss of host addresses.

For this purpose, an Internet Service Provider provides a Class C network with the following basic data:

IP address provider:	192.93.98.222
IP address gateway:	192.93.98.222
IP address networks:	192.93.98.0
Netmask:	255.255.255.0

The following diagram shows the corresponding configuration:



"255.255.255.224" is available as a netmask, as this mask provides 8 sub-networks with 30 hosts each. The number of hosts in each sub-network is covered by the maximum number of stations in an Ethernet segment.

This illustration shows that 2 sub-networks, here "192.93.98.32" and "192.93.98.64", have been assigned both LAN boards of the ITK router. One of the LAN boards is assigned the IP address "192.93.98.33" and the other is assigned "192.93.98.65". In this way each board can support 29 additional stations with IP addresses.

The ISDN (WANODI or Virtual Ethernet) is assigned the IP address "192.93.98.193" from sub-network "192.93.98.192". The default gateway in this case is the IP address of the provider access. This ensures that all packets transferred to networks which do not belong to the local LAN sub-network are forwarded to the provider.

Port numbers on the HG 1500

Client/Server	Protocol	Server	Client	Usage
H.323 (H.225/ Q931)	TCP	1720	ephemeral	Voice over IP for system clients, H.323 clients, AllServe and IP networking applications
RTP/RTCP	UDP	29100...29131	ephemeral[a]	
H.245	TCP	ephemeral[b] 12100...12115[c]	ephemeral[d]	
Gatekeeper registration	UDP		1719	When using a gatekeeper
VOPTISET	TCP	4060		System client
Network Unit	TCP	12050	12050	AllServe / IP networking
Data Gateway	TCP	8765	8765	AllServe / IP networking
ADMIN	TCP	12000		Administration
VCAPI	TCP	12001		VCAPI
Accounting Server	TCP	13042		IP Accounting
SNMP (Get/Set)	UDP	161		SNMP browser, HiPath FM
SNMP (traps)	UDP		162	
DSL diagnostics server	UDP	12200		DSL status display
Registration	TCP		12061	AllServe networking
Call Address Resolution	TCP	12062	12062	
TFTP	UDP	69	69	APS transfer via TFTP

[a] is set by peer (1024 ... 5000)

[b] up to HG1500 V2.0: ephemeral (1024 ... 5000)

[c] HG1500 V2.0 and later: the highest port number is determined by the number of licensed B channels

[d] is set by peer (1024 ... 5000)

Port numbers on the Allserve server

Client/Server	Protocol	Server	Client	Application
ADM	TCP		7000	AllServe networking
SYNC	TCP		7024	
FCT	TCP		7100	
CAR_Server	TCP	12062		
REG_Server	TCP	12061		
SNMP (Get/Set)	UDP	161		SNMP browser, HiPath FM
SNMP (traps)	UDP		162	

Port numbers in Hicom

Client/Server	Protocol	Server	Client	Application
TFTP	UDP	69	69	APS transfer via TFTP, AllServe networking
ADM	TCP	7000		AllServe networking
SYNC	TCP	7024		
FCT	TCP	7100		
SNMP (Get/Set)	UDP	161		SNMP browser, HiPath FM
SNMP (traps)	UDP		162	

Unwanted Internet connections (DNS queries)

If the LAN module establishes Internet connections for no particular reason, or if existing connections do not automatically switch to short-hold, then this is due to DNS queries which are sent from the PC in the LAN to the Internet. To prevent DNS queries from this PC, a resolve name procedure must be implemented for the corresponding entry in the Host/Lmhost file on the PC, so that all subsequent DNS queries can be replied to locally at the PC. In this way an Internet connection is not established unless the user specifically initiates this (e.g. by starting the browser). This problem can also be observed with standard routers (e.g. 3COM). This is a protocol-based procedure which can be canceled by way of a corresponding analysis and configuration of the network/PC.
The customer trace can be used to determine which PC is responsible for dialing into the PC continuously. Trace group 112 (customer trace PPP) is activated (value 4) and the customer trace is deleted for this. Following an observed Internet dial-in attempt, the customer trace contains information on the IP address that led to routing, as well as the TCP/UDP port number or DNS queries in plain text. Based on this information, the system can determine which PC is responsible for continuous dial-in and which service (dPort) is requested.

If the query was actually a DNS query, then the following procedure is recommended:

The sender IP address identifies the PC which sent this query from the LAN. For this PC, the entry must then be made to the local Hosts/Lmhosts. The entry in the Hosts/Lmhosts must include the name contained in the name query (also in trace) and the associated IP address (to be determined by the LAN administrator).

Example:
A software installed in the LAN uses the dongle attached to the server. If the client SW is started on the PC, the software license is determined using the dongle. Thus the client SW sends a name query to the network because only the dongle name is known. As the client PC contains a DNS entry for resolving names e.g. for Internet access, it also sends the name query directly in the Internet. Thus the problem described above also occurs here.
To correct this problem, the IP address of the server where the dongle is attached, as well as the dongle name, are entered in the Hosts/Lmhosts file on the client PC. This prevents automatic setup of Internet connections. According to regulations governing TCP/IP and the resolving of names, the name is always searched for first in the Hosts/Lmhosts file. If the entry cannot be found, a DNS query is forwarded to the configured DNS. For security reasons, the IP firewall in the LAN module must be activated and the PC IP address approved for the Internet should only be enabled for the required ISDN interfaces. Now the customer NT server, for example, which is not entered in the firewall may initiate DNS queries. However these are not sent to the Internet as the appropriate authorization is not available.

Customer trace

Customer trace is used for more in-depth diagnostics in HiPath HG 1500 and provides detailed information which can be evaluated for the purpose of correcting any faults which may occur.

Customer trace can also be used to locate configuration errors during HiPath HG 1500 startup. It should only be activated for fault analysis, otherwise system performance is affected.

Logging function

For reasons of data protection it is necessary to log all changes that were made to a customer system either locally or remotely. On request, the customer can therefore be presented with a substantiated list of changes which have been made to his/her system.

When loading a customer database to HiPath HG 1500, a data record about the modified data is also loaded to the module and saved without reset or delete options. This memory has at least 64kB. This memory can be read out via the menu item
"File->Transfer log file to the PC" and saved in the file.

ETSI error messages

The following table is used for evaluating trace error codes. The error message number output by the tracer is required for this and can be found in the table. The error code is explained in plain text in the right column. Since the value output is formatted in decimal or hexadecimal depending on the trace (applications, Hicom, HiPath HG 1500), three values appear in the table. The values with the offset are sent by the remote station.

Value			ETSI CAUSE (Network delivered)
dec	hex	hex with Offset 80h	
1	1	81	UNASSIGNED (UNALLOCATED) NUMBER
2	2	82	NO ROUTE TO SPECIFIED TRANSIT NETWORK
3	3	83	NO ROUTE TO SPECIFIED TRANSIT DESTINATION
6	6	86	CHANNEL UNACCEPTABLE
7	7	87	CALL AWARDED IN ESTABLISHED CHANNEL
16	10	90	NORMAL CALL CLEARING
17	11	91	USER BUSY
18	12	92	NO USER RESPONDING
19	13	93	ALERTING - NO ANSWER FROM USER
21	15	95	CALL REJECTED
22	16	96	NUMBER CHANGED
26	1A	9A	NON SELECTED USER CLEARING
27	1B	9B	DESTINATION OUT OF ORDER
28	1C	9C	INVALID NUMBER Format (INCOMPLETE NUMBER)
29	1D	9D	FACILITY REJECTED
30	1E	9E	RESPONSE TO Status ENQUIRY
31	1F	9F	NORMAL; UNSPECIFIED
34	22	A2	NO CHANNEL AVAILABLE
38	26	A6	NETWORK OUT OF ORDER
41	29	A9	TEMPORARY FAILURE
42	A2	AA	SWITCHING EQUIPMENT CONGESTION
43	2B	AB	ACCESS INFO DISCARDED
44	2C	AC	REQUESTED CHANNEL NOT AVAILABLE
47	2F	AF	RESOURCES UNAVAILABLE
49	31	B1	QUAL OF SERVICE UNAVAILABLE
50	32	B2	REQUESTED FACILITY NOT SUBSCRIBED
57	39	B9	BEARER CAPABILITY NOT AUTHORIZED

Value			ETSI CAUSE (Network delivered)
dec	hex	hex with Offset 80h	
58	3A	BA	BEARER CAPABILITY NOT AVAILABLE
63	3F	BF	SERVICE NOT AVAILABLE
65	41	C1	BEARER CAPABILITY NOT IMPLEMENTED
66	42	C2	CHANNEL TYPE NOT IMPLEMENTED
69	45	C5	REQUESTED FACILITY NOT IMPLEMENTED
70	46	C6	ONLY RESTRICTED DIGITAL INFO
79	4F	CF	SERVICE NOT IMPLEMENTED
81	51	D1	INVALID CALL REFERENCE VALUE
82	52	D2	IDENT CHANNEL NOT EXIST
83	53	D3	CALL IDENT NOT EXIST
84	54	D4	CALL IDENT IN USE
85	55	D5	NO CALL SUSPENDED
86	56	D6	CALL ID IS CLEARED
88	58	D8	INCOMPATIBLE DESTINATION
91	5B	DB	INVALID TRANSIT NETWORK
95	5F	DF	INVALID MESSAGE; UNSPECIFIED
96	60	E0	MANDATORY INFORMATION ELEMENT IS MISSING
97	61	E1	INVALID MESSAGE
98	62	E2	MESSAGE NOT EXISTENT
99	63	E3	BAD INFOELEMENT
100	64	E4	BAD INFOELEMENT CONTENTS
101	65	E5	MESSAGE NOT COMPATIBLE CALL ST
102	66	E6	RECOVERY ON TIMER EXPIRY
111	6F	EF	ETSI PROTOCOL ERROR
127	7F	FF	INTERWORKING NOT SPECIFIED

PC sound settings for Voice over IP

A number of special PC sound card configurations must be observed when using Voice over IP to make calls via the networks and PCs. Faults such as poor sound quality and one-sided or non-existent connections can often be corrected by modifying your settings. The following chapter suggests solutions which should help when configuring a voice client. This help is generally valid since these settings are dependent on the hardware and software and from the environment where the PC is located. A detailed description is too extensive and therefore unclear.

Poor sound quality is not always an indication of a configuration error, or hardware/software faults. For example, crackling noises, i.e. short interruptions (lost voice packets), could also be caused by a high LAN load. Restructuring the LAN, migrating to 100BaseT or implementing a switch may improve the quality of the Voice over IP connection. If the G.711 audio standard is used (64 kbit/s) rather than G.723 (5 kbit/s), a considerably higher LAN load may result. For a small number of voice applications, G.711 has no noticeable effect on the LAN load. However, if Voice over IP is used intensively (up to 48 simultaneous voice connections in the case of Hicom Office PRO), voice quality can deteriorate significantly if the LAN is already overloaded.

Configuration options

1. Simultaneous talking and listening is not possible
   - The sound card driver is not fully duplex-compatible, an update must be installed to correct this
   - Incorrect voice application configuration, activate full duplex functionality in software
2. Full duplex functionality for the sound card driver can be tested with Netmeeting. Under Options / Audio you can activate/deactivate full duplex functionality. If this item cannot be modified, a fully-duplex driver must be installed for the sound card.
3. One-sided voice connections
   - Full duplex functionality activated
   - Microphone connected
   - Microphone activated for voice application
   - Check PC volume setting, activate "Microphone" under Record
   - Voice gateway in HiPath HG 1500 incorrect or does not exist
4. Own voice is echoed immediately or after a delay
   - Check PC volume setting, activate "Microphone" under Playback and under Record
     deactivate "Wave"

5. Call partner has difficulty hearing you
   - Check volume setting of PC or voice application, increase volume
   - If available, activate Microphone Booster under Volume / Playback / Advanced Settings
6. The call partner hears background noise (over-modulation)
   - If available, deactivate Microphone Booster under Volume / Playback / Advanced Settings
   - Adjust microphone sensitivity in the voice application, e.g. with Netmeeting under Options / Audio Microphone, activate "Set manually" and adjust sensitivity
   - Adjust recording volume, e.g. with Netmeeting under Options/Audio, activate the Audio Wizard
   - Change the audio standard, e.g with Netmeeting under Options / Audio / Extended, switch from G.723 Audio Codec to G.711 Audio Codec (affects the LAN load)
7. A second-long pause occurs during the call
   - Netmeeting 2.1 has difficulty upgrading to Netmeeting Version 2.11 when operated with the HiPath HG 1500 voice gateway.

Abbreviations

This is a list of all the abbreviations used in this manual.

Abbreviation	Definition
AF	Assured Forwarding (see also RFC 2597)
APS	Application program system
CAPI	Common ISDN Application Programming Interface
CHAP	Challenge Handshake Authentication Protocol
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration
DDE	Direct Data Exchange
DFÜ	Datenfernübertragung (Dial-Up Networking)
DiffServ	Differentiated Services (see also RFC 2474)
DIX V2	Ethernet standard for DIX group: DEC, Intel, Xerox
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service, resolution of names into IP addresses
DS	DiffServ
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
DSS1	Digital Subscriber Signalling System one (D channel protocol)
DTMF	Dual Tone Multiple Frequency
EF	Expedited Forwarding (see also RFC 2598)
EMC	Electromagnetic compatibility
GSM	Global System of Mobile communication
MDF	Main distributor feature
HXGM	HiPath HG 1500 Gateway Medium
HXGS	HiPath HG 1500 Gateway Small
IEEE802.1p	Institute of Electrical and Electronic Engineers (here definition of traffic/priority classes)
IP	Internet Protocol
IPX	Internetwork Packet eXchange (from Novell)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider

CDB	Customer database
LAN	Local Area Network
LCR	Least Cost Routing
MAC	Medium Access Control
MODEM	Modulator/Demodulator
MSN	Multiple Subscriber Number
NAT	Network Address Translation
NCP	Netware Core Protocol (from Novell)
NDS	Netware Directory Services (from Novell)
NLSP	Netware Link Services Protocol (from Novell)
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PING	Packet Internet Groper
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
RAS	Remote Access Service
RFC	Request for Comments
RIP	Routing Information Protocol
SAP	Service Advertising Protocol (from Novell)
SIC	Serial Interface Cable
SLA	Subscriber Line Analog (Hicom board)
SLIP	Serial Line Interface Protocol
SLU	Subscriber Line UP0/E (Hicom board)
SNMP	Simple Network Management Protocol
SPX	Sequenced Packet eXchange Protocol
STLS	Subscriber Trunk Line S0 (Hicom board)
CTRL	Control
SUA	Single User Access (in connection with NAT)
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
T-DSL	Telekom Digital Subscriber Line
TLA	Trunk Line Analog (Hicom board)

ToS	Type of Service
TS2	Trunk module S2M (Hicom board)
vCAPI	Virtual CAPI
WAN	Wide Area Network

Index

1P A31003-K5020-B811-5-7619

Reference no.: A31003-K5020-B811-5-7619 • Printed in the Federal Republic of Germany • BA 0800 1.0