innovaphone

VoIP Gateways

Manual

14,00 €
Printed in Germany by Books on Demand, Norderstedt

innovaphone AG Böblinger Str.76 71065 Sindelfingen
Tel +49 (70 31) 7 30 09-0 Fax +49 (70 31) 7 30 09-99
http://www.innovaphone.com
Ausgabe a trgwe.doc 18 300102

VoIP Gateways

Version 4.0

Contents

Figures

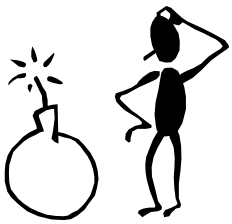
Tables

About this manual

This manual describes the innovaphone® VoIP Gateways IP 21, IP 400 and IP 3000. In terms of their design, these devices are largely identical and vary only in terms of the type and quantity of the physical interfaces. Any differences are explained in the text.

The manual describes the operation of the device as a gateway and a gatekeeper. If you wish to use the device as a telephone set too, please refer to the iPBX manual that accompanies your licence.

This manual is to be considered as an integral part of the device supplied. All advice and instructions contained therein is to be followed carefully and the device is to be used solely as specified. The manufacturer shall not be liable for personal injury, damage to property or consequential loss that can be attributed to improper use of the device.



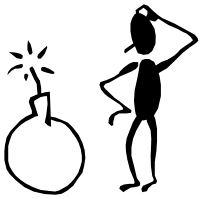
Always comply with the safety instructions given at page 183 onwards!

Conventions

At various places in this manual you will find symbols whose purpose is to direct you to sections of particular relevance.

Points out information that you may possibly first need to become acquainted with in order to configure the gateway correctly.

Gives you advice that makes the gateway particularly simple or easy to work with.



Gives you advice that must be carefully followed without fail to prevent damage to the gateway or other equipment, as well as to ensure your own personal safety.

Typographic conventions help to clarify the meaning of certain elements

LABEL	If reference is made in the text to lettering (perhaps to markings on the gateway or to graphical interface control buttons), the lettering is reproduced in small capitals with background shading.
Thin Ethernet	Technical terms are typeset in black relief.
config change dhcp0 config write	Text, which you must enter exactly in the form specified, is typeset in Courier. If a command does not fit completely on a line in the manual, it is continued on the next line indented. Of course when actually used, the entire command must be entered without the intervening new line. A new command starts again in the manual without indentation.
config change ip0 /addr ***Address*** /mask ***Mask***	If parts of a command have to be replaced with certain values, the sections to be replaced are typeset in ***bold*** and ***italic***.
RELAY0 GW1 /cgpn [m1 [m2 [...]]	Parameters, which are optional within a command line, are set out in square brackets. These brackets are therefore not to be included when entering the values.

... for experts

To help you quickly find the essential information later on, some chapters commence with a brief summary of the latter in a "... for experts" section.

Introduction to the VoIP gateways

Features of the gateways

Congratulations on your purchase of a VoIP gateway!

By choosing this Voice over IP telephony gateway and –gatekeeper you have decided in favour of a cost-effective, future-proof and user-friendly solution.

In addition to exemplary conformity to the relevant standards, the gateway offers you a multitude of features:

- ▲ High voice quality
- ▲ Up to 30 (IP 3000), 4 (IP 400) or 2 (IP 21) conversations in parallel per device, according to installed resources
- ▲ Supports all the relevant voice compression methods (G.711, G.723.1, G.726, G.729A)
- ▲ Reliable transmission of group III fax using T.38 standard
- ▲ Fully featured telephony support with overlapped and en-bloc dialling, local and remote dial tones, and comfort noise generation during gaps in conversation
- ▲ Flexible voice routing possibilities between IP, ISDN and a/b (any to any dialling)
- ▲ Flexible configuration options with connection as subscriber or trunk on the PABX, on the ISDN network (IP 3000 and 4000) or looped into the existing trunk line
- ▲ Connection of a/b terminals with advanced features and supplementary services (IP 21)
- ▲ Connection of BRI ISDN terminals with feeding (IP 400)
- ▲ Can be maintained remotely
- ▲ Optional pre-configuration
- ▲ Built-in gatekeeper

▲ Interoperability with other VoIP products

Overall the VoIP gateways offers you the optimum usage of your existing data network for voice transmission, with good quality and high user-friendliness into the bargain. Dramatic potential savings are yielded in this way and thus substantially reduced costs.

IP 3000 connectors and controls

Rear panel connectors

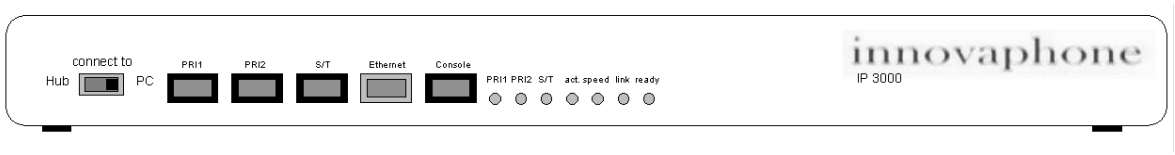
Figure 1 Rear panel connectors of the IP 3000

On the rear of the gateway there is a cold condition IEC socket for connecting the mains lead. The only way of switching the device off is by disconnecting the mains lead from the supply. It is advisable, therefore, to use a wall outlet close to the device.

As a departure from the inscribed markings, the gateway can be connected to any 47-62 Hz, 100-240 V a.c. mains supply.

Front panel indicators and connectors

Figure 2 Connectors and indicators on the front panel of the IP 3000



The following connectors and controls are to be found on the gateway's front panel (from left to right):

Connector	Function
ETHERNET SWITCH	To switch over ETHERNET connection. Left position (CONNECT TO HUB): IP 3000 connected to Hub Right position (CONNECT TO PC): IP 3000 connected directly to a PC
PRI1	RJ45 jack. To connect an ISDN primary rate trunk line
PRI2	RJ45 jack. To connect an ISDN primary rate PABX
S/T	RJ45. To connect an ISDN S/T trunk line
ETHERNET	RJ45 jack. To connect a 100Mbps Ethernet ($10/100_{BASE-T}$ auto sense)
CONSOLE	RJ45 jack. V.24 console port.
RESET button	Cold restart of gateway

Next to them (from left to right) are the following LEDs to indicate status:

Indicator	Meaning
PRI1	Trunk line is active on connection PRI1
PRI2	Device on connection PRI2 is active
S/T	Trunk line on connection S/T is active
ACT.	Data is being sent or received over the ETHERNET link

Indicator	Meaning
	ETHERNET link
SPEED	10/100 Mbps Ethernet control lamp
LINK	The ETHERNET link is ready for data transmission
READY	Device is switched on and configuration is OK

Pin assignments of the ISDN and RS232 interfaces

Table 1 Pin assignments for PRI1

PRI1	ISDN primary rate (TE, connect to ISDN network)		
	Pin 1	Receive	+
	Pin 2	Receive	-
	Pin 4	Transmit	+
	Pin 5	Transmit	-
	Pins 3, 6, 7 and 8	Unassigned	

Table 2 Pin assignments for PRI2

PRI2	ISDN primary rate (NT, connect to PABX)		
	Pin 1	Transmit	+
	Pin 2	Transmit	-
	Pin 4	Receive	+
	Pin 5	Receive	-
	Pins 3, 6, 7, and 8	Unassigned	

S/T	ISDN basic rate (TE, connection for ISDN NTBA)
	Standard ISDN basic rate (TE configuration)

Table 3 Pin assignments for console port

Console	RS232 (V.24) 9600 8N1 (DTE)		
	Pin 1	RTS	DB-9 Pin 8
	Pin 2	DTR	DB-9 Pin 6
	Pin 3	TxD	DB-9 Pin 2
	Pin 4	GND	DB-9 Pin 5
	Pin 5	GND	DB-9 Pin 5
	Pin 6	RxD	DB-9 Pin 3
	Pin 7	DSR	DB-9 Pin 4
	Pin 8	CTS	DB-9 Pin 7

To operate the console port, you can prepare a suitable cable with an RJ-45 plug on one end and DB-9 plug on the other.

If you already have a DB-9 to RJ-45 adapter with the designation TERMINAL, you can use this instead together with a *rollover* RJ-45 cable. With such a cable all of the pins are linked in a cross-over manner, i.e. pin 1 with pin 8, pin 2 with pin 7 etc

Set up your PC's RS232 interface as follows:

Table 4 Console port settings

Speed in bps (baud)	9600
Data bits	8
Parity	None
Stop bits	1
Protocol / Flow control	None

The serial number label

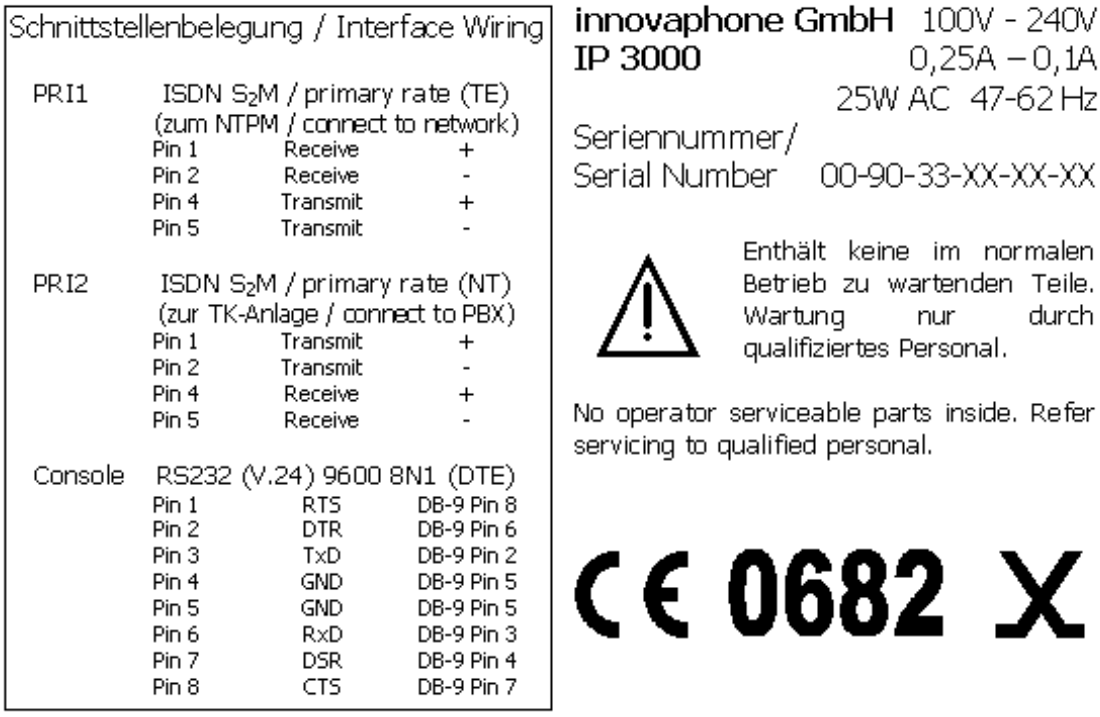
The serial number label is located on the underside of the case.

The last three hyphen-separated (`-´) hexadecimal numbers (shown as `XX-XX-XX´ in the figure) represent the serial number of your IP 3000, whilst the first

three hexadecimal numbers are constant as innovaphone®'s manufacturer identification code.

The serial number is at the same time the MAC address of your IP-3000.

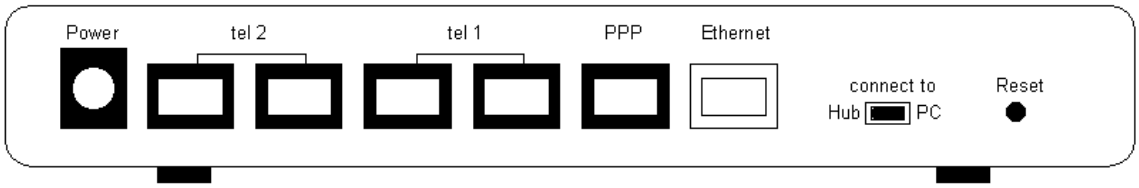
Figure 3 The serial number label



IP 400 connectors and controls

Rear panel connectors

Figure 4 IP 400 Connectors



The following connectors/switches are to be found on the gateway's rear panel (from left to right):

Table 5 Connectors and Controls of the IP 400

Connector	Function
POWER	For the supplied plug-in mains adapter, 12V 900mA
TEL2 (first jack)	RJ45 jack. For ISDN –telephone, -PABX or –trunk line
TEL2 (second jack)	RJ45 jack. To optionally connect a second telephone to TEL2
TEL1 (first jack)	RJ45 jack. For ISDN –telephone, -PABX or –trunk line
TEL1 (second jack)	RJ45 jack. To optionally connect a second telephone to TEL1
PPP	RJ45. To connect an ISDN trunk line
ETHERNET	RJ45 jack. To connect a 10Mbps Ethernet (10_{BASE-T})

Connector	Function
ETHERNET SWITCH	To switch over ETHERNET connection. Left position (CONNECT TO HUB): IP 400 connected to Hub Right position (CONNECT TO PC): IP 400 connected directly to a PC
RESET button	Cold restart of gateway

Front panel indicators

Figure 5 IP 400 Indicators

The following LEDs for status indication are to be found on the front panel of the gateway (from left to right):

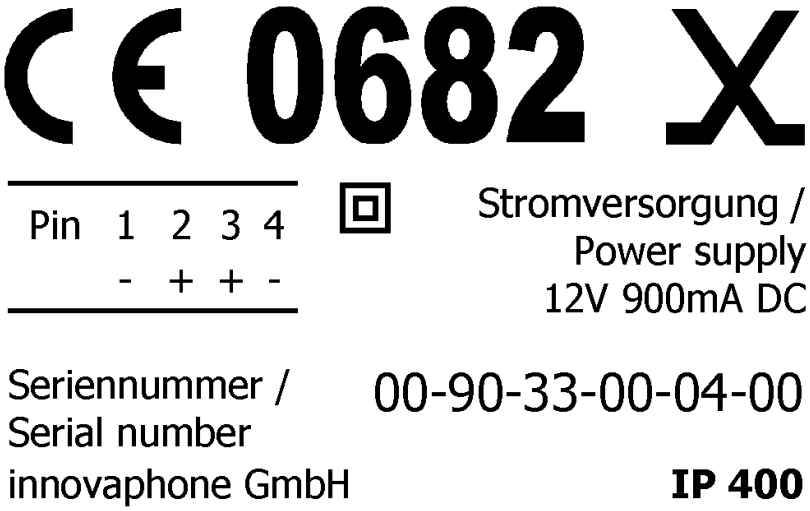
Table 6 IP 400 Indicators

Indicator	Meaning
READY	Device is switched on and configuration is OK
ETHERNET LINK	The ETHERNET link is ready for data transmission
ETHERNET ACT.	Data is being sent or received over the ETHERNET link
PPP	Trunk line connected to PPP is active
TEL1	Device or trunk line connected to TEL1 is active
TEL2	Device or trunk line connected to TEL2 is active

The serial number label

The serial number label is located on the underside of the case.

Figure 6 The serial number label



The last three hyphen-separated (`-´) hexadecimal numbers (shown as `XX-XX-XX´ in the figure) represent the serial number of your IP 400, whilst the first three hexadecimal numbers are constant as innovaphone®'s manufacturer identification code.

The serial number is at the same time the MAC address of your IP-400.

IP 21 connectors and controls

Connectors and Indicators on the Upper Panel

The international and 1-channel versions of the IP 21 have no connectors on the upper panel. The German 2-channel version of the IP 21 has the following TAE connectors (from left to right):

Table 7 Connectors on the Upper Panel of the IP 21

Connector	Function
1 N	TAE Jack. For connecting a fax machine, telephone answering machine or modem to TEL1.
1 F	TAE Jack. For connecting a telephone to TEL1.
2 N	TAE Jack. For connecting a fax machine, telephone answering machine or modem to TEL2.
2 F	TAE Jack. For connecting a telephone to TEL2.

Please note that only one call at a time can be active on TEL1 and TEL2.

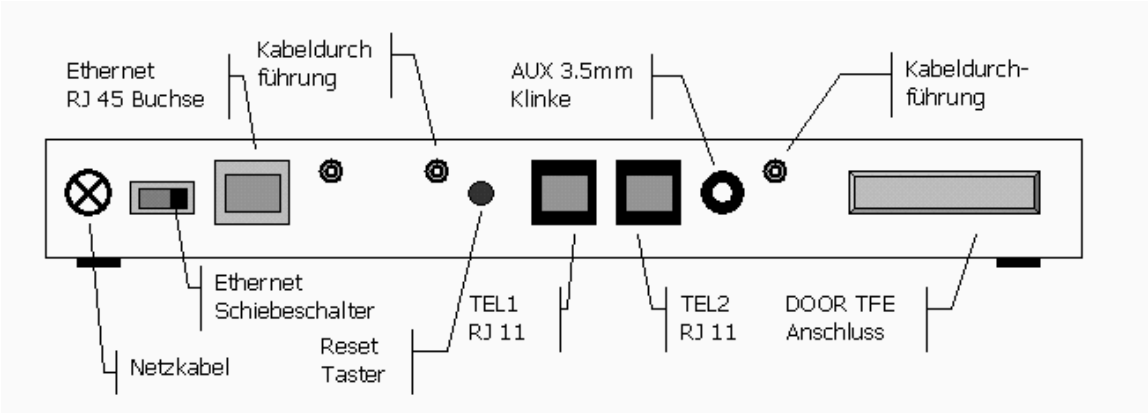
There are also the following indicators on the upper panel of the IP 21 (from left to right):

Table 8 Indicators on the Upper Panel of the IP 21

Indicator	Meaning
READY	Device is switched on and configuration is OK.
100 M	10/100 Mbps Ethernet control lamp Comes on when a 100Mbps Ethernet Link is recognized.
LINK	Comes on when an Ethernet Link ready for data transmission is recognized. The indicator flashes when active.
LINE 1	Indicates activity on TEL1 (1 N or 1 F).
LINE 2	Indicates activity on TEL2 (2 N or 2 F).
DOOR	Indicates activity on DOOR (door intercom).
AUX	Indicates activity on AUX (audio interface).

Front panel connectors

Figure 7 Front panel connectors of the IP 21



The front panel of the IP 21 has the following connectors and controls (from left to right):

Table 9 Connectors and controls on the front panel of the IP 21

Connector	Function
ETHERNET SWITCH	To switch over ETHERNET connection. Left position: IP 21 connected to Hub/Switch Right position: IP 21 connected directly to a PC
ETHERNET JACK	RJ 45. For connection to an Ethernet Hub/Switch or directly to a PC.
TEL1	RJ 11. For connecting an analogue terminal to TEL1.
TEL2	RJ 11. For connecting an analogue terminal to TEL2.
AUX	3.5 mm stereo jack bush. For connecting an audio source to AUX.
DOOR	4+n connector 15-pin strip terminal. For connecting a door intercom.

Pinout of the Door intercom (DI) interface

The door intercom (DI) is connected to the strip terminal on the front panel of the IP 21. The pinout of the strip terminal is as follows (from left to right):

Table 10 Pinout of the Door intercom (DI) interface

Number	Identification	Usage
1	E1	not used
2	E2	not used
3	K2	Ringer 2
4	K1	Ringer 1
5	K	Bell transformer, approx. 8 V AC
6	11	Door opener 1
7	53	Bell transformer, approx. 8 V AC
8	69	not used
9	+	Microphone/Loudspeaker voltage
10	2	Loudspeaker ground
11	6	Microphone ground
12	13	not used
13	12	not used
14	X	Bell transformer
15	Y	Door opener 2

Connections inside the device

The IP 21 has a connector box under the shrouding cover for connecting two analogue terminals. These can be used as an alternative to the TAE and RJ 11 jacks.

- ▲ Before opening the device, disconnect the mains adapter from the mains supply
- ▲ Open the spring latches on the left and right beside the RJ 11 jacks on the front panel
- ▲ Open the housing cover fully
- ▲ The connector box is on the right beside the inscription: FAX OVER IP and is marked: J301
- ▲ Use terminal connections A1 and B1 for connecting a terminal to TEL1 or terminal connections A2 and B2 for connecting a terminal to TEL1
- ▲ For feeding out the connection cable there are two grooves in the front panel
- ▲ When replacing the cover, make sure the cord grip is correctly in place.

The serial number label

The serial number label is located on the underside of the case.

The last three hyphen-separated (`-´) hexadecimal numbers (shown as `XX-XX-XX´ in the figure) represent the serial number of your IP 21, whilst the first three hexadecimal numbers are constant as innovaphone®'s manufacturer identification code.

Figure 8 The IP 21 serial number label

The serial number is at the same time the MAC address of your IP-21.

Commissioning

The gateway is put into operation with the following steps:

- ▲ Installation
- ▲ Setting up of IP interface parameters
- ▲ Definition of the operating environment

The following sections assume that the gateway is in the original state as shipped, and consequently that the standard configuration is loaded. If you are not certain about the state of the configuration, it is advisable to reinstate the standard configuration before proceeding.

Installation of IP 21

Refer to the Safety instructions for the IP 21 on page 183.

The devices may be wall-mounted. The horizontal distance between the suspension points is 16 cm.

Ensure that there is adequate ventilation if installing the unit in a cabinet.

Installation of IP 400

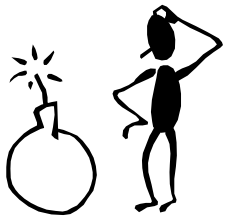
Pay attention to the Safety instructions for the IP 400 on page 184.

The devices may be wall-mounted. The horizontal distance between the suspension points is 12 cm. Take care when mounting not to damage the plate guard film.

Units can be stacked. Ensure that there is adequate ventilation if installing the unit in a cabinet.

Installation of IP 3000

Pay attention to the Safety instructions for the IP 3000 on page 185.



Units can be stacked. Fitment into a 19'' cabinet is also possible using the supplied mounting brackets. In this case the mounting brackets are secured to the front underside of the gateways using the screws supplied. If, for some reason, you do not used the screws supplied for this purpose, ensure that the screws used are not longer than 6mm since otherwise contact may be made with the board giving rise to faults.

Ensure that there is adequate ventilation if installing the unit in a cabinet.

Configuration of the LAN Access

The gateway comes supplied with a standard configuration. In this configuration, the gateway will attempt to configure the IP parameters by DHCP. The built-in DHCP client is therefore activated and the DHCP server also incorporated is deactivated.

Find out from your network administrator whether your network has a DHCP server at its disposal.

If no DHCP server is operating in your network or you do not want any automatic configuration undertaken by DHCP for other reasons, refer to the section "Setting up the IP interface parameters without DHCP" below which starts on page 34. In this case your PC also needs to have available a twisted-pair[1] Ethernet adapter.

If a DHCP server is available, refer to the section “Setting up the IP interface parameters with DHCP” below.

In both cases you can access the gateway via Ethernet. The IP 3000 also offers the option of access via the console port. For this you will need a terminal programme on your PC as well as a suitable connecting cable. The section "Pin

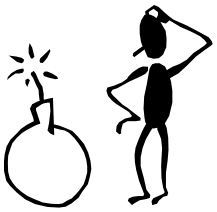
[1] 10_{BASE-T} for the IP 400 and $10/100_{BASE-T}$ for the IP 3000 and IP 21.

assignments of the ISDN and RS232 interfaces" starting on page 16 gives a detailed description of the type of cable required.

Restoring the standard configuration

You can reset the standard configuration at any time by pressing the RESET button and then keeping it pressed for a few seconds[2]. With this, the gateway is re-initialised and takes up a special "Reset" mode. Subsequent switching on and off returns it to normal operating mode[3]. Remember though, that you will lose all the preceding configuration data as a result of this procedure. Where necessary, however, you can save the current configuration in a file beforehand.

Switching on the gateway



Using either the mains adapter supplied (IP 400) or the mains lead (IP 3000), connect up the gateway to the nearest 100V-240V wall socket. For the IP 400 do not use any mains adapter other than the one supplied. Other mains adapters could damage your gateway.

The mains socket-outlet must be close to the device and easily accessible. The only way to switch off the device is to disconnect the power supply.

The device is now switched on and the READY LED at the far left on the front panel comes on.

---

[2] For the IP 400 and IP 3000 this takes around 5 seconds, for the IP 21 around 10 seconds

[3] Press and release the Reset button once more to return the gateway to normal operating mode

In this case the DHCP Server mode is activated (see from Page 34), whereas after switching on/off the DHCP Client mode (see Page 31) is activated.

Setting up the IP interface parameters with DHCP

... for experts

- ▲ If possible use the gateway's DHCP client!
- ▲ In the standard configuration the DHCP client is switched on only after "power cycle". After doing a "Reset" via the Reset button the DHCP server switches on
- ▲ The MAC address can be found on the adhesive label bearing the serial number
- ▲ "Using the "nbtstat" command in Windows 95/98, Windows NT and its derivatives you can now determine the assigned IP address.
- ▲ " shows you the IP address"
- ▲ The configuration is concluded by telnet or via the console port (IP 3000 only) with

  config change CMD0 /user ***name,pw***
  config change dhcp0 /mode client
  config write
  reset
- ▲ or via the Web browser

If your network has a DHCP server available, configuration of the IP interface parameters by DHCP is the most convenient method.

You can ask your network administrator to reserve a permanent IP address for the gateway via DHCP. For this, please notify him of your gateway's hardware address (for this please refer to section "The serial number label" from page 17 or 21 onwards).

In the standard configuration, the gateway attempts a configuration via DHCP after every switch-on. After every "hard reset"[4] the configuration mode is activated without DHCP, however (for this refer to "Setting up the IP interface parameters without DHCP" below).

[4] I.e. with the RESET button, not by switching on/off and not with the `reset` command either.

If you are configuring your gateway via the console port, read from page 33 onward as to how the configuration is to be concluded.

Otherwise, proceed as follows:

- Set the ETHERNET SWITCH on the rear to the "CONNECT TO HUB" position, or to the left position for the IP 21.
- Connect up the ETHERNET RJ45 connector on the gateway and the RJ45 connector on your Ethernet hub or switch using the twisted pair cable supplied.
- Switch the gateway off and then on again in order to activate the DHCP client.

The gateway is now assigned an IP address. If your network administrator has not set up a permanent IP address for you, you now need to determine which IP address has been assigned. There are two ways of doing this:

- The simplest option is to ask your network administrator. He can determine the assigned IP address in the DHCP server administration programme.
- The other option is to consult the gateway itself. Following successful configuration, the gateway logs the NetBIOS name "***id***-XX-XX-XX"[5], where "XX-XX-XX" are to be replaced by the last three hexadecimal figures of the serial number (see section "The serial number label" from Page 17 or 21 onwards).

  Using the "nbtstat" command in Windows 95/98, Windows NT and its derivatives you can now determine the assigned IP address[6].

  ```
  C:> nbtstat –R
  C:> nbtstat –a ip3000[7]-XX-XX-XX
  NetBIOS Remote Machine Name Table
    Name              Type        Status
  ---------------------------------------------
  IP3000-XX-XX-XX<00>  UNIQUE      Registered
  195-226-104-217<00>  UNIQUE      Registered
  MAC Address = 00-90-33-XX-XX-XX
  ```

  In the above example the gateway has the IP address 195.226.104.217.

  Under Linux you can use the command "nmblookup" for this[8]:

---

[5] Where ***id*** is ip21, ip400 or ip3000, according to the device

[6] Display of the IP address with `nbtstat` does not work if your NetBIOS environment is configured exclusively for name resolution via WINS. If the `nbtstat` command does not find your IP 400, talk to your network administrator in order to configure the NetBIOS name resolution appropriately.

[7] ip400 or ip21 respectively, according to the device

[8] Provided that the "SAMBA" package is installed.

[dvl@cobalt ~ 2] $. nmblookup ip400-**XX-XX-XX**

Got a positive name query response from 195.226.104.220 (195.226.104.220)

195.226.104.220 ip400[6]-**XX-XX-XX**<00>

[dvl@cobalt ~ 3] $.

▲ You can conclude the installation by telnet command (or, for the IP 3000, via the console connected to the serial port) or via the Web browser.

To work with telnet, link the program to the assigned IP address: ***ipaddr***.

Under Windows 95™, Windows 98™, Windows NT (and its derivatives) and Linux do this by executing the command:

telnet ***ipaddr***

The gateway responds with its version number (see page 37). For administration you now need to establish your identity with user name and password. In standard configuration the user name is admin and the password (according to the device) is ip3000, ip400 or ip21.

The gateway then responds with the command prompt "$".

You can now enter commands to the gateway.

You conclude the definition of interface parameters with the following commands:

▲ To prevent unauthorised access you should change the user name and password immediately

config change CMD0 /user ***name***,***pw***

where ***name*** is the user name you have chosen for administration and ***pw*** is the associated password. Each of the two values can be up to 15 characters long

▲ Define the configuration by DHCP as the standard method (even after a reset)

config change dhcp0 /mode client

▲ Save the configuration permanently

config write

reset

Your gateway is now ready for operation on the local network.

You can now configure the gateway to suit your own particular circumstances. The procedure is described on page 40.

You conclude the definition of interface parameters as follows using the Web browser:

▲ Run your Web browser and enter the address http://***ipaddr.***

Start the configuration applet via the CONFIG entry in the GATEWAY menu (see page 40). To do this you need to log on to the device. The gateway responds with its version number (see page 37). For administration you now need to establish your identity with user name and password. In standard configuration the user name is admin and the password (according to the device) is ip3000, ip400 or ip21.

The gateway then responds with the command prompt "$".

▲ To prevent unauthorized access, you should immediately change the user name and password in the GENERAL SETTINGS under CHANGE LOGIN PARAMETERS (see page 151)

▲ Specify in the IP INTERFACES / ETHERNET INTERFACE field under DHCP the DHCP "CLIENT" MODE (see page 46)

▲ Save the configuration by pressing SAVE and ACTIVATE (see page 162)

Setting up the IP interface parameters without DHCP

If your network does not have a DHCP server, you have to set up the IP interface parameters of the gateway yourself.

... for experts

▲ If possible configure your PC by DHCP!

▲ In the standard configuration, the DHCP server of the gateway is switched on only after a "reset".

▲ Connect up the Ethernet connectors of the gateway and PC "back to back" (sliding switch to "CONNECT TO PC")

▲ If your PC is configured by DHCP, update the IP address with winipcfg or ipconfig. Otherwise set the IP address of the PC permanently to 192.168.0.2.

▲ The gateway has the address 192.168.0.1.

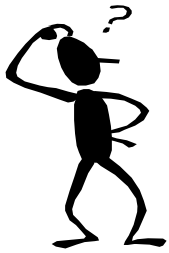
▲ Conclude configuration via telnet with

config change CMD0 /user ***name,pw***
config change ip0 eth0 /addr ***Address*** /mask ***Mask***
If the device is to ***have*** access to other networks, specify the route to the standard gateway with the command:

▲

config change dhcp0 /mode off
config write
reset

▲ Resetting of ARP table
C> arp –d 192.168.0.1

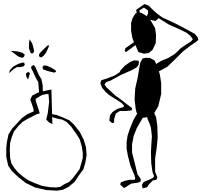


Ask your network administrator if you are not certain which IP address and which subnet mask you can assign for the gateway, as well as whether you can use a default gateway, and if so, which one.

If you are configuring your gateway via the console port, read from page 37 onward as to how the configuration is to be concluded.

In addition, you have to deactivate the DHCP client built into the gateway and activate the built-in DHCP server. Both steps are effected by pressing the RESET button briefly after a cold restart.

For configuration, the gateway is first connected directly to your computer.



▲ If your computer is connected to the local network, disconnect it from the network for the duration of the initial configuration of the gateway.

If the computer is connected to the network through a BNC cable (thin Ethernet), remove the BNC T-piece from the Ethernet adapter. Take care to ensure that the network cable is not detached in the process, as otherwise your network will no longer work.

If the computer is connected to the network through a twisted pair cable with RJ45 plugs, unplug the cable from the Hub or Switch or withdraw it from the wall-jack, depending on where your computer is connected up.

▲ Set the ETHERNET SWITCH on the rear to position "CONNECT TO PC". This makes the gateway function as an Ethernet Hub for your computer.

▲ Connect up the ETHERNET RJ45 connector and the RJ45 connector of your Ethernet adapter with the twisted pair cable supplied.

Your computer's Ethernet adapter will now be configured to allow it to communicate with the gateway in the state as shipped. The most convenient way for this to be done is with your computer obtaining its IP configuration via the DHCP protocol.

If your computer can handle the DHCP protocol, you should use it in any case. If this is not the case, the configuration can be carried out manually.

▲ If your computer is configured for use of the DHCP protocol, the assignment of a suitable IP address for communication with the gateway is now brought about

Your PC must now be assigned an IP address suitable for the initial configuration of the gateway. Under Windows 95™ and Windows 98™ this is achieved by executing the command:

winipcfg

and selecting the options "RELEASE ALL" and "UPDATE ALL".

Under Windows NT and its derivatives you execute the commands:

ipconfig /release /all

ipconfig /renew /all

You can also restart your computer, if desired.

▲ If your computer is configured with permanent IP addresses, alter the settings in accordance with the following table

Table 11 IP configuration for commissioning

Address	192.168.0.2
Network mask	255.255.255.0

Under Windows 95™, Windows 98™ and Windows NT and its derivatives this is done by suitably adjusting the settings for the TCP/IP protocol in SYSTEM CONTROL in the area NETWORK. In this case the computer needs to be restarted.

▲ You can conclude the installation by telnet command (or, for the IP 3000, via the console connected to the serial port) or via the Web browser.

To work with telnet, link the program to the assigned IP address: 192.168.0.1.

Under Windows 95™, Windows 98™, Windows NT™ (and its derivatives) and Linux do this by executing the command:

telnet 192.168.0.1

The gateway responds giving its version number. For administration you now need to establish your identity with user name and password. The gateway responds with its version number (see page 37). For administration you now need to establish your identity with user name and password. In standard configuration the user name is admin and the password (according to the device) is ip3000, ip400 or ip21.

The gateway then responds with the command prompt "$".

The gateway then responds with the command prompt "$".

You can now enter commands to the gateway.

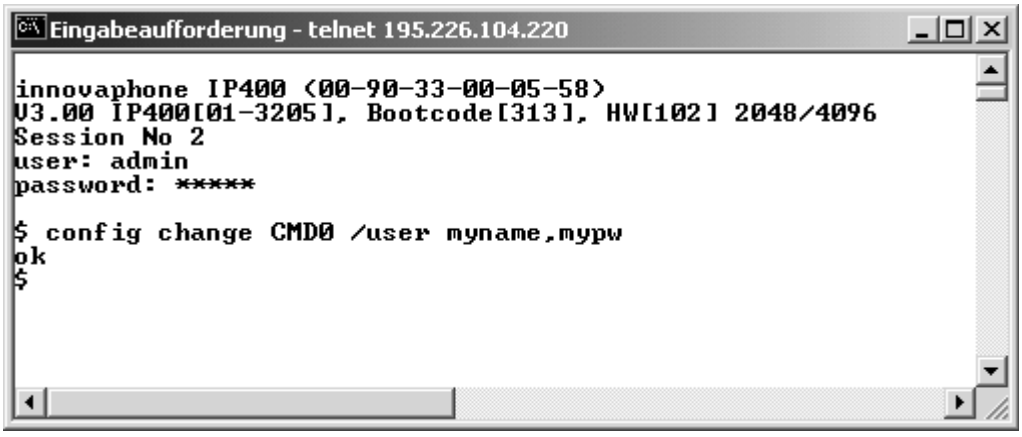
You conclude the definition of interface parameters as follows:

▲ To prevent unauthorised access you should change the user name and password immediately

config change CMD0 /user ***name***,***pw***

where ***name*** is the user name you have chosen for administration and ***pw*** is the associated password. Each of the two values can be up to 15 characters long

Figure 9 Logging on to the gateway via telnet



▲ If the device is to have access to other networks, specify the route to the standard gateway with the command:

config change ip0 rt0 /gateway ***Address***

where *Address* is the IP address of your standard gateway in "dotted-decimal" format *x.x.x.x.*

▲ Define the IP interface parameters for the gateway using the commands

config change ip0 eth0 /addr ***Address*** /mask ***Mask***

config change dhcp0 /mode off

config write

reset

Address has to be an unassigned and valid IP address from your local network and *Mask* a correspondingly suitable subnet mask. Both are specified using the "dotted-decimal" notation *x.x.x.x* (e.g., **255.255.255.0** for the subnet mask)

You conclude the definition of interface parameters as follows using the Web browser:

▲ Run your Web browser and enter the address http://192.168.0.1**.**

Start the configuration applet via the CONFIG entry in the GATEWAY menu (see page 40). To do this you need to log on to the device. The gateway responds with its version number (see page 37). For administration you now need to establish your identity with user name and password. In standard configuration the user name is admin and the password (according to the device) is ip3000, ip400 or ip21.

The gateway then responds with the command prompt "$".

▲ To prevent unauthorized access, you should immediately change the user name and password in the GENERAL SETTINGS under CHANGE LOGIN PARAMETERS (see page 151)

▲ Specify in the IP INTERFACES / ETHERNET INTERFACE field under DHCP the DHCP "OFF" MODE (see page 46)

▲ Specify in the same place the parameters under ETHERNET INTERFACE ADDRESS

▲ Specify in the same place your DEFAULT IP ROUTER

▲ Save the configuration by pressing SAVE and ACTIVATE (see page 162)

The gateway is now ready for connection to your local network.

- ▲ Set the ETHERNET SWITCH on the rear to the "CONNECT TO HUB" position. The gateway now works like a standard Ethernet terminal and can be connected to a hub or switch.
- ▲ Connect the gateway's ETHERNET jack to your hub or switch or respective wall jack.

Do not forget to re-connect your computer to your local network and to restore its original IP configuration.

If you want to configure further gateways in this way, before connecting the next device to your PC you first have to delete the assignment of the IP address to the hardware address[9]. Under Windows™ and Unix™ systems this is done using the arp command.

```
C> arp –d 192.168.0.1
```

You can now configure the gateway to suit your own particular circumstances. The procedure is described on page 40.

[9] This is necessary because despite the new device having a different hardware address, it has to respond to the same IP address.

Defining the working configuration

The working configuration can be set up using the telnet programme or via your Web Browser. This section describes the use of the Web Browsers for configuration, which is normally the most convenient method for common application scenarios. However, information about configuration using the telnet commands can be found in the VoIP gateway reference manual.

Please note that your browser must support HTML 4.0, HTTP 1.1 and Java applets. We test the configuration applet with Microsoft's Internet Explorer™ 6.x. Certain functions, such as sorting lists, require the XML and XML stylesheets function. However, the devices are fully functional even without these functions.

If access to the gateway is protected by a firewall, the services tcp/23 (telnet) and tcp/80 (http) need to be enabled. Please note that only configuration access is enabled as a result. If calls, too, are to pass across the firewall, please refer to section "NAT and Firewalls" from page 189 onwards.

Definition of the working configuration requires the following steps:

- Configuration of the ISDN interfaces.
  With this you specify the type of connection for ISDN interfaces of the gateway.
- Definition of further VoIP gateways and terminals.
  Through this you inform the gateway as to which further innovaphone gateways, VoIP gateways from third-party manufacturers and VoIP terminals or PC programmes you want to use.
- If necessary, configuration of the WAN interfaces.
  Through this you specify the parameters of your Internet or intranet access, in the event that you also intend using the gateway as an ISDN BRI- or PPPoE-IP router[10].

[10] Only the IP 3000 and IP 400 can work as ISDN routers. The IP 3000 needs in addition the optional HDLC hardware module. The IP 3000, IP 400, IP 200 and IP21 can work as PPPoE routers.

▲ Configuration of the call routings.
Through this you specify which terminals are to be reached in the end under which numbers.

The configuration of the optional iPBX components is described in a separate manual, shipped together with your iPBX licence.

First launch your Web Browser and open the URL **http://***Address***/**, where *Address* is the IP address of the gateway that you are about to configure. It has to be typed in "dotted-decimal" format (*x.x.x.x)*. Should you have entered a host name for the gateway in the DNS name directory, you can of course use this too, e.g. **http://h323gw.ihredomaene.de**.

Now, click on “Config” in order to start the configuration applet. You will be requested to enter the correct (administrator's) user id and password that was entered during commissioning (refer to page 37).

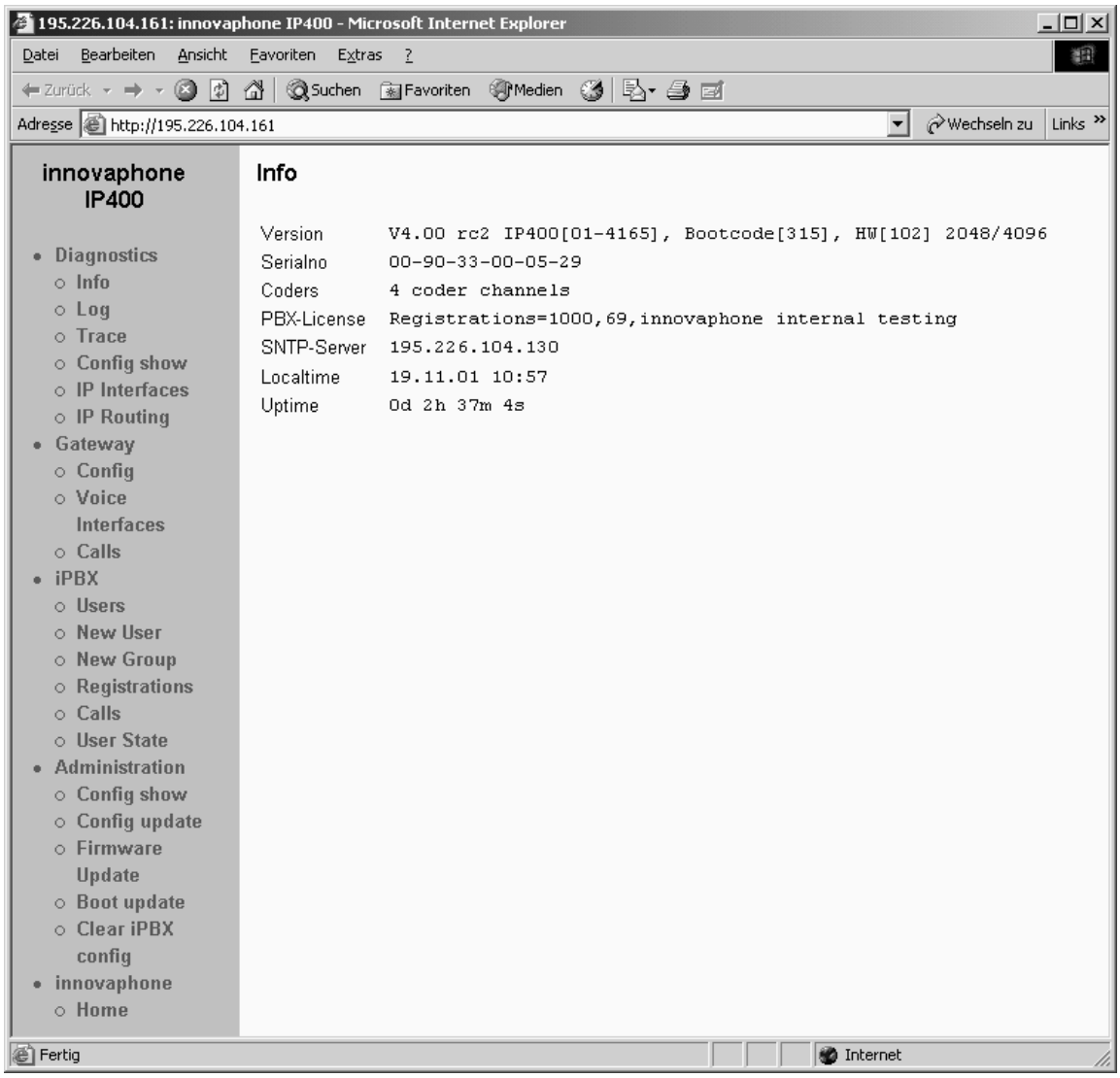
General details about the configuration interface

The gateway's configuration interface consists of two parts. The first part consists purely of HTML pages and is mainly used for calling up run-time information. Operation is by the familiar method used with other Web sites. The individual functions are described in more detail from page 164 onwards.

The configuration proper is done via a separate configuration applet, a JAVA application. You start the applet by invoking the "Config" entry in the administration interface.

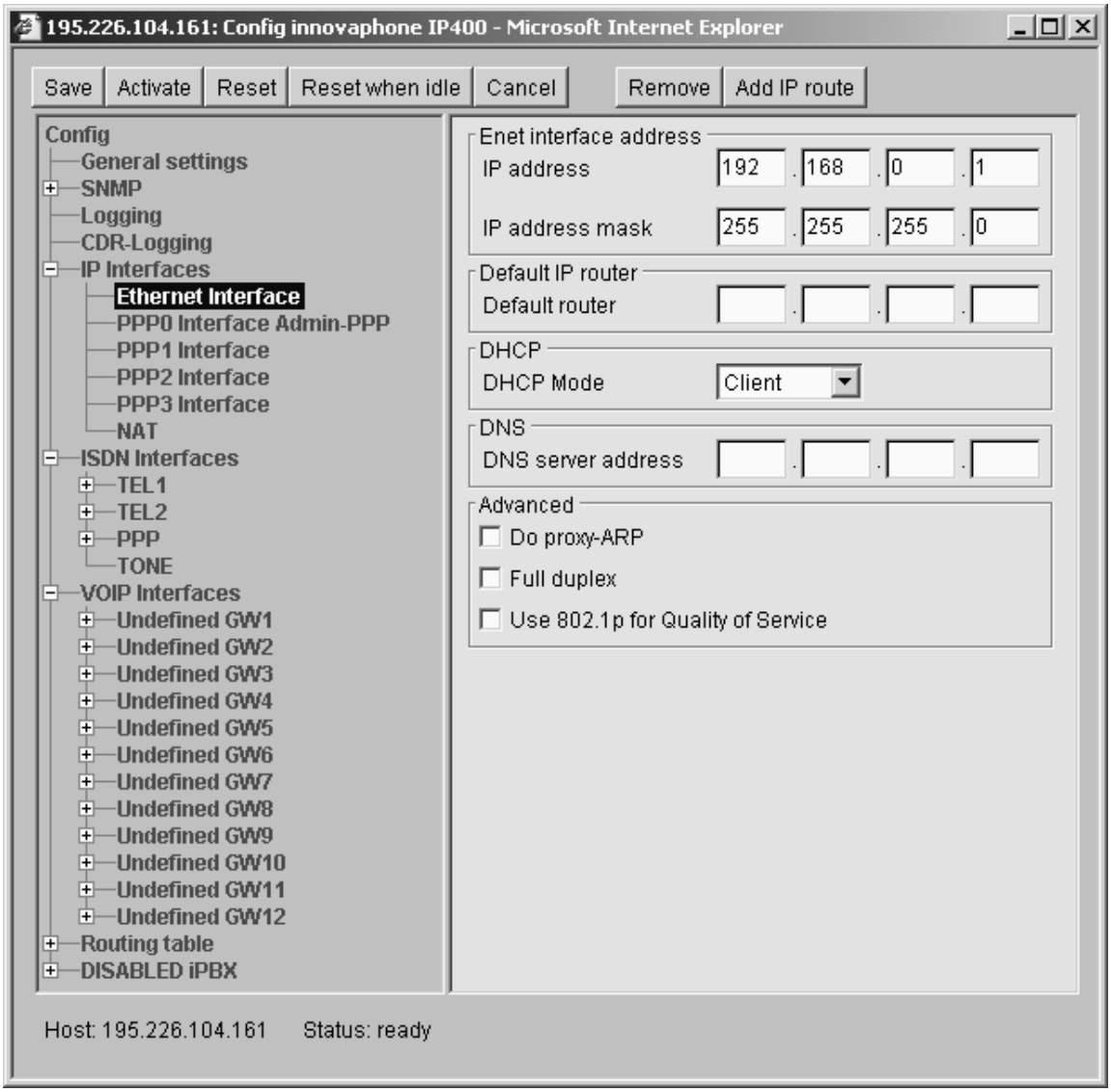
The applet runs in a separate window. This allows you to access the various administration interface functions during configuration of the gateway, without having to close the configuration applet or open a second browser window.

Figure 10 The administration interface



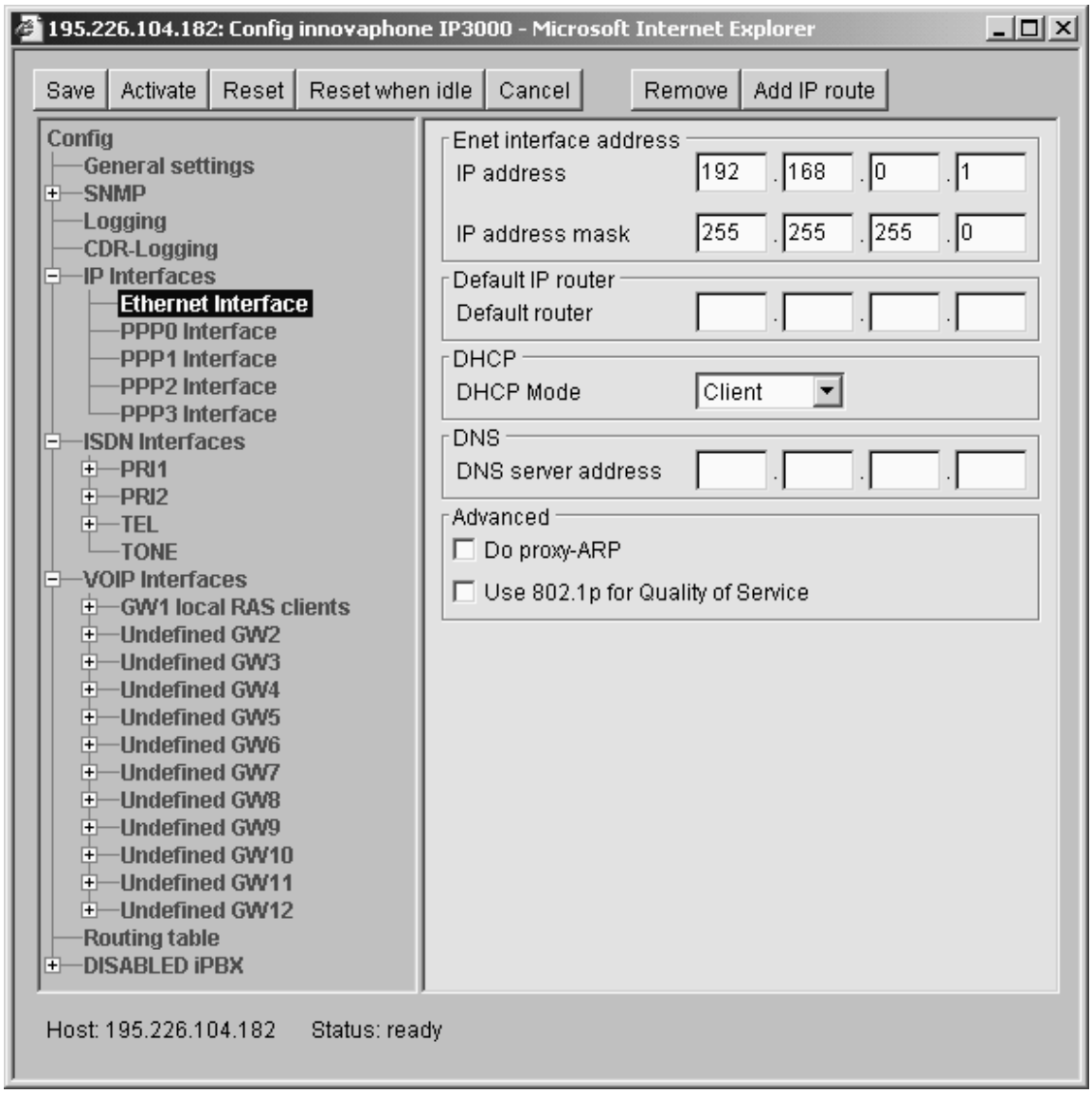
Two areas are to be found in the applet. On the left-hand side, the entire configuration of the gateway is depicted as a tree, like the one you are accustomed to when using a file browser. When you select an object in this tree by clicking on it, detailed information about it is displayed on the right-hand side. The window on the left is used to navigate through the configuration. Entries can be made in the right-hand window only.

Figure 11 The configuration applet of IP 400



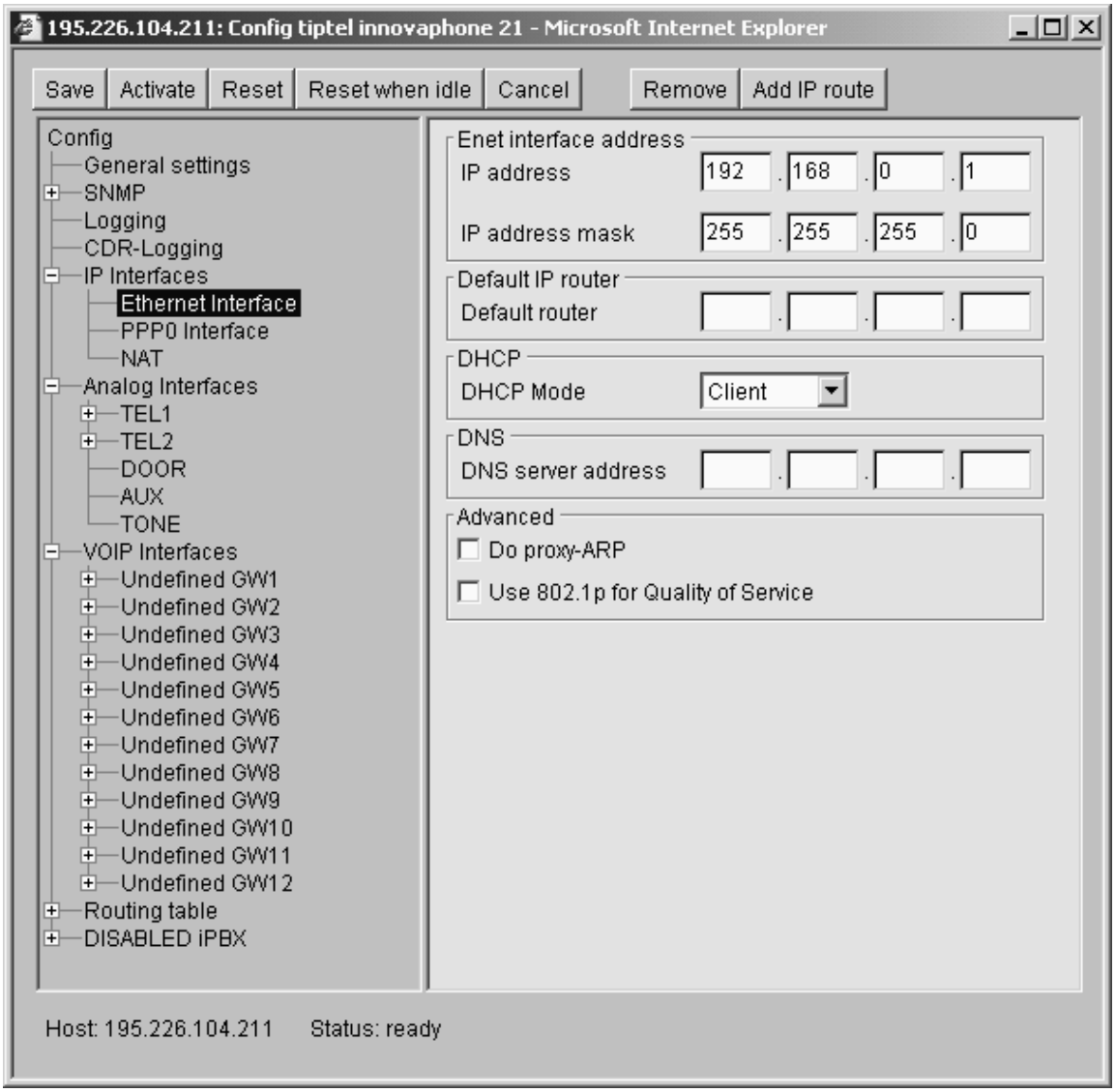
A button bar is to be found at the upper border of the applet window. The SAVE, ACTIVATE, RESET, RESET WHEN IDLE and CANCEL buttons relate to the entire configuration. The remaining buttons (ADD, REMOVE etc.), are applicable to the object currently selected in the left-hand window.

Figure 12 The configuration applet of IP 3000



For most of the configuration elements you can preset your own names in the DESCRIPTION field. These then always appear in the tree depiction on the left-hand side. If you make frequent use of this option it helps you maintain an overview later on.

Figure 13 The configuration applet of IP 21



Various configuration forms contain the DISABLE option. This allows you to temporarily disable the object to be configured there, without losing the configuration settings. The object is, so to speak, "commented-out".

Configuring the IP interfaces

Configuring the Ethernet interface

The Ethernet IP interface is usually configured during the commissioning and normally needs no further alteration. Should this be the case, however, you can adjust the settings in the IP / ETHERNET area.

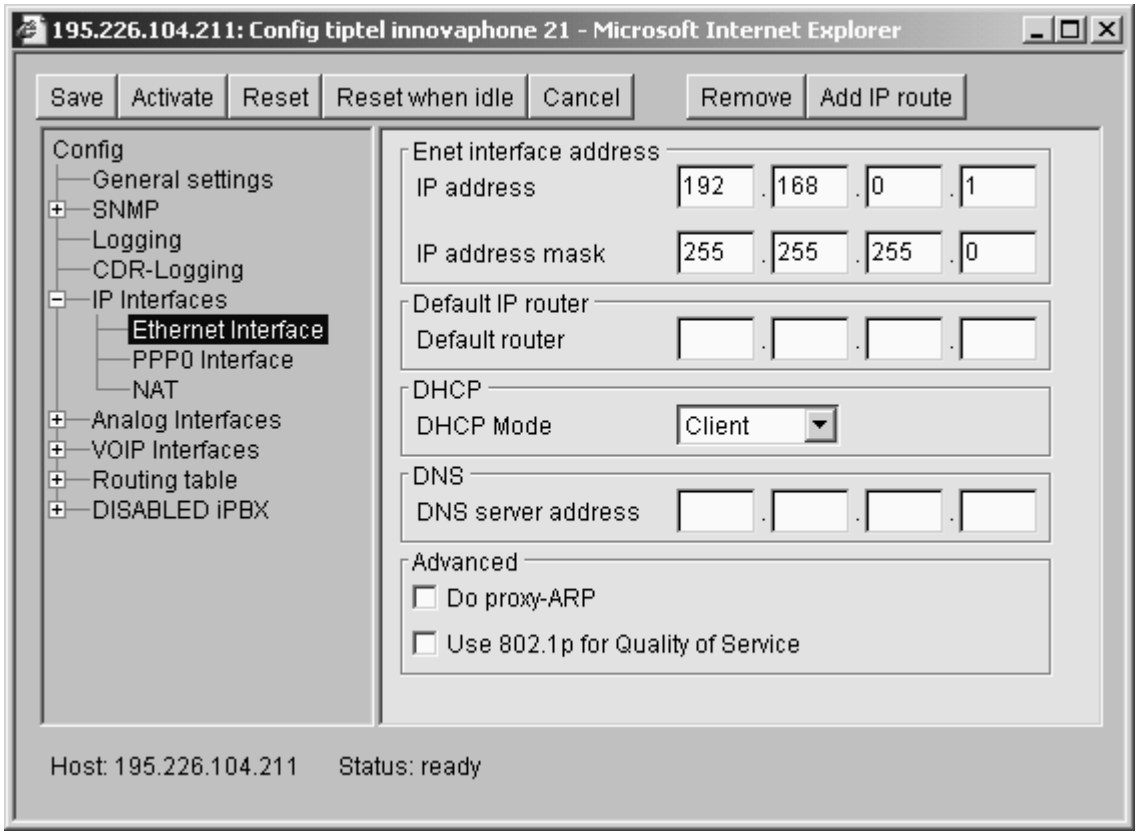
The gateway's DHCP function has four operating modes in all:

Mode	Function	Usage
Off	No DHCP function	If you configure the IP parameters permanently
Server	DHCP server[11] active	Hooked up devices are given an IP address assigned by the gateway.
Client	DHCP client active	The gateway receives its IP configuration from a DHCP server in the network. Section "DHCP configuration options" from page 48 onwards lists the evaluated DHCP options
Automatic	After switching on the DHCP client is active, after a reset the DHCP server is active	The gateway is in the as-shipped state (and after a long reset is in this state (see page 30))[12].

[11] This setting makes sense in exceptional cases only since the gateways contain no complete DHCP servers. It is used primarily in test- or demo structures.

[12] This setting makes sense at the start only. During the commissioning it should in any case be replaced by the setting "off" or "Client"

Figure 14 The IP parameters of the Ethernet interface

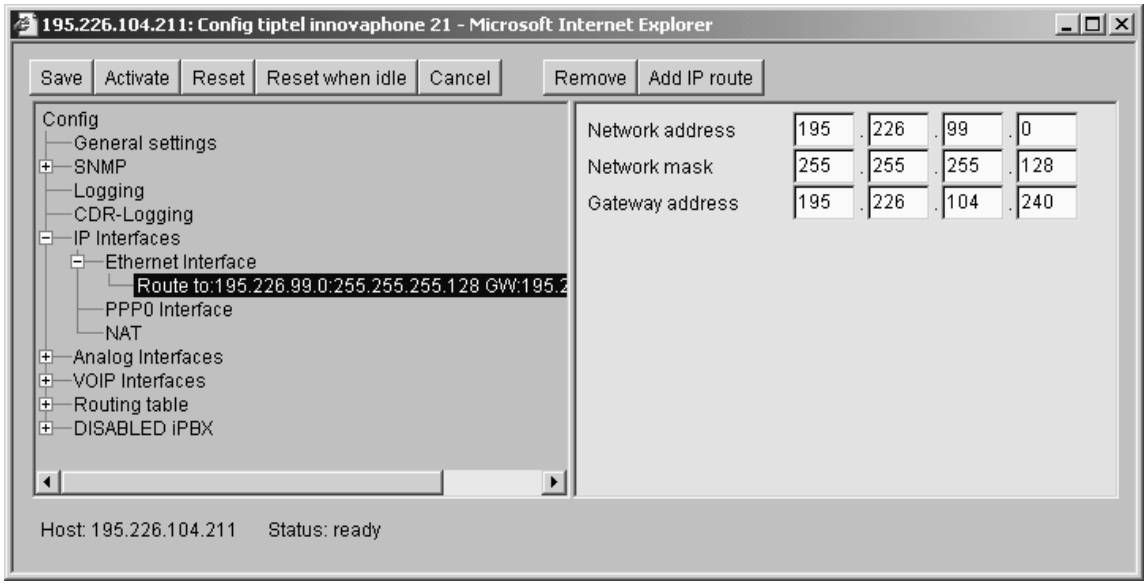


- For complete configuration of the Ethernet interface the standard gateway of your network must also, if necessary, be registered as DEFAULT GATEWAY.
- If still further routes have to be inserted on the other side of the standard gateway, this can be done via the ADD IP ROUTE button.

  For network routes specify the NETWORK ADDRESS with the host part at 0 as well as the correct NETWORK MASK.

  For host routes specify the complete IP address of the host and the NETWORK MASK 255.255.255.255.

Figure 15 Adding routes to the Ethernet interface



- If it is not intended that your gateway should also take on the function of a WAN router, leave the DNS SERVER ADDRESS entry blank and deactivate the DO PROXY-ARP checkbox.
- Under normal circumstances do not activate the FULL DUPLEX checkbox[13]
- Activate the 802.1p checkbox if the Ethernet packets of the device need to be prioritised in the switch.

DHCP configuration options

As well as the actual IP address assigned, your gateway's DHCP client processes the DHCP options listed in Table 12 DHCP configuration options, provided that they are communicated on granting the DHCP lease.

Options communicated by DHCP always overwrite any parameters that may be defined in the gateway configuration.

[13] This option is only necessary with the IP 400. The IP 3000 and IP 21 handle Full Duplex mode automatically with the switch or hub.

Table 12 DHCP configuration options

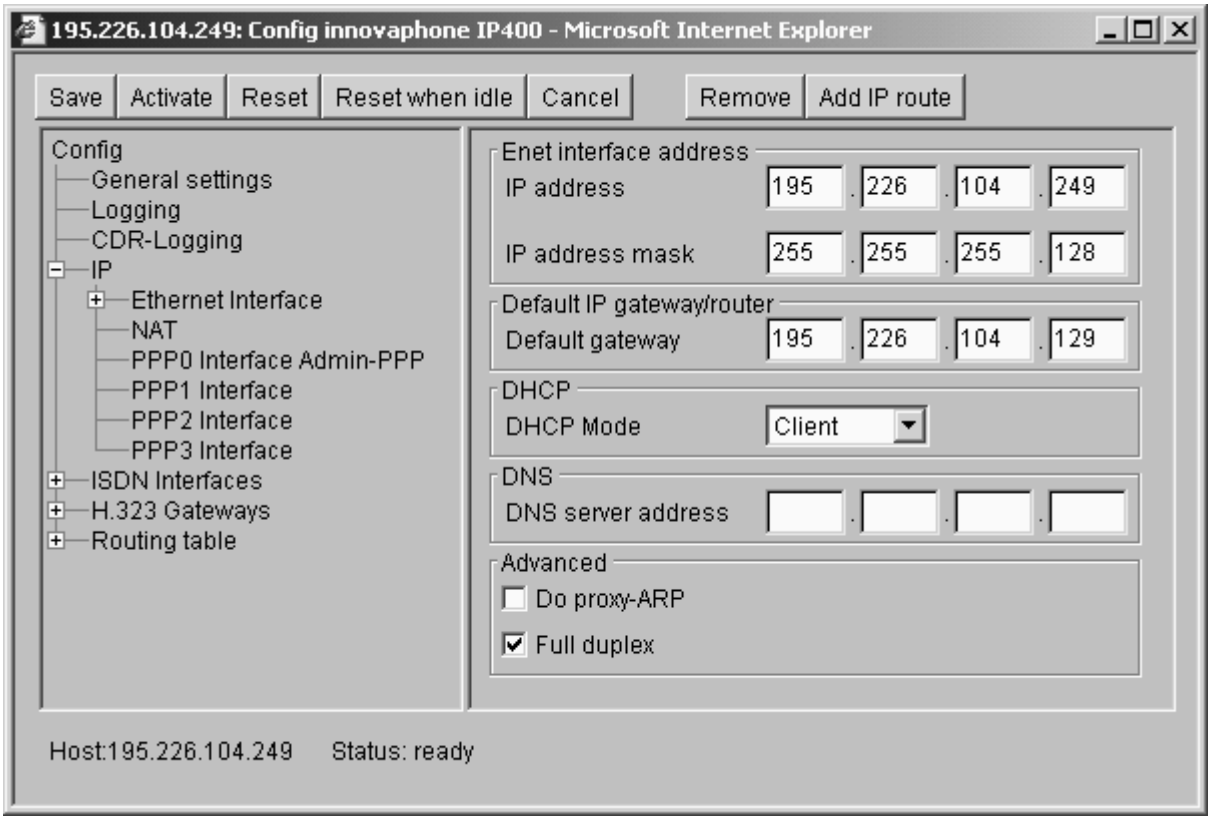
DHCP #	DHCP Name	Configuration parameter overwritten	Description
001	Subnet mask	IP ADDRESS MASK	The registered network mask is used
002	Time offset	OFFSET TO UTC	The offset to UTC in seconds
003	Routers	DEFAULT GATEWAY	From the list of registered routers, the first entry is used as IP standard gateway
006	Domain name servers	DNS SERVER ADDRESS	From the list of registered DNS servers, the first two entries are used as DNS servers
042	NTP servers	SNTP SERVER IP ADDRESS	From the list of registered NTP servers, the first entry is used as NTP server

Full duplex Ethernet

The IP 400's Ethernet controller can be set into the full duplex mode. In the normal case, the IP 400 is operated in the half-duplex mode.

The IP 3000 and IP 21 negotiate the operating mode and so do not have to be configured specifically.

Figure 16 Setting up Ethernet full duplex mode (IP 400)



For full duplex operation:

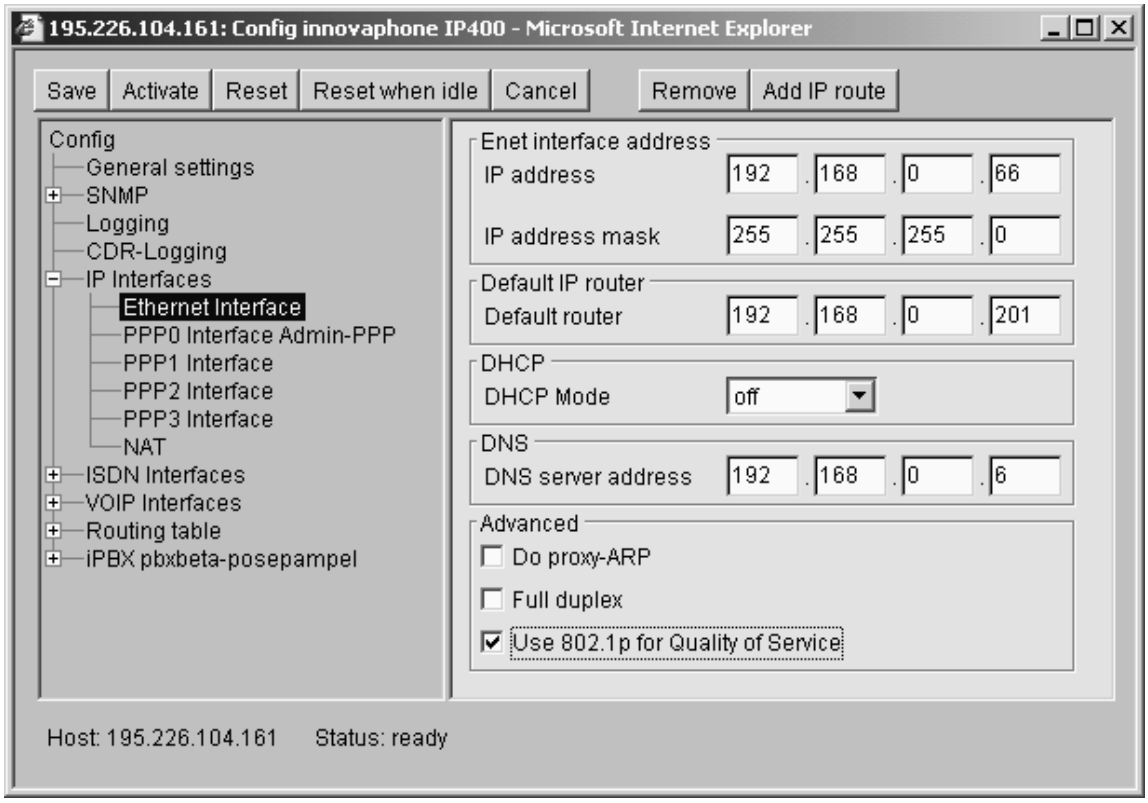
- ▲ Mark the FULL DUPLEX checkbox on the Ethernet Interface form
- ▲ Adjust your Ethernet switch so as to always run in full duplex mode for the port to which the IP 400 is connected. This is necessary since the operating mode of the IP 400 is not negotiated. If the IP 400 and the Ethernet switch settings do not coincide, malfunctions will occur.

Prioritisation on the Ethernet

The Ethernet packets sent in the device may be prioritised at level 2 in the switch. For this, the packets must be correspondingly tagged for transmission. This function must be supported by the switch used.

- ▲ To tag the sent packets with VLAN ID 0 and Priority 7, check USE 802.1P FOR QUALITY OF SERVICE in the ETHERNET INTERFACE form.

Figure 17 Setting up Ethernet for IEEE 802.1p



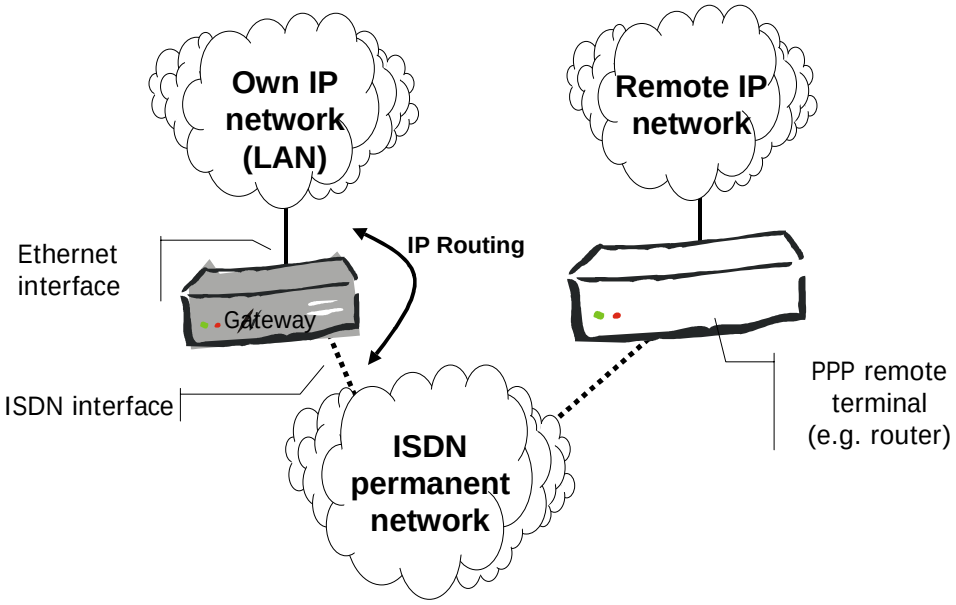
Configuring the WAN interfaces

Your gateway can also be used as an ISDN- or PPPoE[14]- router. In this case it takes over transportation of TCP/IP data between your local network and the WAN connection, regardless of whether voice or other data is being dealt with.

The devices offer various possibilities for routing in the WAN. The use of ISDN for the WAN interface requires a special additional module for the IP 3000. For the IP 400, this possibility is supplied as standard. The IP 3000, IP 400, and the IP 21 all support PPPoE for the WAN interface.

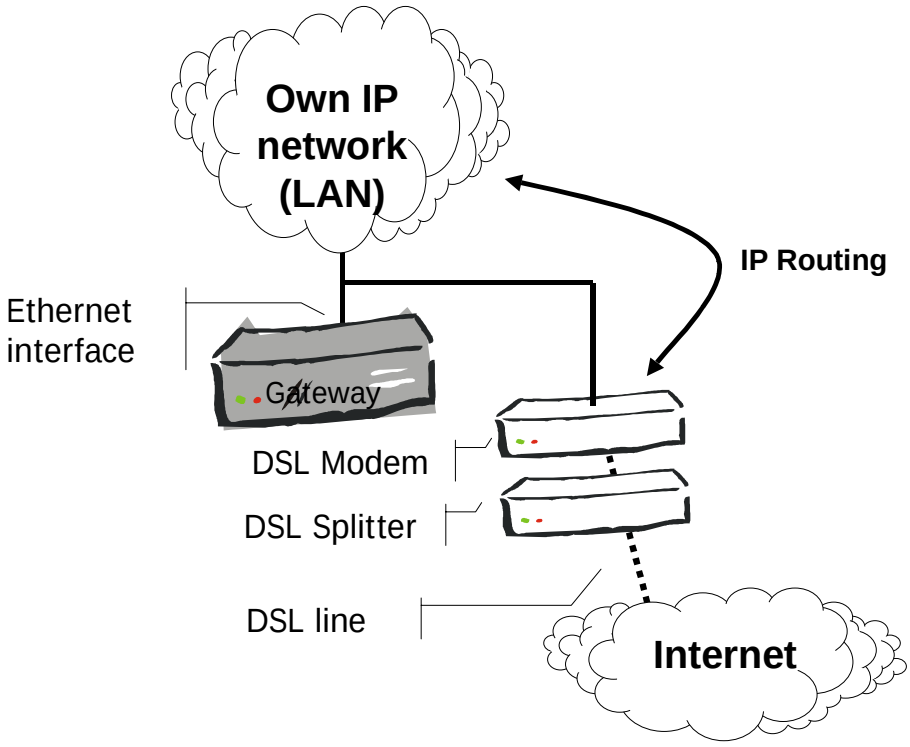
[14] PPPoE ::= PPP via Ethernet

Figure 18 Use of the gateway as an ISDN router



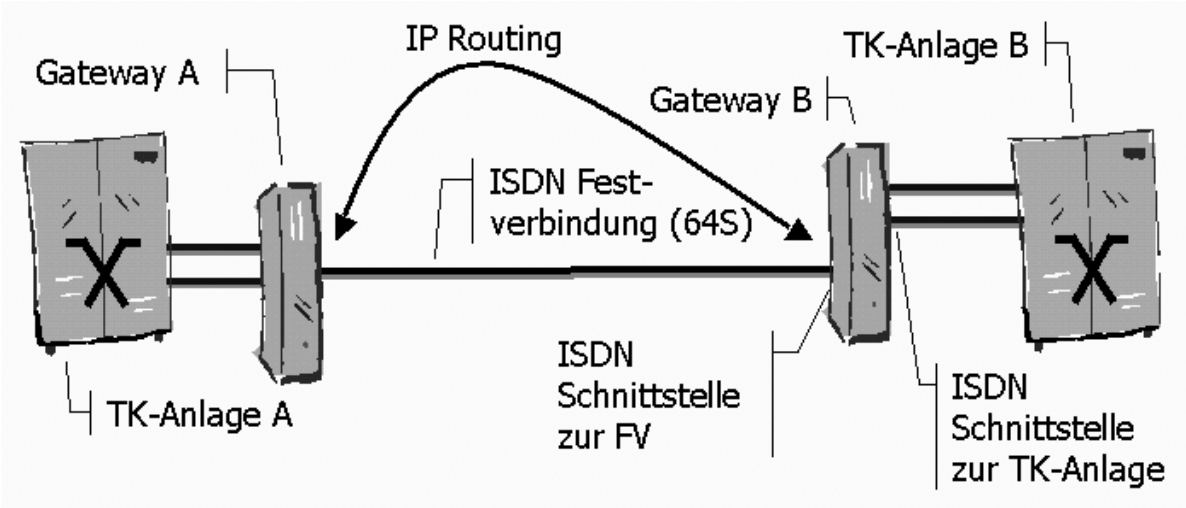
Any ISDN- or PPPoE router with PPP capability may be used as PPP remote terminal. Figure 18 illustrates access to a remote IP network with an IP 400 as ISDN router. Figure 19 Connection to a DSL line via PPPoE illustrates access to the Internet via a DSL connection

Figure 19 Connection to a DSL line via PPPoE



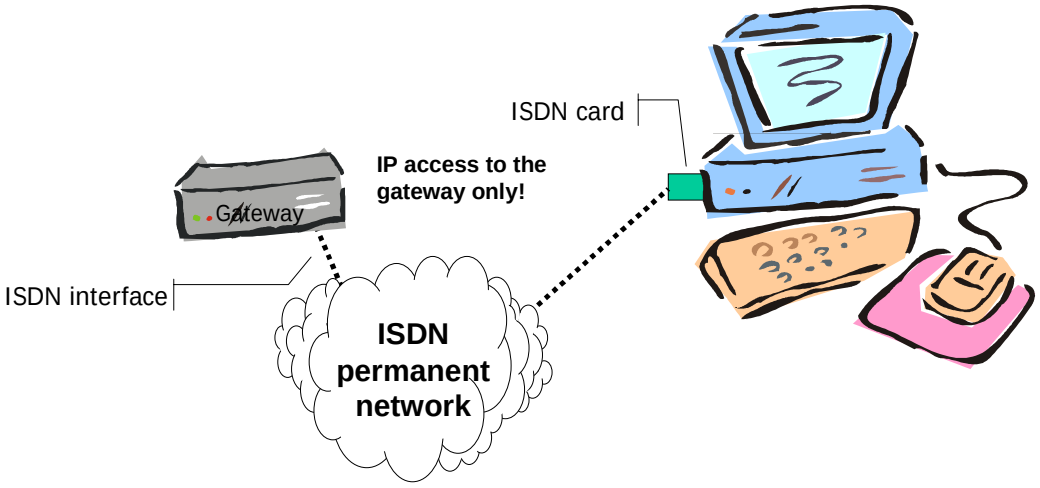
The connection can also be set up directly between two gateways. For example, in the course of a PABX link-up between two locations via an ISDN permanent connection. Figure 20 Gateway hook-up with ISDN permanent connection shows a configuration of this kind.

Figure 20 Gateway hook-up with ISDN permanent connection



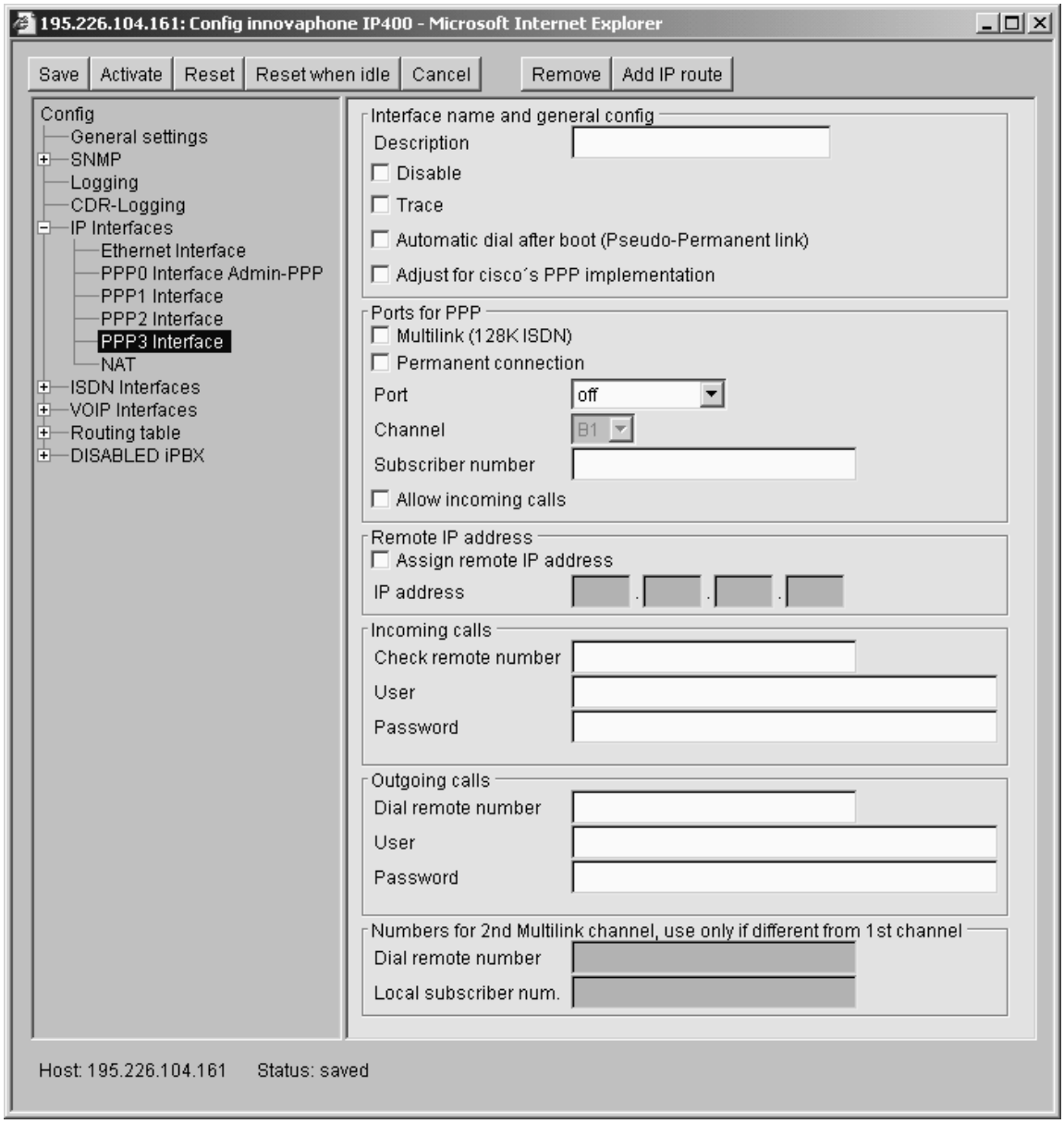
One specific application of the ISDN WAN interface is dial-in to the gateway for maintenance purposes. This allows assured remote maintenance of the gateway without having to set the precondition of access to the local IP network, as Figure 21 Remote maintenance access via ISDN illustrates.

Figure 21 Remote maintenance access via ISDN



To configure the IP routing you define so-called logical PPP INTERFACES in the IP area of the configuration applet.

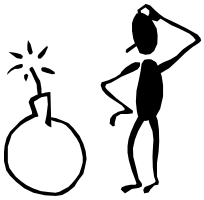
Figure 22 Configuration of logical PPP interfaces



General considerations for configuring the PPP connections

Connection set-up

Normally when dialup lines[15] are used, the gateways do not automatically set up any connections. Thus PPP connections are established only when an incoming data call is received for a configured PPP interface or the connection set-up is explicitly initiated in the IP INTERFACES area via the administration interface. As a result, full control is maintained over cost-generating data connections and, in particular, events in the local network cannot give rise to any undesired connection set-up (no dial on demand).



In some cases though, it may be that a dial-up line kept permanently open is wanted. This achieved through the setting AUTOMATIC DIAL AFTER BOOT. This causes the corresponding PPP connection to be set up and then always kept open immediately after starting the gateway. Exercise the appropriate caution in the use of this setting.

Figure 23 Connection control in the administration interface

The CONNECT link initiates set-up of the chosen connection. The CLEAR link, by contrast, initiates cleardown of the connection.

[15] A PPoE connection is then treated as a dial-up line

Channel bundling (multi link)

The gateways support channel bundling on 2 ISDN B channels (128 kbps).

Addressing of WAN interfaces

Normally, a router's WAN interfaces are assigned their own IP addresses (normally from a special transfer network). This is not necessary with the gateways and thus they do not require any particular IP addresses apart from those of their own IP network.

Compression of voice data on the PPP link

The gateways support the compression of voice data over the PPP link using the RTP Header Compression[16] method. This drastically reduces the required bandwidth for VoIP calls.

If the PPP remote terminal used is not an innovaphone® gateway, compatibility problems may arise in practice. If a Cisco router is used at the opposite end and problems arise in the transmission of voice data, try the option ADJUST FOR CISCO'S PPP IMPLEMENTATION.

Configuring the IP routes

For every PPP interface you can add separate IP routes with the ADD IP ROUTE interface. Configuring is done in the same way as with the routes for the Ethernet interface (refer to page 47). All IP routes must be defined explicitly. No data will be routed via a PPP interface for which no IP routes are defined.

Please remember though, that the configured IP routes are static routes, which are always active. This is still the case even if the corresponding PPP interface is not connected. IP routes superimposed on one another on different PPP interfaces (several Default Routes for example) are thus not possible.

[16] Conformant to RFC 2508 / 2509

Settings for outgoing ISDN PPP switched connections

The following steps are used to configure your gateway for an outgoing PPP data circuit.

- ▲ Uncheck the AUTOMATIC DIAL AFTER BOOT checkbox
- ▲ Uncheck the MULTILINK checkbox
- ▲ Uncheck the PERMANENT CONNECTION checkbox
- ▲ In the PORT selection field, choose the ISDN interface(s) on which you want to put the outgoing call into operation
- ▲ The CHANNEL selection field is significant for permanent connections only and thus is not alterable here
- ▲ In the SUBSCRIBER NUMBER field, enter the calling MSN to be used for the call. Generally speaking this may also be left blank
- ▲ Uncheck the ALLOW INCOMING CALLS checkbox
- ▲ Uncheck the ASSIGN REMOTE IP ADDRESS[17] checkbox
- ▲ Leave the CHECK REMOTE NUMBER field blank
- ▲ If the called PPP remote terminal is itself do provide authentication at your gateway, enter the appropriate data in the USER and PASSWORD fields in the INCOMING CALLS area
- ▲ Enter the call number of the PPP remote terminal to be called in the DIAL REMOTE NUMBER field
- ▲ If your gateway is to provide authentication at the called PPP remote terminal, enter the appropriate data in the USER and PASSWORD fields in the OUTGOING CALLS area
- ▲ Configure the IP routes, as described under "Configuring the IP routes" from page 57 onwards

Expansion to Multilink

In place of a connection via a B channel, you can also configure a multilink connection via 2 bundled channels.

[17] Through this the called end is not assigned any IP address during the PPP connection set-up. This is not usual with outgoing calls.

- ▲ Mark the MULTILINK checkbox
- ▲ If a different call number must be used for the second channel of the PPP remote terminal to be called, enter this in the DIAL REMOTE NUMBER field in the NUMBERS FOR 2ND MULTILINK CHANNEL area. Leave this field blank if the same call number can be used as for the first channel
- ▲ Enter the outgoing number to be used for the second channel in the LOCAL SUBSCRIBER NUMBER field. Generally speaking this may also be left blank

Settings for incoming ISDN PPP switched connections

With the following you configure your gateway for an incoming PPP data circuit.

- ▲ Uncheck the AUTOMATIC DIAL AFTER BOOT checkbox
- ▲ Uncheck the MULTILINK checkbox
- ▲ Uncheck the PERMANENT CONNECTION checkbox
- ▲ In the PORT selection field, choose the ISDN interface(s) on which you want to accept the incoming call
- ▲ The CHANNEL selection field is significant for permanent connections only and thus is not alterable here
- ▲ Enter the call number into the SUBSCRIBER NUMBER field under which incoming calls are to be accepted. This should not be left blank[18]
- ▲ Mark the ALLOW INCOMING CALLS checkbox
- ▲ Uncheck the ASSIGN REMOTE IP ADDRESS[19] checkbox if the calling PPP remote terminal has a permanent IP address. Check this checkbox if the device in question at the calling PPP remote terminal is a device that requires a dynamically assigned IP address. This is the case, for example, with a Windows™ PC that dials in to a gateway via the remote data transmission network. In this case enter the IP address that is to be assigned in field IP ADDRESS and add to the PPP interface an IP route at precisely this IP address (see "Configuring the IP routes" above)

---

[18] If this field is left blank, all data calls will be accepted on the chosen ISDN interfaces. However in this case it is not possible to assign these calls to the various PPP interfaces. Such kinds of configuration should therefore be avoided.

[19] Through this the called end is not assigned any IP address during the PPP connection set-up. This is not usual with outgoing calls.

- If the dial-in is to be restricted to a single PPP remote terminal, enter its call number in the CHECK REMOTE NUMBER field. The end of the calling party's calling number is compared against the contents of this field and must match, otherwise the call is not accepted. If, for example, the number 7031730090 is recorded there, calls will be accepted from 07031730090 as well as from 004907031730090
- If the calling PPP remote terminal is to provide authentication at your gateway, enter the appropriate data in the USER and PASSWORD fields in the INCOMING CALLS area
- Leave the DIAL REMOTE NUMBER field blank
- If your gateway is to provide authentication at the calling PPP remote terminal, enter the appropriate data in the USER and PASSWORD fields in the OUTGOING CALLS area
- Configure the IP routers as described under "Configuring the IP routes" from page 57 onwards

Expansion to Multilink

In place of a connection via a B channel, you can also accept a multilink connection via 2 bundled channels.

- Mark the MULTILINK checkbox
- Leave blank the DIAL REMOTE NUMBER and LOCAL SUBSCRIBER NUMBER fields in the NUMBERS FOR 2ND MULTILINK CHANNEL area. Your gateway accepts the calls for both channels on the same number configured in the SUBSCRIBER NUMBER field

Settings for incoming and outgoing ISDN PPP switched connections

You can also configure a PPP interface for incoming and outgoing calls. as desired. For this combine the previously described settings for incoming and outgoing calls.

Specific points with WAN connection via Ethernet (PPPoE)

Operation of the WAN connection via PPPoE, for example on a DSL modem, is very straightforward. Bear in mind though, that outgoing calls only are possible in this mode.

The PPPoE connection – i.e. the DSL modem, for example – must be attached to the same Ethernet segment (or –switch) as the gateway.

PPPoE connections are basically switched connections, like ISDN connections are too. However, various providers offer so-called flat-rates, in which the charges that are incurred are independent of the call duration. In such cases it is possible and advisable to keep the PPPoE connection open permanently.

- Mark the AUTOMATIC DIAL AFTER BOOT checkbox, if you want to keep the PPPoE connection permanently open. Otherwise, or if you are uncertain about the costs that may be incurred, uncheck this box
- Uncheck the MULTILINK checkbox
- Uncheck the PERMANENT CONNECTION checkbox
- In the PORT selection field, choose the setting PPPOE
- The CHANNEL selection field is significant for ISDN permanent connections only and thus is not alterable here
- Leave the SUBSCRIBER NUMBER field blank since it has no significance
- Only outgoing PPPoE connections are possible so uncheck the ALLOW INCOMING CALLS checkbox
- Uncheck the ASSIGN REMOTE IP ADDRESS[20] checkbox
- Leave the CHECK REMOTE NUMBER field blank since it has no significance
- Leave the USER and PASSWORD fields blank in INCOMING CALLS area, they have no significance
- Leave the DIAL REMOTE NUMBER field blank, it has no significance
- If your gateway is to provide authentication at the called PPP remote terminal, enter the appropriate data in the USER and PASSWORD fields in the OUTGOING CALLS area

[20] Through this the called end is not assigned any IP address during the PPP connection set-up. This is not usual with outgoing calls.

▲ Configure the IP routes, as described under "Configuring the IP routes" from page 57 onwards

Remote maintenance facility in the standard configuration

In the standard configuration, the PPP ISDN interface is configured for dial-up for remote maintenance purposes. This allows the gateway to be configured remotely from any PC with an ISDN card and a PPP communications programme (e.g. "Networking Communications" in Windows 98™).

The settings for this access are configured in the logical interface PPP0.

▲ Calls are accepted on the PPP interface (ISDN PORT is PPP, ALLOW INCOMING CALLS checkbox is ticked)

▲ Calls are accepted on every MSN (SUBSCRIBER NUMBER is blank)

▲ An IP address (192.168.0.253) is allocated to the calling end (the ASSIGN REMOTE IP ADDRESS checkbox is ticked).

▲ Calls are accepted from all remote terminals (CHECK REMOTE NUMBER is blank).

▲ As USER and PASSWORD, admin and ip21/ip400/ip3000[21] are used.

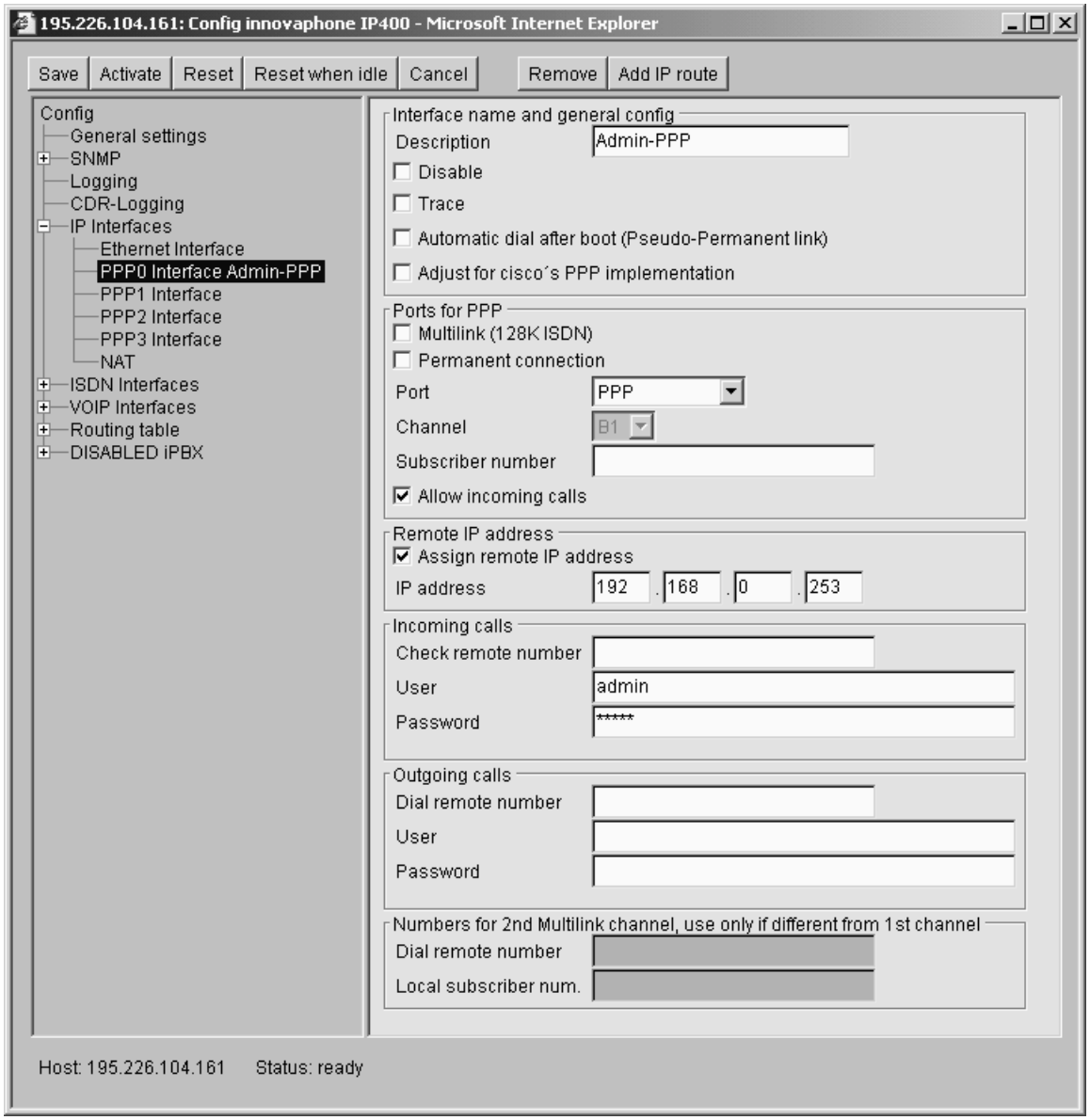
▲ A backward authentication does not take place (the fields under OUTGOING CALLS are blank).

▲ The called gateway receives the IP address 192.168.0.254.[22]

[21] According to the device

[22] In normal circumstances this IP address should not overlap with the address of a device on the LAN. However if, by way of exception, a device is present on the network with the IP address `192.168.0.254`, then the IP 400 itself will not be able to communicate with this device. This address is permanently programmed into the gateway. This ensures that a gateway can always be accessed under this IP address via the remote maintenance facility, regardless of the particular IP address that is set on the Ethernet interface of the gateway.

Figure 24 Remote maintenance access via the PPP interface



With this configuration an ISDN BRI bus[23] can be plugged into the PPP interface allowing the gateway to be configured from any PC with a PPP dial-up application.

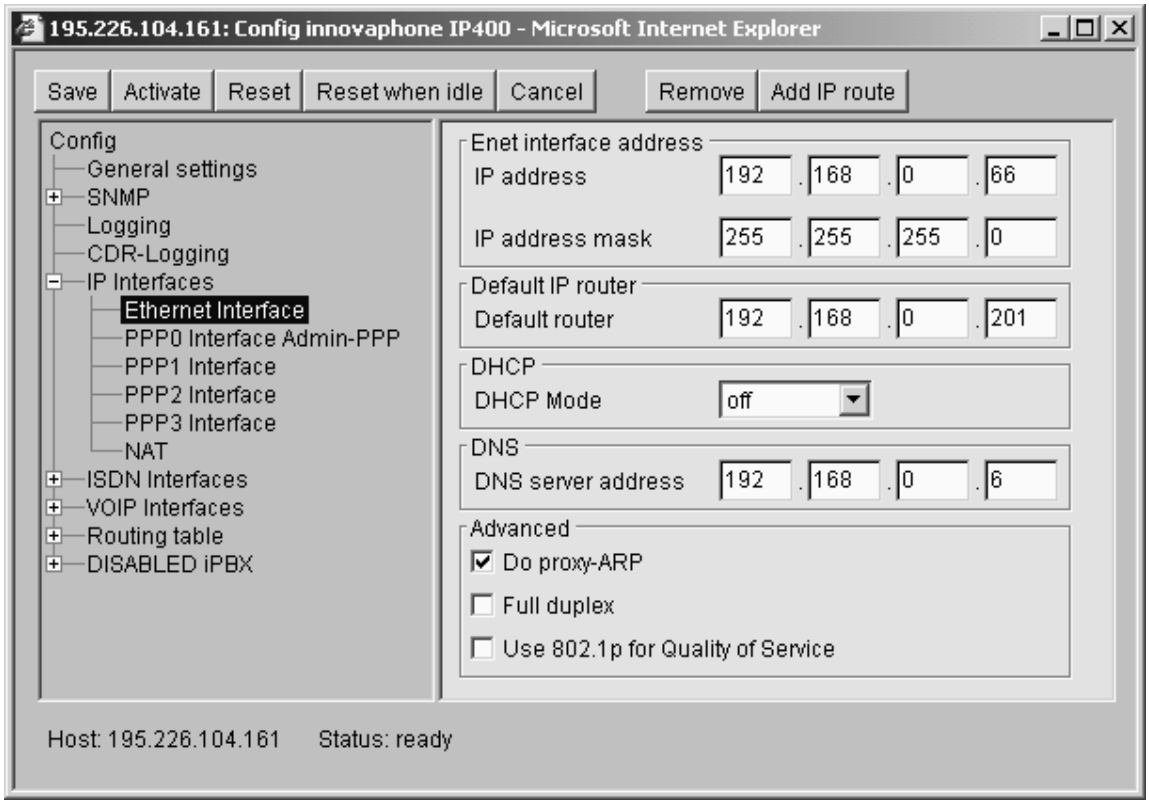
Of course, this configuration can be adapted to the local circumstances. For this refer to the advice in "Settings for incoming ISDN PPP switched connections" from page 59 onwards.

[23] For example, a BRI trunk line or a BRI subscriber line of a PABX.

Permit dial-up access to the entire network

For IP packets which have to be routed by Ethernet via the gateway to logical PPP interfaces, the gateway is able to appear to the local network as if it were the addressed terminal itself. This also allows IP terminals on the same Ethernet segment, without a correct routing setting, to communicate beyond the gateway and make use of the WAN connection. This function called proxy arp is activated by ticking the DO PROXY-ARP checkbox in the ETHERNET INTERFACE area of the configuration applet.

Figure 25 Activation of proxy arp



For this purpose, the remote terminal linked through ISDN has to be assigned an IP address from the same subnet as that from which the IP address of the gateway originates. This is done through an appropriate entry in the REMOTE IP ADDRESS area and ticking the ASSIGN REMOTE IP ADDRESS checkbox.

It is essential to remember though, that the entire home network then becomes accessible to the dial-up end, which may present a security problem in certain circumstances.

Configuration of the ISDN and Analogue interfaces

The IP 21 has analogue interfaces. For the configuration of these interfaces, refer to page 87 onwards.

All three gateway types have two “virtual” interfaces, whose configuration is described on page 97 onwards.

IP 400 and IP 3000 have ISDN interfaces. To configure the ISDN interfaces you first need to be aware of the following points:

- Which devices you want to link to the gateway via ISDN. These may be telephones, (IP 400 (ISDN) and IP 21 (analogue) only), PABXs, network terminations of your ISDN network provider or other ISDN terminals
- Whether the ISDN lines are to be used exclusively for voice connections, or whether an ISDN/PPP link for the data routing is also to be implemented via one of them.

Configuration is done in the "ISDN Interfaces" area of the configuration applet.

ISDN interfaces of IP 400

The IP 400 comes equipped with 3 ISDN BRI interfaces, denoted PPP , TEL1 and TEL2 (see page 19). Choice of connection is:

- TEL1 and TEL2 can be used to connect a trunk line, one or two[24] telephone lines or a PABX.
- PPP may be used solely to connect a PABX.

All three interfaces can be used to set up ISDN data lines (PPP). This is the case both as permanent connections and as dial connections.

[24] Technically, up to eight terminals can be connected to an ISDN interface. It is to be noted, however, that from all these devices only 2 calls can be carried out simultaneously. It must further be ensured that the power consumption of all terminals together does not exceed the permitted value of 4 watts.

ISDN interfaces of IP 3000

The IP 3000 comes equipped with 2 ISDN PRI and one BRI interface, denoted PRI1 , PRI2 and S/T (see page 15).

- PRI1 is a primary multiplex (PRI) interface in TE mode, i.e. for connection of a trunk line.
- PRI2 is a primary multiplex (PRI) interface in NT mode, i.e. itself acts like a trunk line and is used to connect a PABX or a terminal intended for operation on an exchange line.

  PRI1 and PRI2 are short-circuited in the quiescent state and intended for looping the gateway into an existing trunk line.
- S/T[25] is a BRI interface in TE mode and can be used solely for connecting a trunk line.

... for experts

BRI

- TEL1 and TEL2 can be operated in the TE and NT modes with and without feeding and termination
- PPP and S/T can be operated in the TE mode only
- TEL1, TEL2, PPP and S/T can be operated in point to point and point to multipoint mode
- TEL1, TEL2, PPP and S/T can be operated in DSS1 and QSIG signalling mode (mixed as well)
- NT (LINE EMULATION) switches on the NT mode for layers 1, 2 and 3.
- POWER switches on the power supply for terminals on the bus (in NT mode only, maximum 4W)
- 100 OHM TERMINATION switches on the bus terminations
- PERMANENT ACTIVATION (in TE mode only) activates the line permanently (clock)
- POINT TO POINT switches on the point to point mode

[25] The S/T interface is erroneously referred to as TEL in the configuration applet.

PRI

- PRI1 is always in the TE mode
- PRI2 is always in the NT mode
- CONNECT PRI1 AND PRI2 WITH RELAY switches through the two PRI interfaces electrically, as with the gateway switched off
- NO CRC4 switches off the generation of CRC4 checksums
- ASSIGN OUTGOING CHANNELS FROM TOP assigns the B channels downwards from the top (starting at 30 down to 1), otherwise starting at the bottom upwards, recommended if the interface is operated in TE mode

PRI and BRI

- DISABLE OVERLAP RECEIVE suppresses a SETUP_ACK on incoming overlapped dialling on a point to multipoint connection in the TE mode
- SUPPRESS SENDING OF HLC suppresses the sending out of high layer compatibility information elements on the interface
- SUPPRESS SENDING OF FTY suppresses the sending out of facility information elements on the interface
- PROVIDE INBAND PROGRESS TONES (in the TE mode only) forces the generation of tones (dial tone, calling tone, busy tone) in the TE mode as well (always occurs in NT mode)
- GENERATE CONNECTED TIME inserts the local gateway time into every outgoing CONNECT message
- The D-CHANNEL PROTOCOL meanings: EDSS1 = Euro-ISDN, QSIG = ECMA QSIG (CR len=1, channel id accord. to basic rate), QSIG-PRI-ECMA1 = ECMA QSIG (CR len=2, channel id accord. to primary rate, B channels 1 to 30), QSIG-PRI-ECMA2 = ECMA QSIG (CR len=2, channel id accord. to primary rate, B channels 1 to 15 and 17 to 31)
- The DIALTONE TYPE meaning (in NT mode or with PROVIDE INBAND PROGRESS TONES): GERMAN PBX = like German PABX, GERMAN = like German trunk, US = American dial tone, UK = British dial tone
- With ADD CGPN MAP, replacements for calling numbers (CLI) can be effected that apply for this interface only (separated according to incoming/outgoing calls)
- With ADD CDPN MAP, replacements for called numbers can be effected that apply for this interface only (separated according to incoming/outgoing calls)

Figure 26 Configuration of a BRI ISDN interface

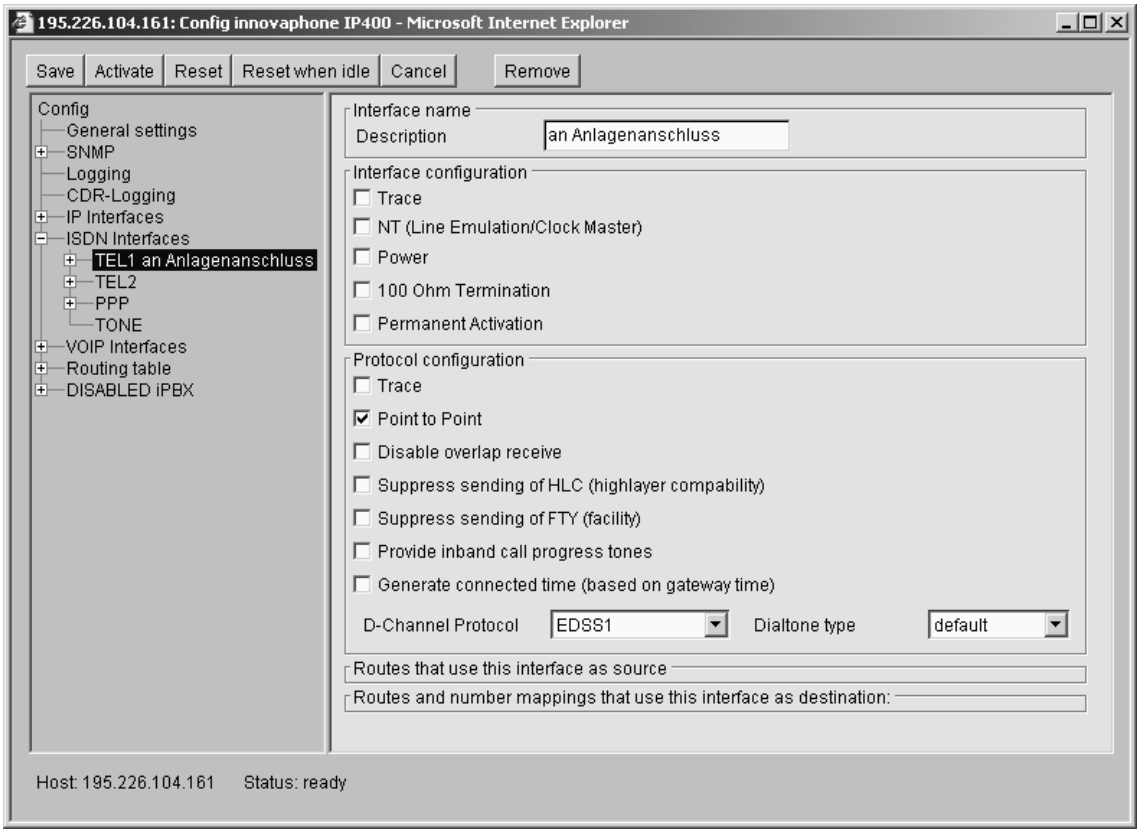
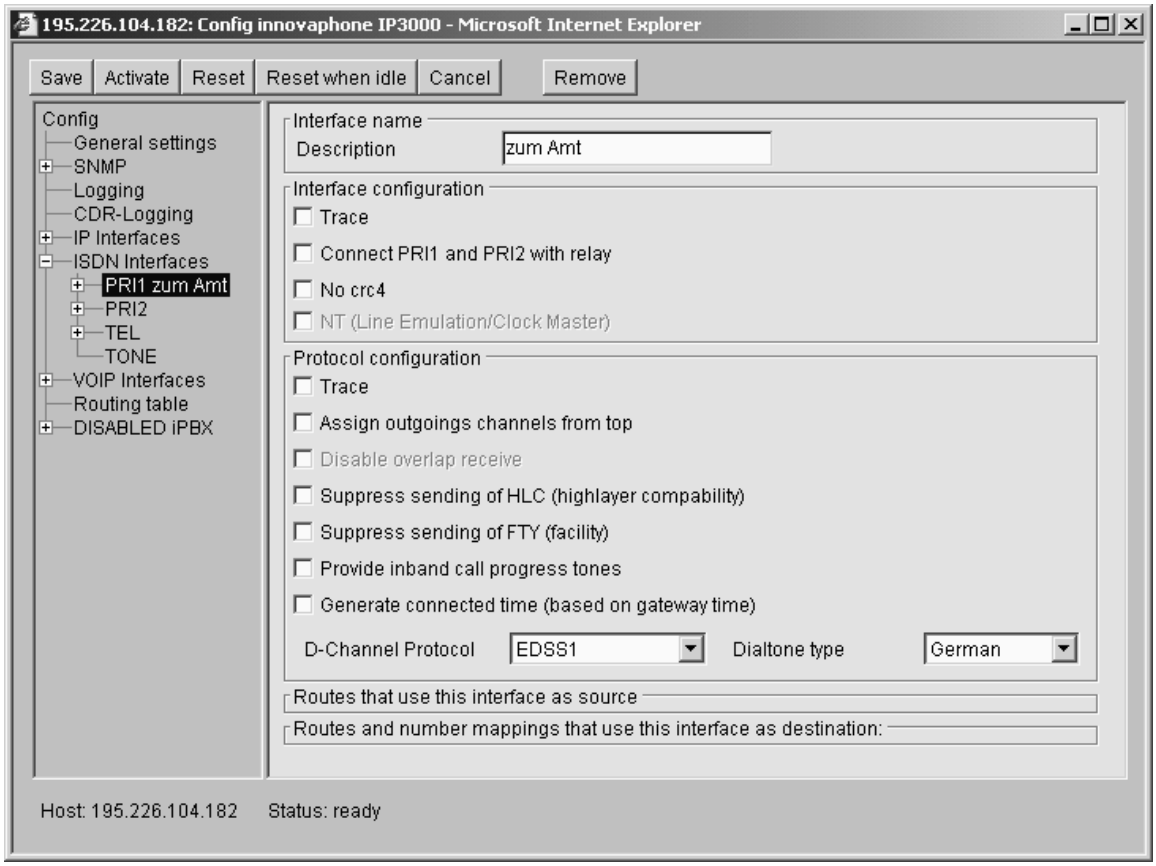


Figure 27 Configuration of a PRI ISDN interface



With the REMOVE button you can delete all the settings for the chosen interface.

Considerations for configuring the ISDN interfaces

The TE- and NT modes

The interfaces TEL1 and TEL2 can be operated in the TE or NT mode, as desired. PRI1, PRI2, PPP and S/T are defined in the mode.

The TE (terminal equipment) mode means here that the interface acts like a normal ISDN terminal. This means that:

- Layers 2 and 3 of the ISDN protocol are configured as terminals

- The service lines are correspondingly seized
- The gateway synchronises itself to the network clock (clock slave)

The NT (network termination) mode on the other hand means that the interface acts like an ISDN network termination (NTBA). This means that:

- Layers 2 and 3 of the ISDN protocol are configured as a network
- The services lines are correspondingly seized transposed
- The gateway provides the clock (clock master)

The signalling protocols

The gateways support basically two different D channel protocols on the ISDN interfaces: Euro-ISDN (EDSS1) and QSIG.

Euro-ISDN is the form of signalling that has gained acceptance worldwide for ISDN subscriber line interfaces and, despite the name, is commonly found outside of Europe. The chief exception to this at the moment is the United states where other digital signalling methods are generally used.

QSIG is a standardised signalling protocol that is mainly used for the networking of PABXs. Here, basic call and tunnelling are supported by the gateways. This particularly allows homogenous PABX link-ups to be implemented with QSIG, in which manufacturer-specific properties are exchanged through QSIG.

Unfortunately, there are several variants of the QSIG standard and various implementations that are conformant to a greater or lesser extent. The gateways therefore support 3 different variants that differ with regard to

▲ the length of the call reference,

▲ the coding of the channel id and

▲ Numbering of the B channels

The following table shows the differences.

Table 13 Difference between the QSIG variants

Variant	Call reference length	Channel id coding	Numbering of the B channels	Usage
QSIG	1 Byte	As for basic rate		BRI[26]

[26] If the setting QSIG for PRI1 or PRI2 is used, it acts in the same way as with the setting QSIG-ECMA1

Variant	Call reference length	Channel id coding	Numbering of the B channels	Usage
QSIG-PRI-ECMA1	2 Bytes	As for primary rate	1 to 30	BRI, PRI
QSIG-PRI-ECMA2	2 Bytes	As for primary rate	1 to 15, 17 to 31	PRI[27]

The assignment of B channel numbers with PRI connections

Although a mechanism is defined in ISDN to determine how incoming and outgoing calls of different B channels get assigned concurrently, every now and then collisions occur on PRI (PRI) connections. With outgoing calls the gateways normally assign the B channels starting at the bottom (i.e. 1, 2, ...). If this results in collisions, allocation must be altered so that the B channels are assigned starting at the top (i.e. 30, 29, ...). This is done through the setting ASSIGN OUTGOING CHANNELS FROM TOP.

If you are uncertain as to which assignment mechanism is the right one, select "from top" for PRI1 and "from bottom" for PRI2.

Overlapped dialling on terminals on point to multipoint connection

Normally, terminals (i.e. devices in the TE mode) on a point to multipoint connection are not called with overlapped dialling (overlapped sending). In some circumstances though, the gateways can be connected to a PABX in precisely this mode and then also support the incoming overlapped dialling (overlapped receive). Here, conformant to the standard, an incoming SETUP message is answered with a SETUP_ACK message. Many PABXs, however, do not expect any such message from a terminal and abort the call at this point. In such a case, the DISABLE OVERLAP RECEIVE setting can be used to cause the gateway not to answer the incoming SETUP message with a SETUP_ACK.

[27] If the setting QSIG-PRI-ECMA2 for TEL1, TEL2, PPP or S/T is used, it acts in the same way as with the setting QSIG-ECMA1

Suppression of certain protocol elements

Not all ISDN implementations are able to cater for reception of certain standard-conformant information elements (so-called IEs). Such IEs may arise, for example, in the linking-up of different PABXs or in the transmission of H.323 calls to an ISDN interface and vice-versa.

If malfunctioning occurs as a result of the transmission of certain IEs, the gateways can be caused to remove such IEs from the transmitted messages.

Table 14 Suppression of the transmission of information elements

Setting	Effect
SUPPRESS SENDING OF HLC	No high layer compatibility information elements are transmitted
SUPPRESS SENDING OF FTY	No facility information elements are transmitted

Dial tones

The gateways are able to generate dial tones on the ISDN interfaces (free-line signal, ringing signal, busy signal).

This is always done for outgoing calls from the gateway in the direction of the calling party if the called end does not generate any dial tones of its own[28].

For incoming calls on the ISDN interface, this is normally done in the direction of the calling party only if the interface is in the NT mode, not though in the TE mode. In a few cases though, particularly with the link-up of PABXs via tie lines, it can be useful to also generate these tones in the TE mode. This can be achieved with the PROVIDE INBAND CALL PROGRESS TONES setting.

Generation of timestamps during connection set-up

The ISDN network normally generates a timestamp in the CONNECT message. This is used by telephones or PABXs, for example, to set their own clock at the first connection. The gateways normally pass on such timestamps unaltered.

However, what may be wanted is the provision of a consistent timestamp in all CONNECT messages with the current system time of the gateway. This can be achieved through the GENERATE CONNECTED TIME setting. For this, the gateway should always have the correct time at its disposal. Since it does not have its

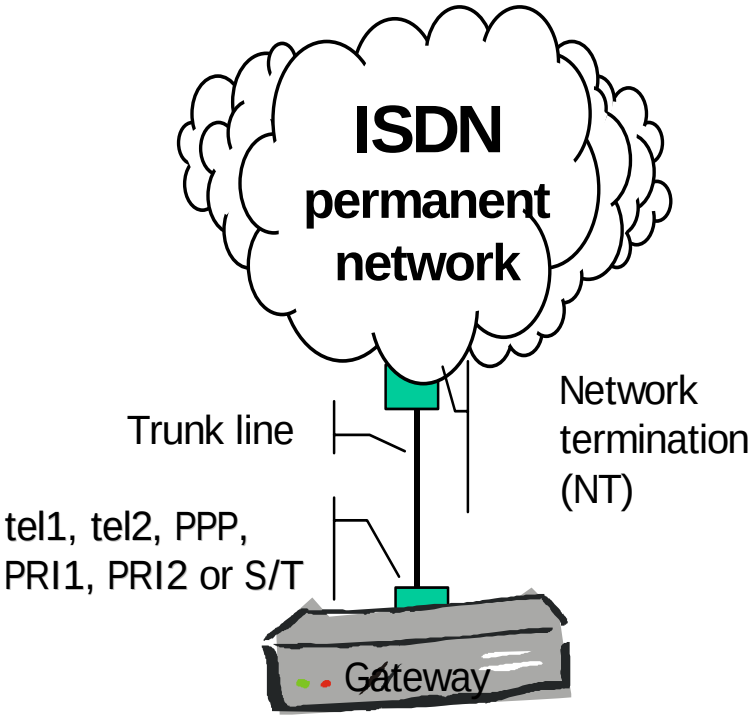
[28] Dial tones are recognised in that an in band information is signalled by the called end.

own real-time clock, an NTP time server should be configured for this (see page 151). This setting is normally meaningful in NT mode only.

Use as connection for a trunk line (dial- or permanent connection)

In this case, the gateway is connected to one of your ISDN network provider's trunk lines. This mode is possible for TEL1, TEL2, PPP, PRI1, and S/T. PRI2 can only be used in NT mode and therefore is not appropriate for this kind of connection.

Figure 28 Gateway connected to a trunk line



There are a number of scenarios in which this usage makes sense:

- Use of the gateway as a gateway for H.323 calls in the permanent network. This allows H.323 terminals to reach standard terminals in the permanent telephone network and vice versa.
- Use as an IP router for manual dial-in to ISP or into the company network. Through this the gateway and connected LAN with its Ethernet line are

connected to the IP (Inter- or Intra-) network. A separate IP router is no longer needed.

- Use as an IP router for operation on a permanent connection (IP 400 only). Through this the gateway is connected up via a 64kbps or 128kbps ISDN permanent connection to a PPP remote terminal (at the ISP or in the company network).

The specific configuration depends on whether the trunk line is configured as a point to point or point to multipoint or as a permanent connection. PRI ISDN interfaces are always operated in point to point mode.

Furthermore, the type of signalling for dial connections must be set up correctly. For trunk lines the signalling is always EDSS1, while for PABX connections the relevant choice may also be a variant of QSIG (refer to the "The signalling protocols" above). For permanent connections the signalling is of no importance.

For PRI interfaces it finally needs to be known whether CRC4 checksums will be generated on this and how the assignment of B channels takes place (see “The assignment of B channel numbers with PRI connections” above).

If you are uncertain about the configuration of your line, consult your network administrator or your ISDN network provider.

- Uncheck the NT checkbox (TEL1, TEL2 and S/T only)
- Uncheck the POWER checkbox (TEL1 and TEL2 only)
- Uncheck the 100 OHM TERMINATION checkbox (TEL1 and TEL2 only)
- Uncheck the PERMANENT ACTIVATION checkbox (TEL1, TEL2, PPP and S/T only)
- If your trunk line is the point-to-point type, check the POINT TO POINT checkbox. However, if it is point to multipoint, uncheck this particular checkbox. With a permanent connection this setting is irrelevant. If the connection is operated in mixed mode, however, (one B channel permanently on one permanent connection, one B channel in dial operation), the setting is dependent on the dialup line's operating mode (TEL1, TEL2, PPP and S/T only)
- Uncheck the CONNECT PRI1 AND PRI2 WITH RELAY checkbox (PRI1 only)
- If CRC4 checksums are generated on the connection, uncheck the NO CRC4 checkbox. Otherwise check the NO CRC4 checkbox. In Germany PRI lines are mostly operated with CRC4 (PRI1 and PRI2 only)
- If the assignment of B channels is to be from the top down, mark the ASSIGN OUTGOING CHANNELS FROM TOP checkbox (PRI1 and PRI2 only)
- Uncheck the DISABLE OVERLAP RECEIVE checkbox
- Uncheck the SUPPRESS SENDING OF HLC and SUPPRESS SENDING OF FTY checkbox (see "Suppression of certain protocol elements" above)

- ▲ Uncheck the PROVIDE INBAND CALL PROGRESS TONES checkbox (see "Dial tones" above)
- ▲ Select the EDSS1 protocol in the D-CHANNEL PROTOCOL selection field (refer to "The signalling protocols" above)
- ▲ The DIALTONE TYPE is of no importance in this configuration
- ▲ The special modification of called party and calling party number is normally not necessary in this configuration. Read up on this in section "Treatment of the various ISDN address types" on page 87.

If the trunk line is connected point to point, aside from the gateway no further ISDN device may be connected there.

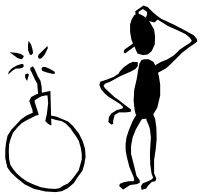
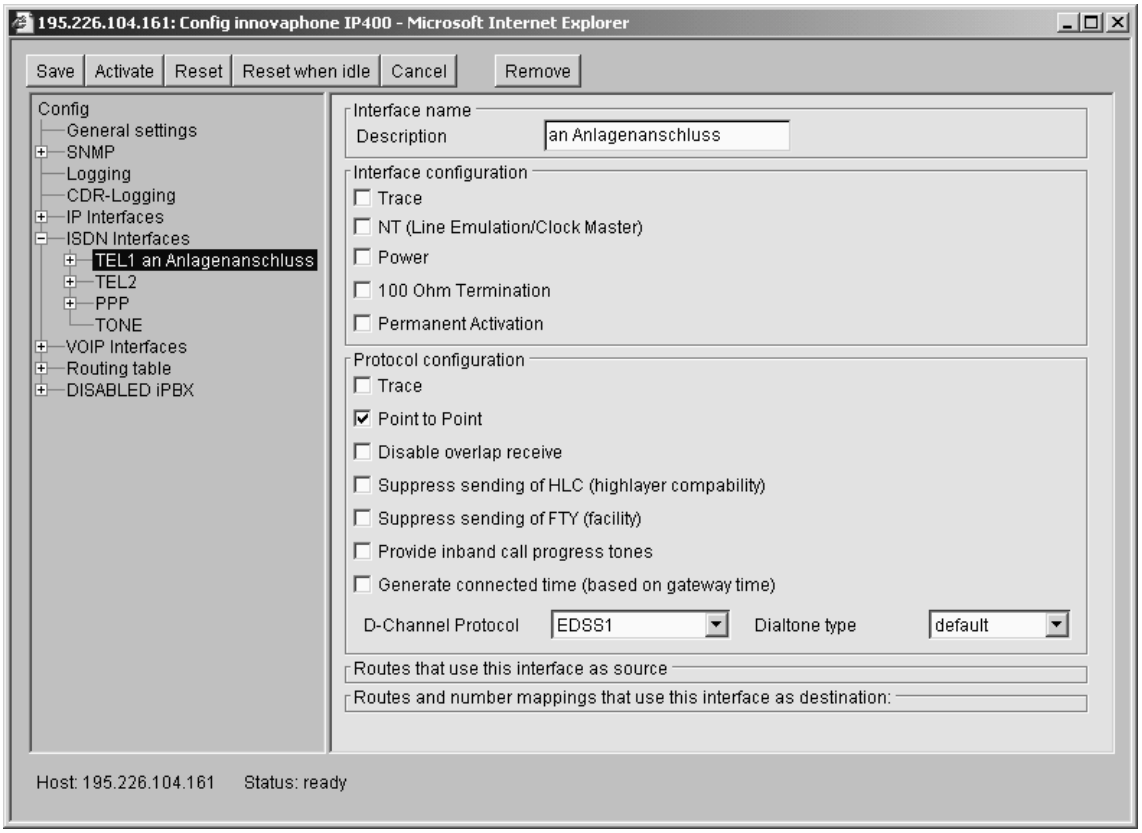


Figure 29 Configuration of TEL1 on trunk line (point to point)



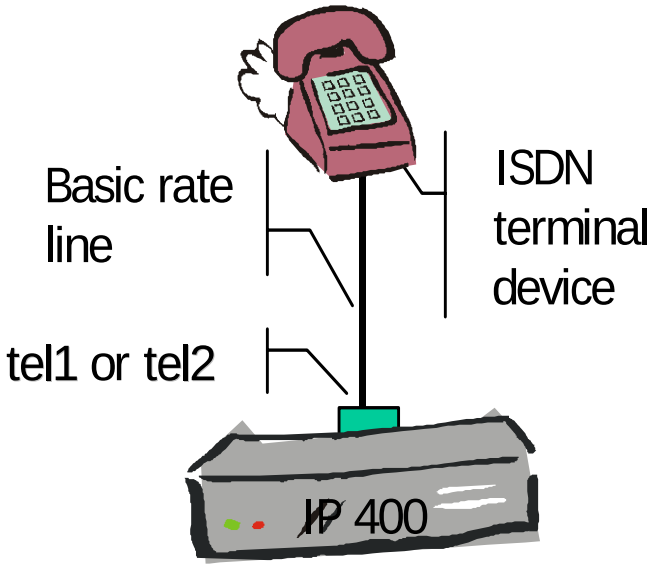
If it is a point to multipoint connection, further ISDN terminals can then be attached there. However, take into consideration that, incoming calls can then be accepted by all terminals connected. Read up in section "Configuring the call routing" on page 124, as to how the gateway can be configured to allow only calls for the desired telephone numbers to be accepted.

For configuration of the IP routing via the ISDN interface in the event of use as an IP router please refer to the section "Configuring the WAN interfaces" starting page 51.

Use for connecting a telephone or other ISDN terminal equipment

In this case, one or more ISDN terminal devices are connected to the interface. To the device it then acts like a point to multipoint connection of your network provider. This mode is available only for the TEL1 and TEL2 interface[29].

Figure 30 ISDN device connected to the IP 400



The specific configuration depends on whether the devices attached have their own power supply or not. Telephones typically have no power supply of their own and are therefore fed from the ISDN line.

If you are uncertain whether your devices require power feeding or not, simply enable the power feeding feature anyway.

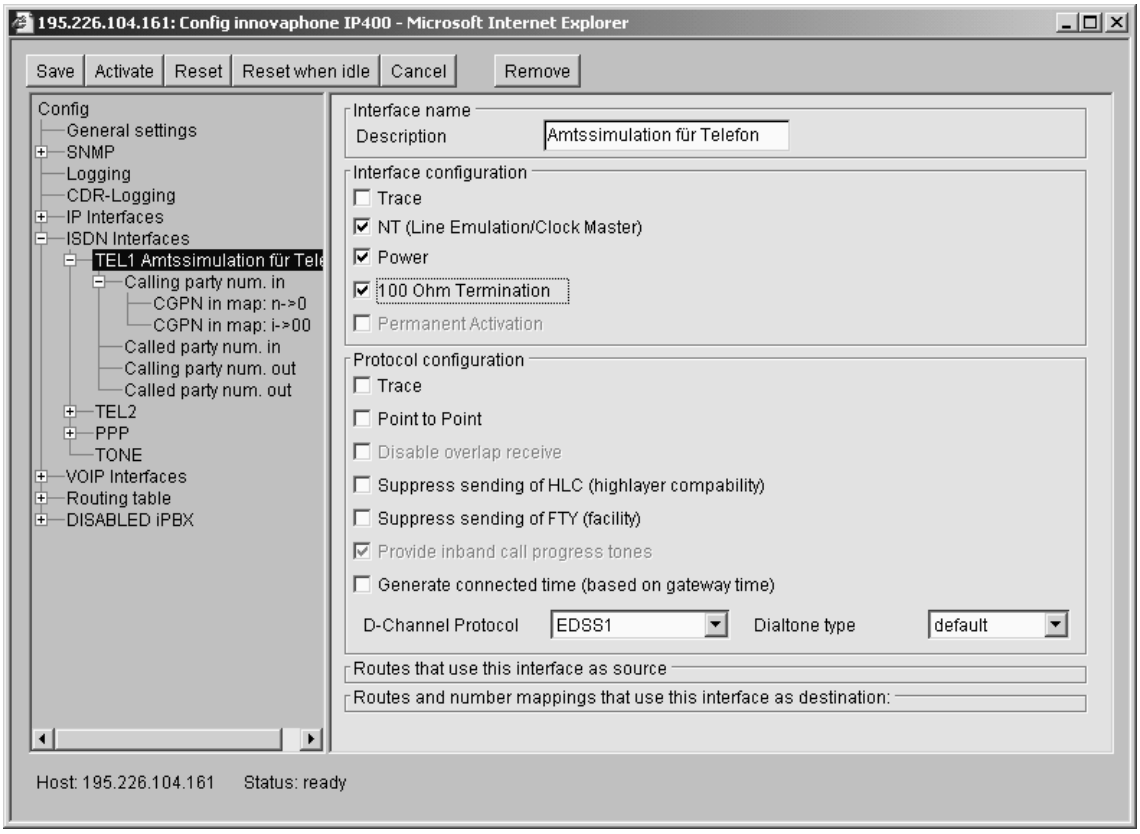
▲ Mark the NT checkbox

[29] And thus not for the IP 3000

- ▲ Mark the POWER checkbox if an attached device requires power feeding from the ISDN line
- ▲ Mark the 100 OHM TERMINATION checkbox
- ▲ Uncheck the PERMANENT ACTIVATION checkbox
- ▲ Uncheck the POINT TO POINT checkbox.
- ▲ Uncheck the DISABLE OVERLAP RECEIVE checkbox
- ▲ Uncheck the SUPPRESS SENDING OF HLC and SUPPRESS SENDING OF FTY checkbox (see "Suppression of certain protocol elements" above)
- ▲ Select the EDSS1 protocol in the D-CHANNEL PROTOCOL selection field (refer to “The signalling protocols” above)
- ▲ Select the desired dial tone in the DIALTONE TYPE selection field
- ▲ The special modification of called party and calling party number is normally not necessary in this configuration. Read up on this in section "Treatment of the various ISDN address types" on page 87.

In this mode, two telephones or other ISDN terminal equipment can be directly connected to each of the ISDN interfaces TEL1 and TEL2, thus making an overall maximum of four units connected to one IP 400. With an ISDN bus link to TEL1 or TEL2, up to eight devices can be connected to each of the interfaces. If the terminal equipment concerned obtains its power supply from the ISDN network, the total current consumption of all devices attached must not exceed 4 watts.

Figure 31 Configuration of TEL1 for the connection of ISDN telephones

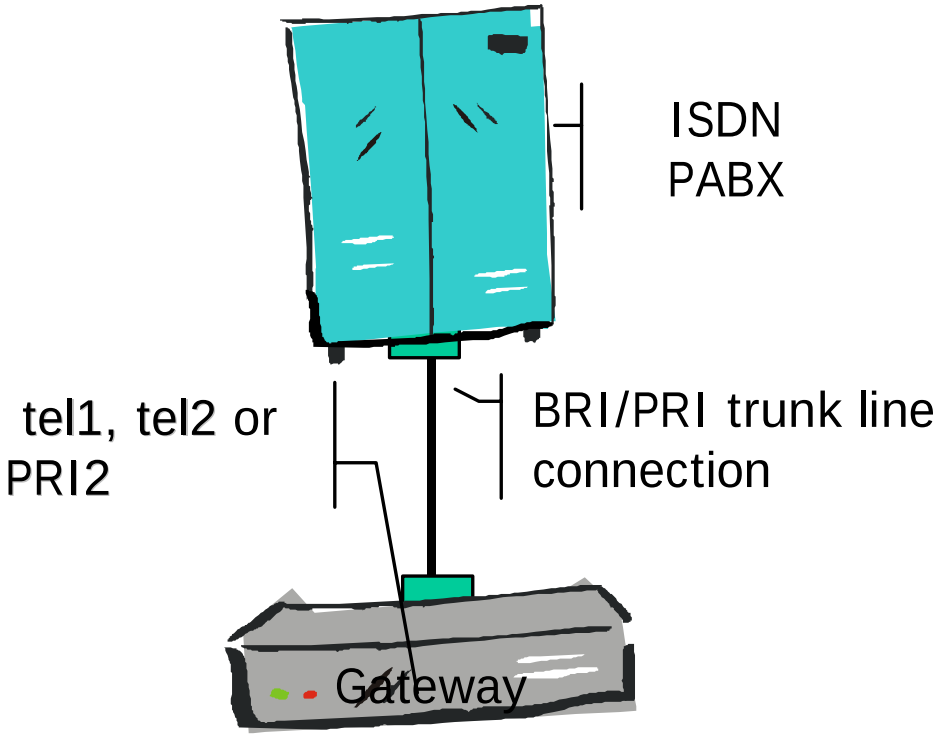


Use as a trunk line for an ISDN PABX

In this case, the gateway interface is connected to an ISDN PABX as sole trunk line or as an additional line within a trunk group. It then acts like a "point to point" connection of your network provider.

For this the interface must be operated in the NT mode. Consequently, only the TEL1, TEL2 and PRI2 interfaces are appropriate to this type of use.

Figure 32 Gateway providing a trunk line

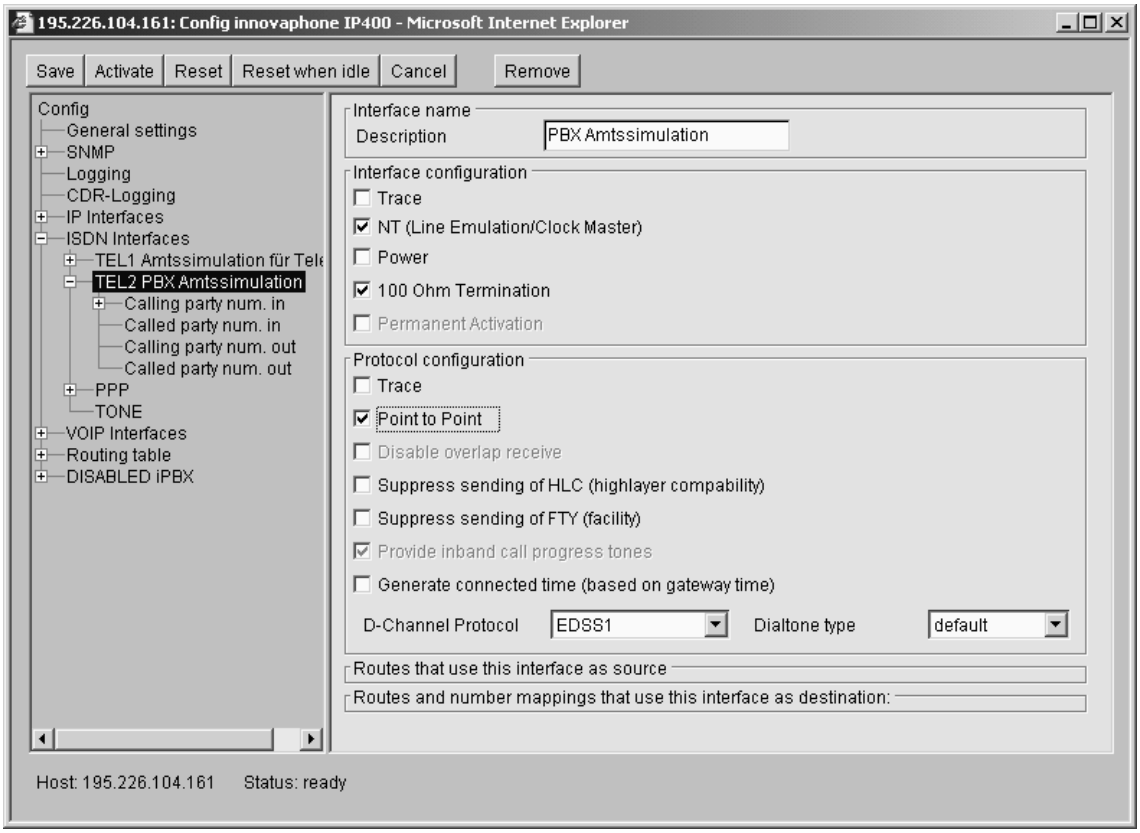


Some BRI PBXs (especially the smaller ones) are intended for connection to a trunk line in "point to multipoint" mode. Configuration of the ISDN interface must match this. If you are uncertain about the line mode your PABX requires, consult the appropriate documentation that came with your PABX.

- Mark the NT checkbox (TEL1 and TEL2 only)
- Uncheck the POWER checkbox (TEL1 and TEL2 only)
- Mark the 100 OHM TERMINATION checkbox (TEL1 and TEL2 only)
- If your PABX is intended for operation on a POINT TO POINT connection, mark the POINT TO POINT checkbox. If it is meant for operation on POINT TO MULTIPOINT, uncheck the POINT TO POINT checkbox (TEL1 and TEL2 only)
- If CRC4 checksums are generated on the connection, uncheck the NO CRC4 checkbox. Otherwise, check this option. In Germany PRI lines are mostly operated with CRC4 (PRI2 only)
- If the assignment of B channels is to be from the top down, mark the ASSIGN OUTGOING CHANNELS FROM TOP checkbox; for this refer to "The assignment of B channel numbers with PRI connections" on page (PRI2 only)
- Uncheck the DISABLE OVERLAP RECEIVE checkbox

- ▲ Uncheck the SUPPRESS SENDING OF HLC and SUPPRESS SENDING OF FTY checkbox (see "Suppression of certain protocol elements" above)
- ▲ Uncheck the PROVIDE INBAND CALL PROGRESS TONES checkbox (refer to "Dial tones" on page 72)
- ▲ Select the EDSS1 protocol in the D-CHANNEL PROTOCOL selection field (refer to "The signalling protocols" on page)
- ▲ Select the desired dial tone in the DIALTONE TYPE selection field
- ▲ The special modification of called party and calling party number is normally not necessary in this configuration. Read up on this in section "Treatment of the various ISDN address types" on page 87.

Figure 33 Configuration of TEL1 as trunk line for a PABX

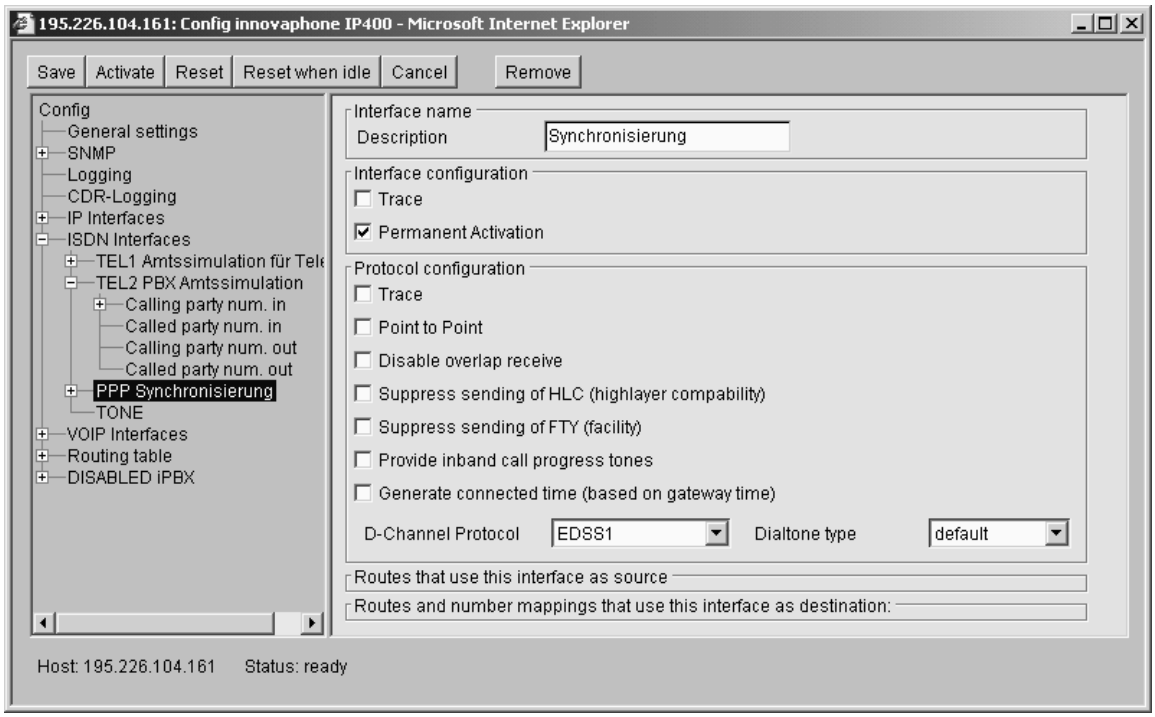


The PPP and S/T interfaces are intended solely for connecting a trunk to the gateway. Therefore, connection of an ISDN PABX in this manner is not possible here (however, refer to "Use as subscriber on an ISDN PABX" on page 82).

If, aside from the gateway, the PABX is also connected to another trunk line, it must be ensured that both trunk lines are synchronised. This is done by connecting the IP 400's PPP interface or IP 3000's S/T interface to the direct trunk line with a standard ISDN cable parallel to the PABX. The second RJ45

jack normally available on the (network provider's) network termination unit (NTBA) can be used for this. If the PABX is not connected via a basic access to the ISDN permanent network (thus, for example, on a primary rate access), the PPP interface can instead be connected with an unused BRI subscriber line of the PABX.

Figure 34 Configuration of the interface for clock synchronisation



In this case, the interface must under no circumstances be used for incoming or outgoing calls (refer to "Configuring the call routing" on page 124). The interface's POINT TO POINT checkbox must be unchecked and the PERMANENT ACTIVATION checkbox must be checked.

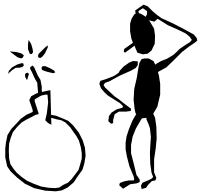
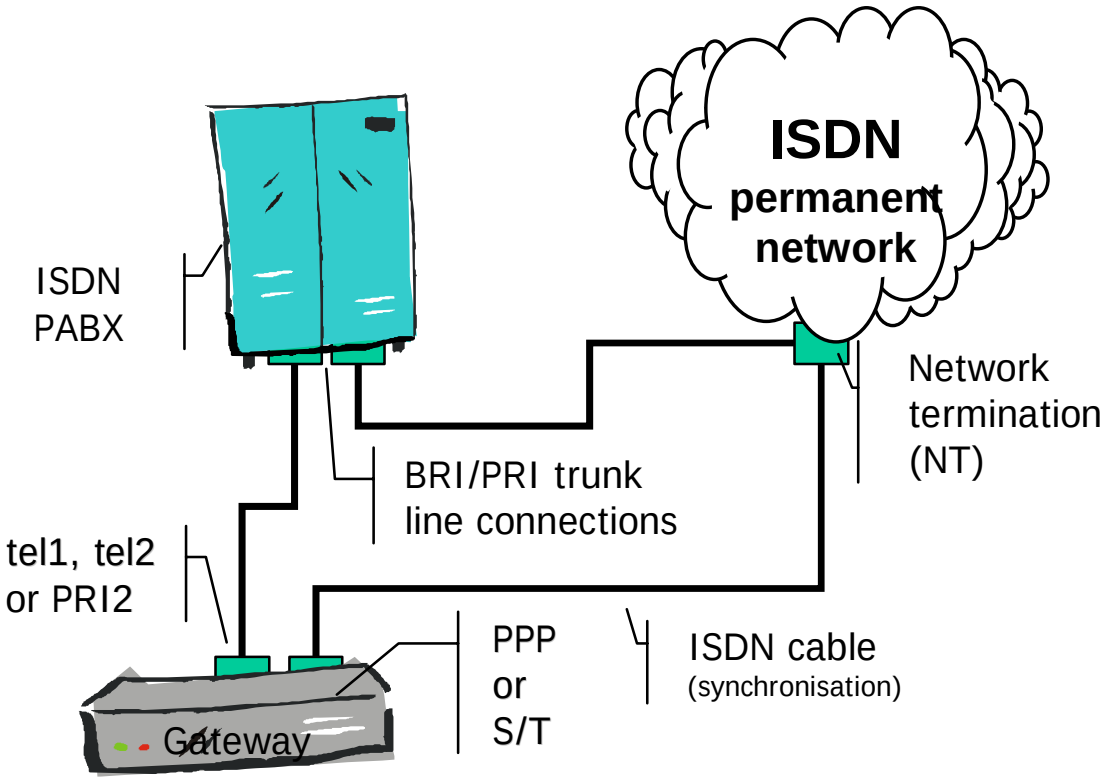


Figure 35 Synchronisation of a gateway with an ISDN BRI connection



Use as subscriber on an ISDN PABX

In certain case, it may be necessary to connect the gateway as subscriber to a terminal equipment access[30] of the ISDN PABX. This is required, for example, if the PABX does not support an additional trunk line and the existing one is to continue working unchanged, and no tie line is available either (refer to "Use on a tie line of a PABX").

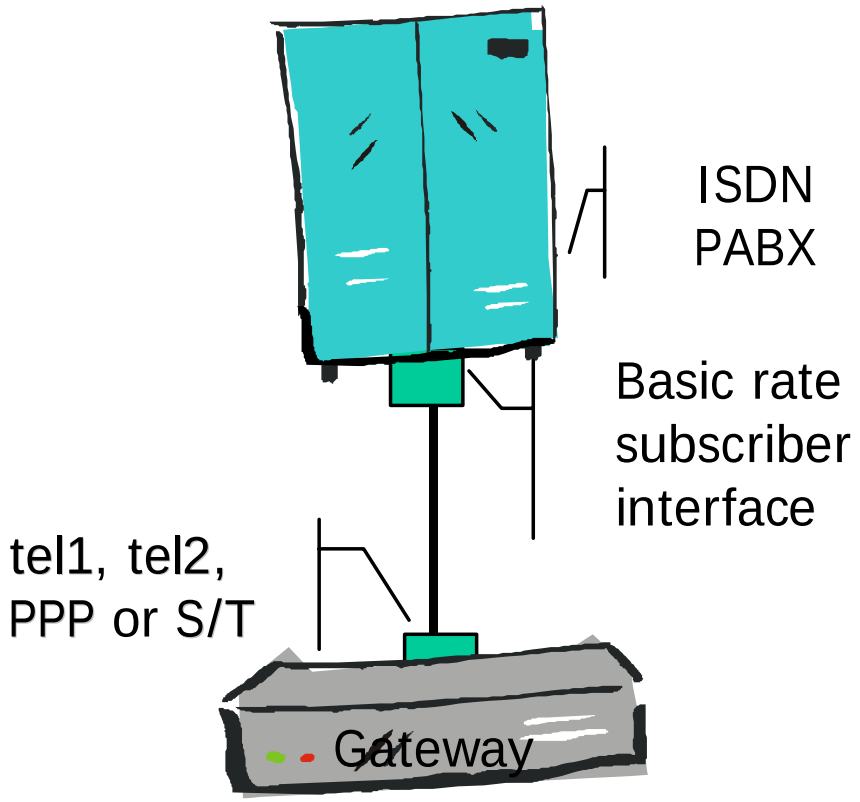
Remember though, that in this case various limitations apply depending on the PABX, since it expects a single terminal device on this connection and not an intermediate terminal.

[30] And therefore a point to multipoint connection

This type of connection occurs only in connection with BRI interfaces and therefore is normally of relevance only for the IP 400, although in theory it can also occur on the IP 3000's S/T interface.

In this case, the PABX is connected to the gateway like a trunk line, as described in section "Use as connection for a trunk line (dial- or permanent connection) on page 73. However, the line provided by the PABX is typically configured in "point to multipoint" mode. The "POINT TO POINT" checkbox must then be unchecked accordingly. If the PABX does not support overlapped dialling to the terminal device, mark the DISABLE OVERLAP RECEIVE checkbox (refer to "Overlapped dialling on terminals on point to multipoint connection" on page 71).

Figure 36 Gateway on PABX subscriber interface



The limitations mentioned above generally do not apply if the PABX provides a point to point connection on the subscriber line (this is often referred to as a "tie line").

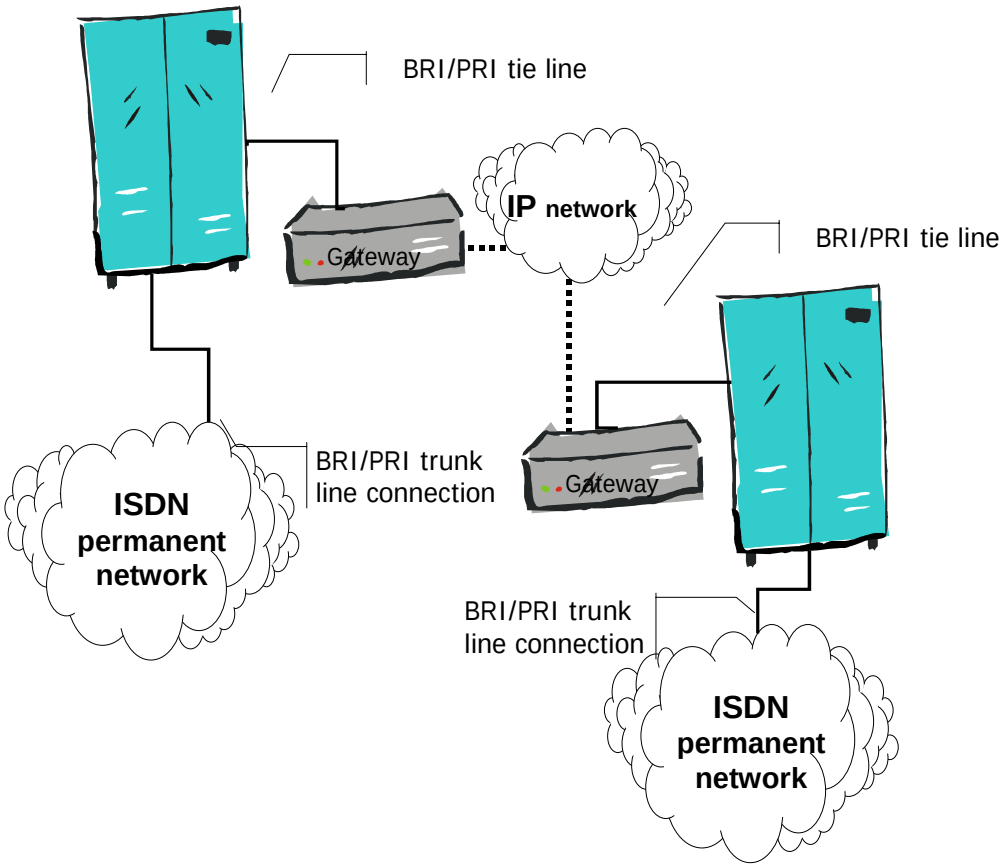
Note, however, that the gateway does not support any proprietary subscriber protocol for operating telephones on PABXs.

Use on a tie line of a PABX

Connection of the gateway to a tie line of a PABX is generally the most sensible method of linking two or more PABXs.

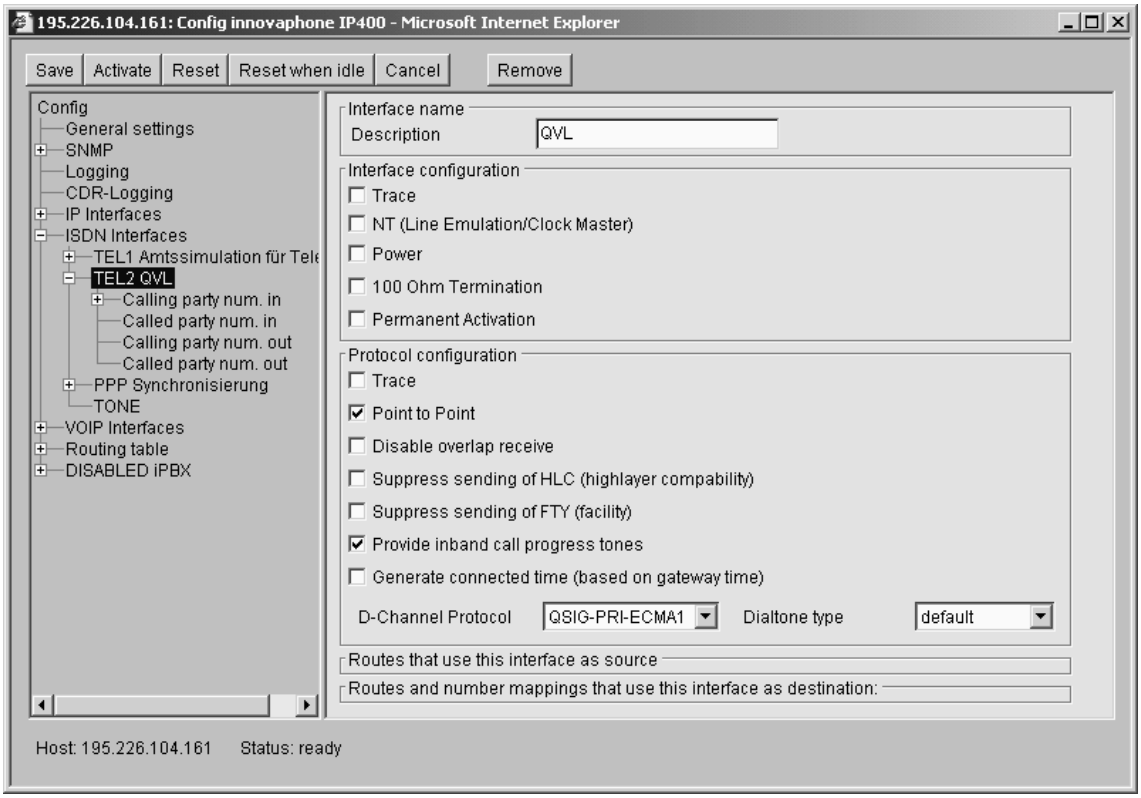
Here the gateway can be operated as Clock-master (NT) or Clock-slave (TE) (for this refer to page 69). If the PABX has its own clock, the gateway can be operated in TE mode without any difficulty. This is also possible at both ends of the link.

Figure 37 Gateway on a tie line



- ▲ Mark the "NT" checkbox if the gateway is to supply the clock. Uncheck (deactivate) the checkbox if the PABX requires the clock (TEL1, TEL2 only)
- ▲ Uncheck the POWER checkbox (TEL1 and TEL2 only)
- ▲ Uncheck the 100 OHM TERMINATION checkbox (TEL1 and TEL2 only)
- ▲ Uncheck the PERMANENT ACTIVATION checkbox (TEL1, TEL2, PPP and S/T only)
- ▲ Mark the POINT TO POINT checkbox

Figure 38 Connection as tie line



- ▲ Uncheck the CONNECT PRI1 AND PRI2 WITH RELAY checkbox (PRI1 only)
- ▲ If CRC4 checksums are generated on the connection, uncheck the NO CRC4 checkbox. Otherwise check the NO CRC4 checkbox. In Germany PRI lines are mostly operated with CRC4 (PRI1 and PRI2 only)
- ▲ If the assignment of B channels is to be from the top down, mark the ASSIGN OUTGOING CHANNELS FROM TOP checkbox (PRI1 and PRI2 only)
- ▲ Uncheck the DISABLE OVERLAP RECEIVE checkbox
- ▲ Uncheck the SUPPRESS SENDING OF HLC and SUPPRESS SENDING OF FTY checkbox (refer to "Suppression of certain protocol elements" on page 72)
- ▲ Mark the PROVIDE INBAND CALL PROGRESS TONES checkbox (refer to "Dial tones" above)[31]
- ▲ Select the correct signalling in the D-CHANNEL PROTOCOL selection field (refer to "The signalling protocols" on page 70)
- ▲ Select the desired dial tone in the DIALTONE TYPE selection field (refer to "Dial tones" starting page 72)

[31] Turn this option off if it leads to errors in call mediation via the tie line or in call cleardown

▲ If call numbers with a different type of address are transmitted on the tie line as unknown, then special modification of the called party and calling party number is necessary. Read up on this in section "Treatment of the various ISDN address types" on page 87.

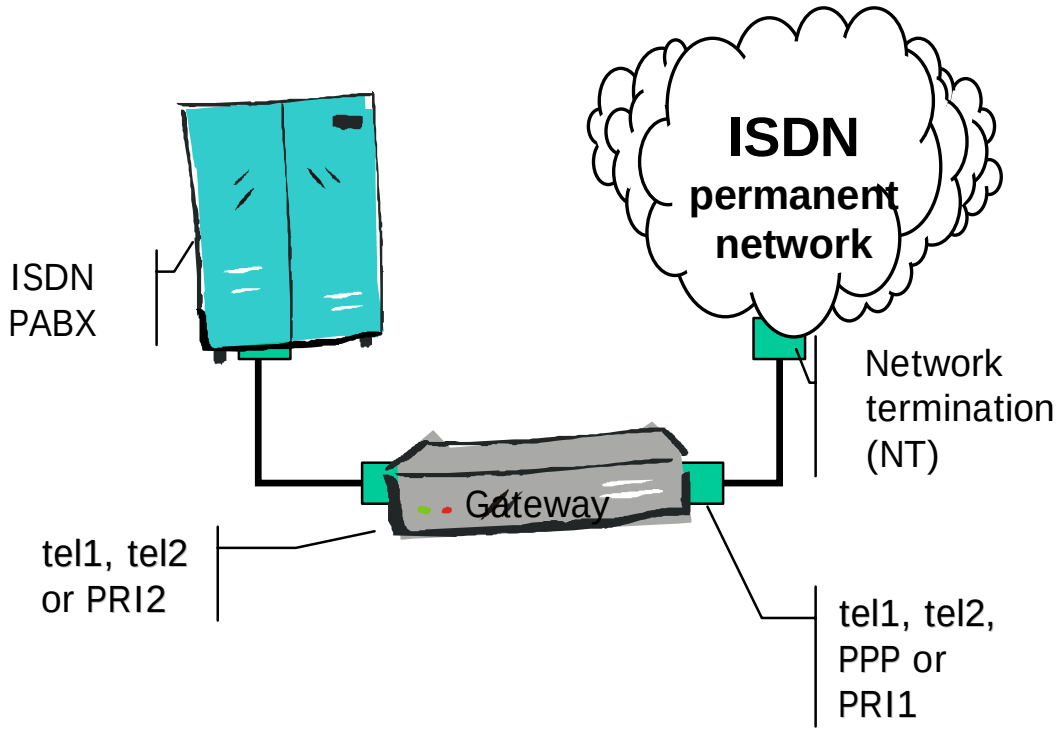
Looping the gateway into an existing trunk line

In some cases no further ISDN interfaces can be used to connect the gateways to the PABX. In such cases it is useful to loop the gateway into the existing trunk line.

Per trunk line this requires the gateway to have one ISDN interface for the trunk (TE mode) and one for the PABX (NT mode). This is the reason why the IP 3000 is equipped with two PRI interfaces, PRI1 and PRI2. The IP 400 can also be looped into a trunk line, except that in this operating mode not all of the four possible calls in parallel can be utilised, since although the IP 400 has two NT interfaces (TEL1 and TEL2), it has only one TE interface (PPP).

Configuration of the interfaces in the trunk direction is done as described in section "Use as connection for a trunk line (dial- or permanent connection)" starting page 73 and in the PABX direction as described in section "Use as a trunk line for an ISDN PABX" starting page 78. In general, however, call numbers with various types of address are transmitted on a trunk line, so special modifications to the called party and calling party number are required. It is essential to read up on this in section "Treatment of the various ISDN address types" below.

Figure 39 Looping of the gateway into a trunk line



Treatment of the various ISDN address types

Internally the gateways principally deal with call numbers using number type[32] unknown. In ISDN though, there are various types of call number (refer to Table 15 Number types), so call numbers are only ever to be interpreted in conjunction with their number types. Thus, for example, in Germany a called number 0711654321 of unknown number type on a trunk line corresponds to the called number 711654321 of national number type. The reason for this is that in Germany the discriminating digit for national numbers is 0. On the other hand, the calling number 43551234 of number type unknown denotes a line in the home local network, whereas the same number 43551234 with international number type denotes a connection in the Pfäffikon local network in Switzerland.

The evaluation of call numbers within the gateway thus calls for a normalisation in the call number type unknown. This can be done with the aid of the so-called

[32] "type of number"

CGPN[33] MAP and CDPN[34] MAP entries, which can be defined both on the ISDN interfaces and on the individual gateway definitions.

Table 15 Number types

Designation	Meaning	Typical usage	Abbrev.[35]	Prefix[36]
Unknown	Unspecified	Called number with the outgoing call	u	
Subscriber	Call number in local network	Called number with the incoming call	s	
National	Call number with area code	Calling number from home country	n	0
International	Subscriber's number with country code and area code	Calling number from abroad	i	00
Abbreviated		not usual	a	
Network specific		not usual	x	

The following mappings for the calling number are contained in the standard configuration for all ISDN interfaces and for the gateways (refer to Figure 40 Standard CGPN/CDPN Mappings below):

Table 16 CGPN Mappings in the standard configuration

Type	Number type	Number prefix	Replaced number prefix	Usage
Incoming calling	National	Blank	0	Prefixes discriminating

[33] CGPN ::= **c**allin**g** **p**arty **n**umber

[34] CDPN ::= **c**alle**d** **p**arty **n**umber

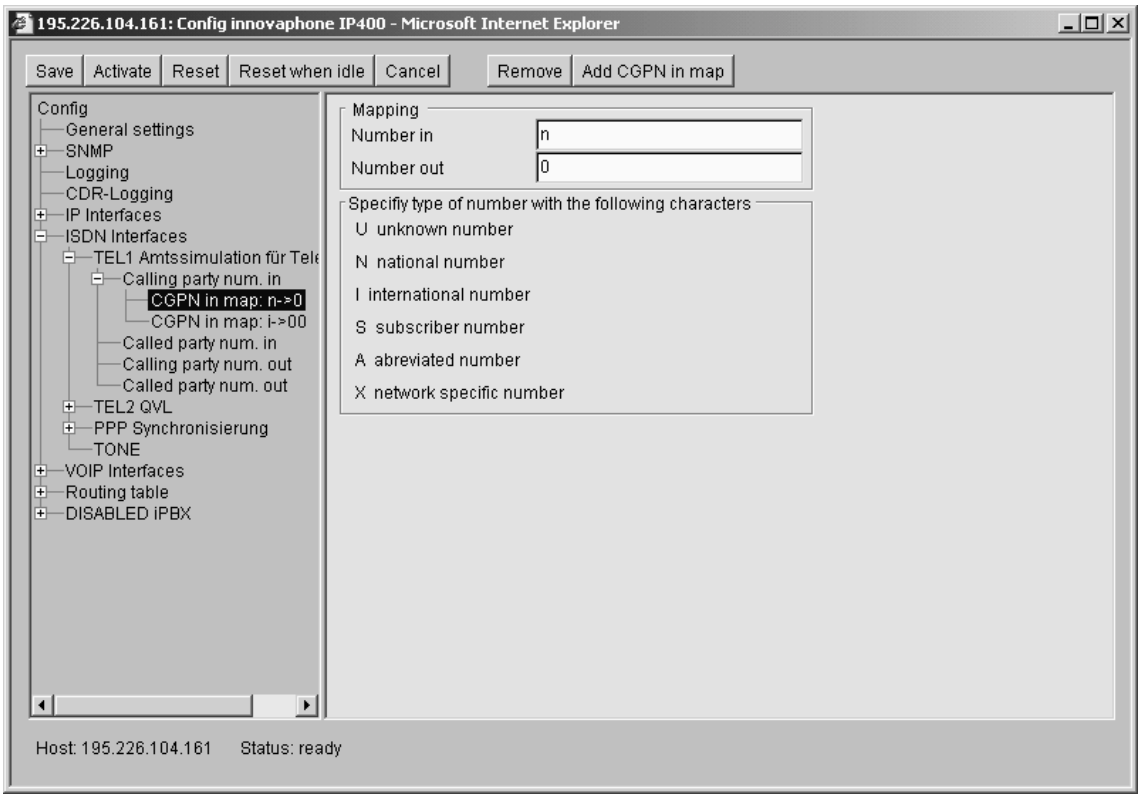
[35] in the CGPN/CDPN Mappings

[36] Equivalent discriminating digit for outgoing calls in Germany

Type	Number type	Number prefix	Replaced number prefix	Usage
number				digit 0 to national CLIs
Incoming calling number	International	Blank	00	Prefixes discriminating digits 00 to international CLIs

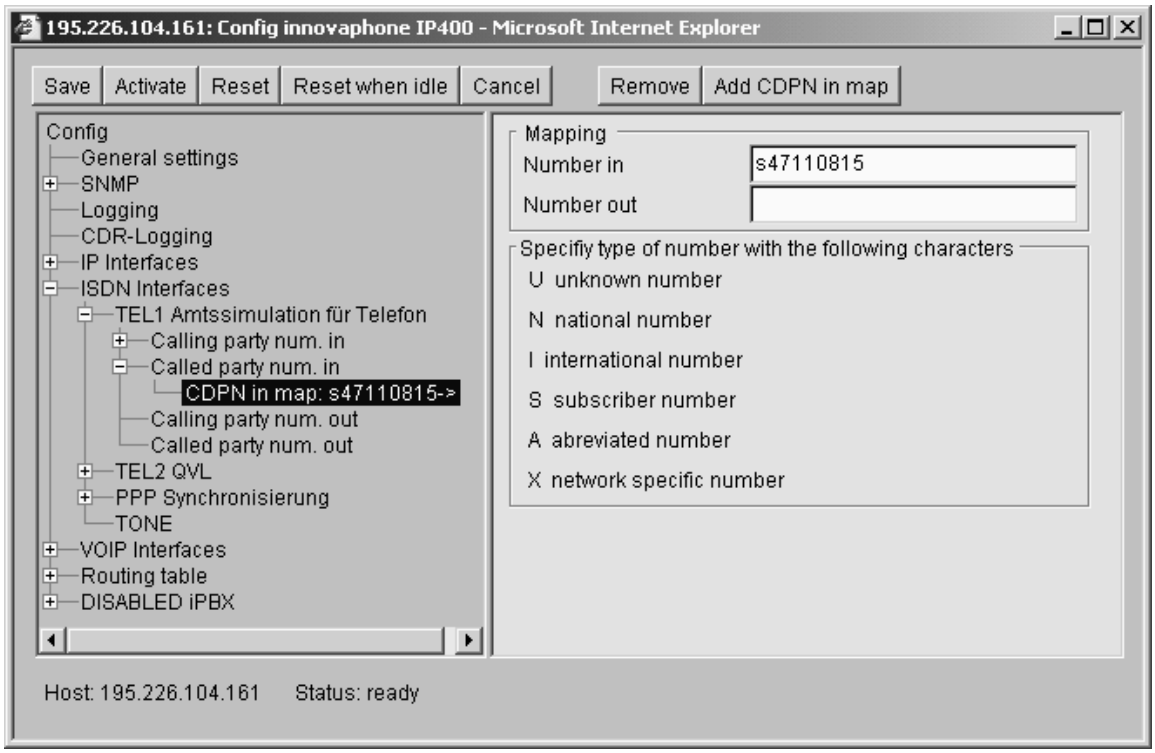
Through this it is ensured that display of the calling number is correct with incoming calls of all number types.

Figure 40 Standard CGPN/CDPN Mappings



A typical application of CDPN mappings is the manipulation of the root number on the point to point connection for incoming calls. Here the root is removed from the called number, which mostly comes in as a number of subscriber type. After that just the direct dialling is dealt with in the routing table of the gateway. Figure 41 Manipulation of the root number through CDPN MAPPINGS below shows a configuration of this type.

Figure 41 Manipulation of the root number through CDPN mappings



- ▲ In the left half of the configuration applet, choose the interface for which you want to set up call number modifications
- ▲ If necessary extend the tree depiction by clicking on the ?symbol next to the interface name
- ▲ Select one of the following lines in the depiction on the left-hand side
  - ▲ CALLING PARTY NUM. IN if you want to manipulate the calling number of incoming calls
  - ▲ CALLING PARTY NUM. OUT if you want to manipulate the calling number of outgoing calls
  - ▲ CALLED PARTY NUM. IN if you want to manipulate the called number of incoming calls
  - ▲ CALLED PARTY NUM. OUT if you want to manipulate the called number of outgoing calls
- ▲ Insert mappings by clicking on the ADD CGPN/CDPN IN/OUT MAP button at the upper border
- ▲ Under NUMBER IN define the number type and –prefix that you wish to have replaced. The number type is denoted here using the respective abbreviation from Table 15 Number types on page 88

▲ Define the substitution under NUMBER OUT

The result of the example shown in Figure 41 Manipulation of the root number through CDPN MAPPINGS is thus that the called number of incoming calls (CDPN in) is replaced when the call number type is subscriber (abbrev. s) and the number starts with the digits 47110815.

Note that call numbers within the gateway are always processed in unknown format. Thus the result of a number replacement for incoming calls is always of type unknown and the call number type of outgoing calls for replacement is similarly always unknown. Accordingly, you cannot specify a number type for replacements of incoming numbers in the NUMBER OUT field and for replacements of outgoing numbers in the NUMBER IN field.

Considerations for configuring the analogue interfaces

... for experts

- ▲ TEL and TEL2 are intended solely for connecting analogue terminals
- ▲ Call waiting can be suppressed, in particular in fax mode (BUSY ON BUSY)
- ▲ In special case, flash/hook interpretation can be disabled with PASSIVE
- ▲ Connect Audio (AUX) with 3.5mm stereo jack
- ▲

The IP 21 IP Adapter has 2 analogue terminal device interfaces (TEL1 and TEL2), an analogue stereo line-in interface (AUX) and a 4+n door release connection (DOOR). According to the number of available DSP channels (see Figure, page 165), 1 or 2 interfaces may be used simultaneously.

Analogue end device interfaces

The two TEL1 and TEL2 analogue interfaces of the IP 21 are intended solely for connecting analogue end devices[37]. Typically, an analogue telephone or Group 3

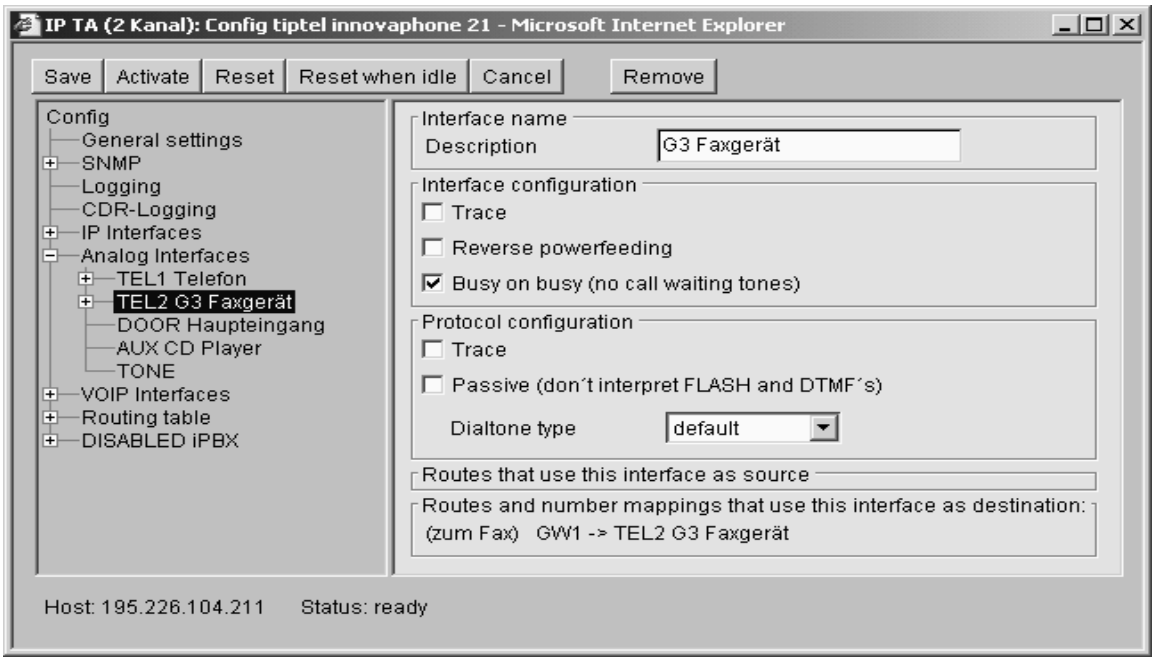
[37] This involves a so-called FXS interface

fax machine can be connected to them. The connection of analogue PABXs is not supported.

Call waiting

The analogue interfaces support the Call waiting function. If another call arrives while a call is in progress, it is announced by an Call waiting tone in the active terminal. If the interface is connected to a fax machine, the function is undesirable since the Call Waiting Tone would interfere with the fax transmission.

Figure 42 No Call Waiting on the analogue interface



▲ If a fax machine is connected or if call waiting is not wanted for the telephone, check the BUSY ON BUSY checkbox

Performance characteristics on the analogue connection

If a telephone is connected to TEL1 or TEL2, it can use extended performance characteristics, such as Call Hold, Enquiry Call and Broker's Call, by means of certain Flash/DTMF sequences.

Table 17 Extended performance characteristics on the analogue connection

Performance characteristic	Description	Usage
Accepting a waiting call and terminating the current call	During an active call you receive another incoming call. You want to terminate the active call and take the waiting call.	▲ You hear the Call Waiting tone ▲ Hang up ▲ The active call is terminated and the phone rings again ▲ Take the call in the usual way ▲ The call that was waiting is now active
Accepting a waiting call without terminating the current call	During an active call you receive another incoming call. You want to accept this call without terminating the current call	▲ You hear the Call Waiting tone ▲ Press the R-key[38] ▲ Press 2 ▲ The first call is put on hold and the call that was waiting is now active
Enquiry call	You want to make a second call during an active call	▲ Press the R-key ▲ Dial the desired number ▲ The first call is put on hold while the new call is set up
Call hold	You have two calls at the same time and wish to switch between the two	▲ Press the R-key ▲ Press 2 ▲ The previously active call is put on hold and the call

[38] The R-key is also described as the Flash- or Hook/Flash-key

Performance characteristic	Description	Usage
		previously on hold becomes active
Connect	You have one active call and one call on-hold and you want to connect the two	▲ Hang up
Cutting off one of two calls	You have two calls at once and want to cut one of them off	▲ Press the R-key ▲ Press 1 ▲ The active call is terminated
3-party conference[39]	You have two calls at once and want to set up a 3-party conference	▲ Press the R-key ▲ Press 1 ▲ The active call is terminated

The audio connection

The IP 21 has a 3.5 mm stereo jack bush designated AUX for connecting to an audio source. This allows you to connect the Line-out output to a music source[40] or a PC sound card. Make sure you use a stereo cable, otherwise one channel of your music source will be short-circuited, and this could lead to damage.

The AUX interface may only usefully be employed as a call destination, since it can never initiate a call. An incoming call on this interface will be accepted immediately and the audio signal over the jack bush will be played to the caller.

The interface requires no configuration.

[39] Please note that this function needs two DSP channel installed. Furthermore, the IP-21 in this mode is no longer available to make another call on another interface.

[40] A CD player, for example.

The door intercom

The IP 21 has a DOOR interface designated 4+n for connecting to a door intercom (DI).

This interface can be used both as a destination and source of a call. It is usually used as a call source. When the doorbell activates the DI, this triggers in the IP 21 a call from the DOOR interface. When a call is received on the DOOR interface, it is connected to the DI and the caller can communicate over the station. Extra dialling digits are ignored.

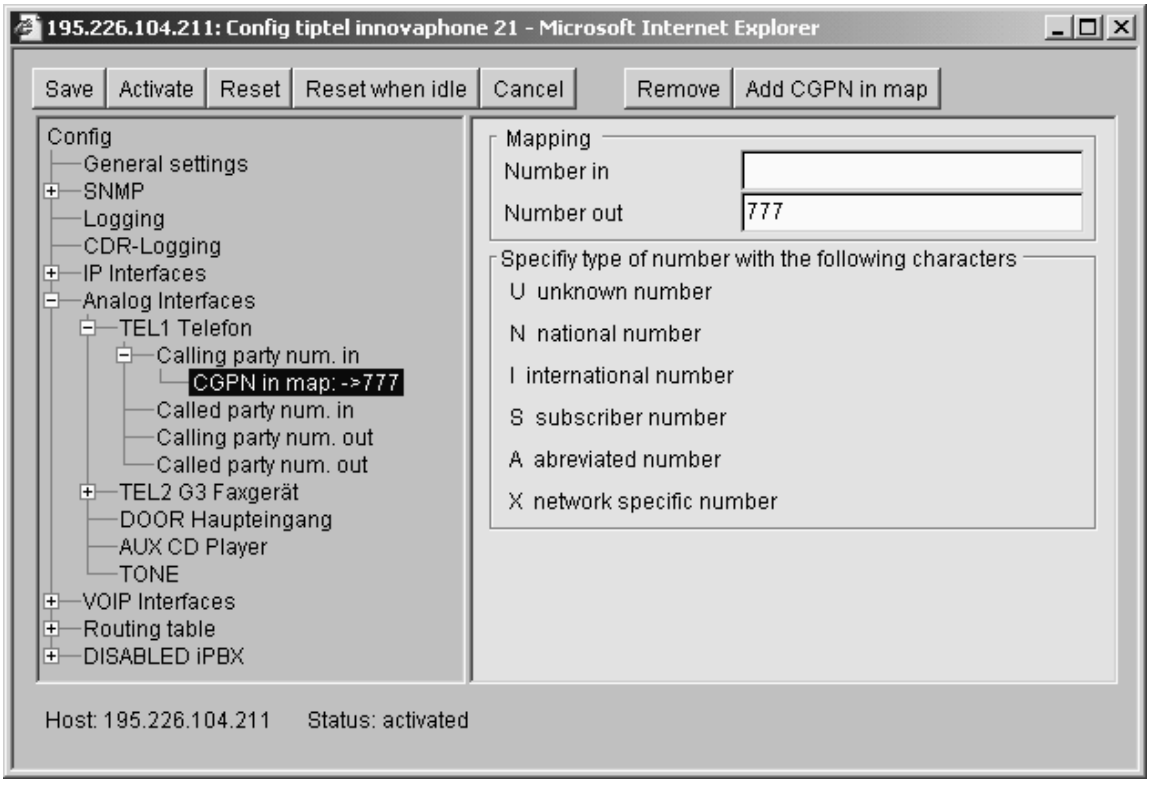
While you are connected to the station, you can activate two door openers by telephone. This is done by dialling ``*´´ for Opener 1 or ``#´´ for Opener 2.

The interface requires no configuration.

Handling call numbers on the analogue interfaces

As with the ISDN interfaces (see page 87), call number manipulation can also be configured on the analogue interfaces.

Figure 43 Call number manipulation on the analogue interface



In principle the same manipulations can be used. Since, however, no calling call numbers (CLI) can be registered by analogue terminals (or by the door release device), no CGPN numbers can be manipulated on arrival either. However, a CGPN may be added for the interface. As with the ISDN interfaces (see page 87), call number manipulation can also be configured on the analogue interfaces.

 above shows how the calling number identification 777 is assigned to the telephone on the TEL1 interface[41]

The IP 21 currently supports no CallerId[42], so there is no point in manipulating outgoing call numbers on an analogue interface.

To assign a call number to a telephone or door intercom, proceed as follows:

▲ Check the corresponding interfaces in the ANALOGUE INTERFACES section

▲ Check the CALLING PARTY NUMBER IN entry

▲ Click on the ADD CGPN IN MAP button

[41] Please note that the assignment of calling numbers to the interface is carried out by the optional iPBX component if used, in which case this is not necessary.

[42] CallerID is the transfer of the calling number to the analogue terminal.

- Leave the NUMBER IN field in the MAPPING area empty
- Enter the desired number in the NUMBER OUT field

Considerations for configuring the virtual interfaces

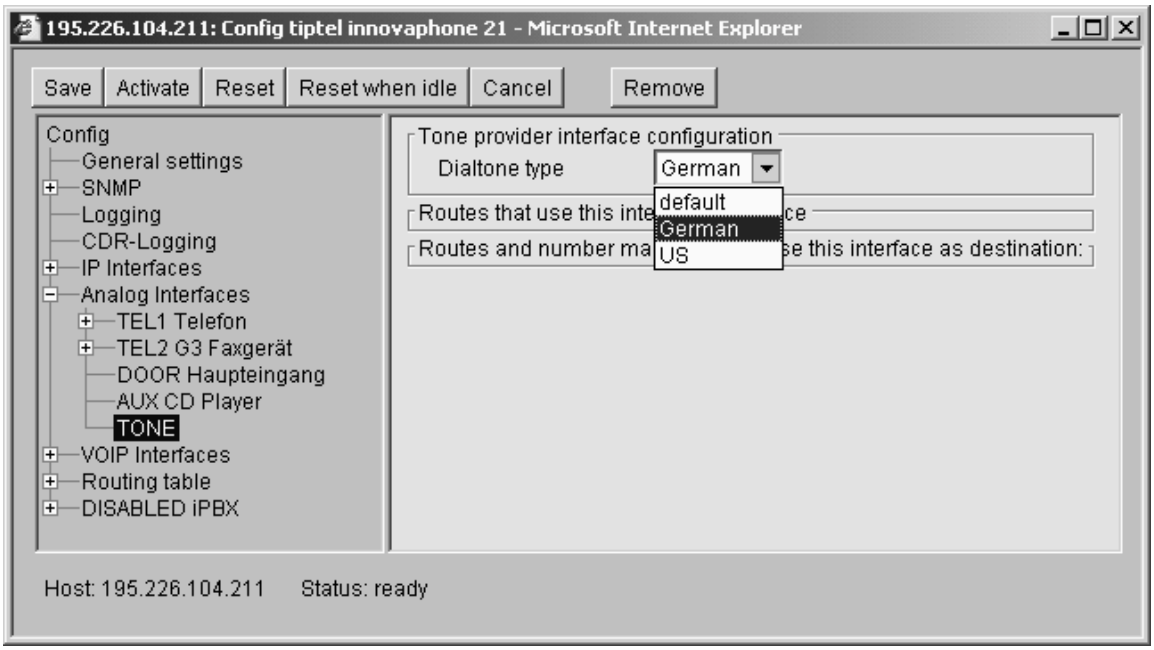
The gateways have the TONE and TEST virtual interfaces. These are not physical interfaces, but virtual interfaces created within the device.

The TONE dial tone interface

The gateways have an internal TONE interface. This may only usefully be employed as a call destination. If a call goes via the TONE interface, it is not connected but receives the dial tone configured for the interface[43]. If an extra digit is dialled or the original call contains already dialled digits, the call will be refused.

[43] The incoming call will then be acknowledged with a SETUP_ACK and a media channel will be set up.

Figure 44 Configuration of the TONE interface



The Tone interface can be used to play a caller a dial tone, even though the caller's call has not yet been connect to a "genuine" trunk line. This occurs in particular for least-cost-routing scenarios, whereby the routing of the call can only be undertaken following analysis of several call digits.

The Tone interface can process several calls at once. The dial tone used is configured in the ANALOGUE/ISDN INTERFACES, TONE area under TONE PROVIDER INTERFACE CONFIGURATION.

The TEST interface

The gateways have an internal TEST interface. This may only usefully be employed as a call destination. If a call goes via the TEST interface, it is connected and the hold music contained in the non-volatile memory is played back. Subsequent digits are ignored.

Please note that the TEST interface can only work with G.729A or G.723 calls. For G.711 calls, no music is played.

The interface cannot be configured.

Configuration of VoIP interfaces

Just as ISDN interfaces lead in the world of classical telephony, by similar token "VoIP interfaces" are channels in the Voice over IP world. Thus if your gateway needs to communicate with other devices via VoIP, access to these devices has to be configured as a VoIP interface.

Here, different types of devices may be involved:

- Other innovaphone® gateways
- VoIP terminal equipment, for example IP telephones such as the innovaphone® IP 200
- VoIP terminal adapters, such as the innovaphone® IP 21 for connection of analogue terminal equipment or a DECT base station
- Third-party VoIP gateways, as a gateway to telephony switches or into the SS7 network, for example
- Further gatekeepers for call control
- VoIP PC programmes such as Microsoft™'s NetMeeting, for example

Each VoIP interface defines access to a group of devices that in a certain way will be handled similarly. For example, this allows all IP telephones in a location to be configured via just a single VoIP interface. Since your gateway allows the definition of 12 different groups, overall it is able to communicate with several hundred VoIP devices.

Configuration is done in the VoIP INTERFACES area of the configuration applet.

General considerations for configuring the VoIP interfaces

A telephony infrastructure in the VoIP environment is basically made up of three different building blocks:

- VoIP end points

  In this block are devices that implement the end points of telephone calls. For example, an IP telephone such as the innovaphone® IP 200 or VoIP

software such as Microsoft™'s NetMeeting. Such end points are mostly assigned to just a single user.

- VoIP Gateways

  Here we are concerned with gateways to other telephony networks or – techniques. This may include gateways into the ISDN network or the analogue telephone network, or adapters for connecting traditional, analogue terminal equipment or existing PABXs. Gateways most often afford the opportunity of reaching a number of users or terminal devices.

- Gatekeepers

  Gatekeepers are used for call control and call switching. They have the ability to manage VoIP terminal equipment and gateways, and to interpret call numbers and names, and thus can carry out the call switching. Thus they take on the role of the PABX or switching centre in classical telephony. Gatekeepers are optional though, and end points and gateways can also communicate with one another directly, if desired.

Your innovaphone® gateway also always contains a gatekeeper that you may use if desired. Gatekeepers and VoIP end points or VoIP gateways normally communicate via the so-called RAS protocol. Your gateway may be used with or without the RAS protocol, as desired. As far as the telephony performance characteristics are concerned, no disadvantages result from using it without RAS. Even the sophisticated routing functions of your gateway can be fully exploited in this mode.

There are several advantages that come from using the RAS protocol though:

- The gatekeeper is able to carry out the translation of logical device names (so-called Aliases) into IP addresses. This allows VoIP devices to be integrated whose IP address is assigned dynamically. Only in this way can use be made of VoIP devices configured through DHCP or via a PPP dial-up connection
- The gatekeeper is able to continuously keep a record of the availability of the VoIP devices known to it. This allows the administrator to get an overview of the status at any time. On top of this, the switching of calls can be made to depend on the availability, without requiring time-consuming checking of this at the time of the call. This results in significantly improved response in the event of a fault
- With many third-party VoIP devices the RAS protocol is obligatory for operation.

It is advisable to put into operation the gateway contained in your gatekeeper, and to use the RAS protocol if possible. Should any individual VoIP devices that your gateway needs to communicate with not permit the RAS protocol, these can still be addressed directly without any difficulty.

Of course you can also operate your gateways in conjunction with an already available gatekeeper.

Note, however, that many performance characteristics in a VoIP network are also dependent on the gatekeeper that is used. The specific performance characteristics available when using an external gatekeeper is therefore dependent on the individual case.

Understanding your gateway's gatekeeper

Basically, there are two tasks that the gatekeeper has to carry out

- Management of the terminal equipment (device management)
- The switching of voice calls (call switching)

Both functions are contained within your gateway, although device management is optional.

Figure 45 Call sequence with a gatekeeper and RAS

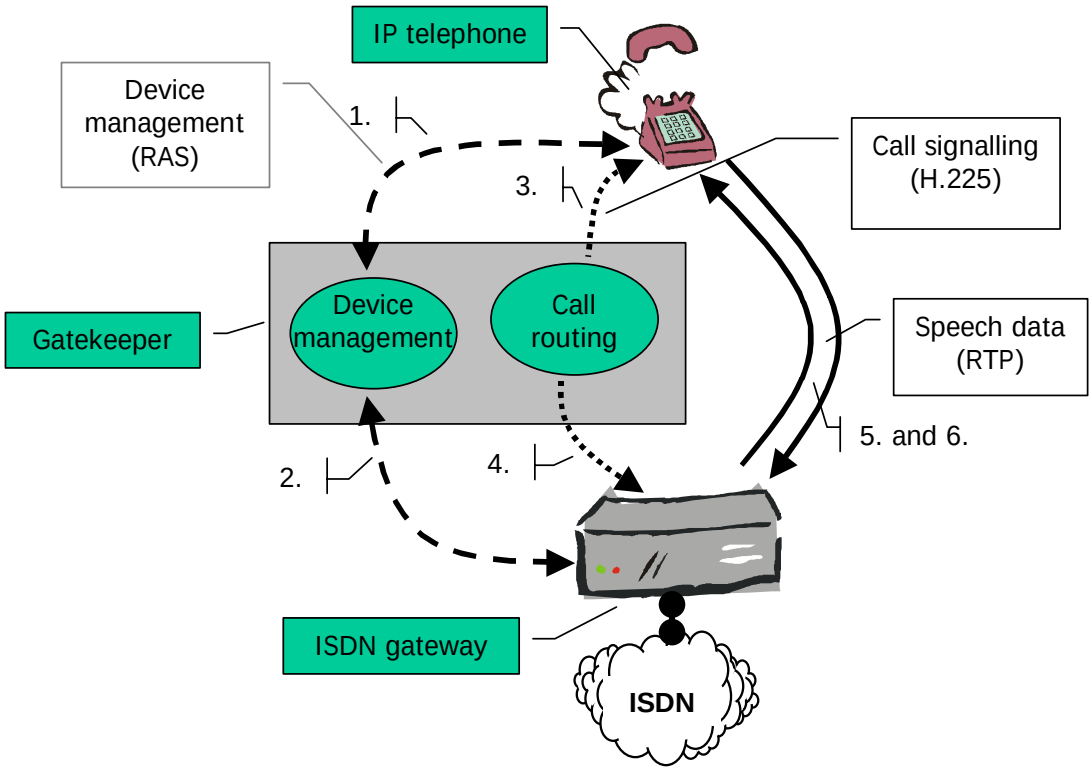


Figure 45 Call sequence with a gatekeeper and RAS shows a scenario with an IP telephone, an ISDN gateway and a gatekeeper. It is possible that the gatekeeper may be another innovaphone® gateway or, alternatively, it may be the gatekeeper contained in every innovaphone® gateway. For a clearer understanding though, the gatekeeper and ISDN gateway are depicted separately.

The separate steps involved in a call are described below[44].

- Both the IP telephone (1.) and the ISDN gateway (2.) register at the gatekeeper's device management. In the process they give their identification along with their current IP address. This step presupposes the RAS protocol and accordingly does not apply if operation is without the RAS protocol
- The IP telephone initiates a call (3.) and sets up a signalling connection to the gatekeeper
- The gatekeeper determines the call destination and sets up a signalling connection to the destination (4.). The IP telephone and gateway exchange their IP addresses. Further signalling between the two is done via the gatekeeper
- The IP telephone and ISDN gateway directly set up the two voice channels between one another (5. and 6.)

In fact, call source and call destination do not necessarily have to use the same gatekeeper. Figure 46 Call sequence with two gatekeepers and RAS shows the sequence for a call that is connected via two gatekeepers.

For the destination and source of the call, the sequence looks exactly the same as in Figure 45 Call sequence with a gatekeeper and RAS, with the more complex infrastructure fully concealed by the gatekeepers. The two gatekeepers now merely have to be known to one another. This again can be done via the RAS protocol with one gatekeeper registering at the other, or by reciprocal registering of both gatekeepers (step 1). The incoming call from the IP telephone is now routed by the first gatekeeper to the second, which in turn routes it to the destination gateway. In this way very complex structures can be set up with a number of gatekeepers.

The device management is configured in the configuration applet in the VOIP INTERFACES area.

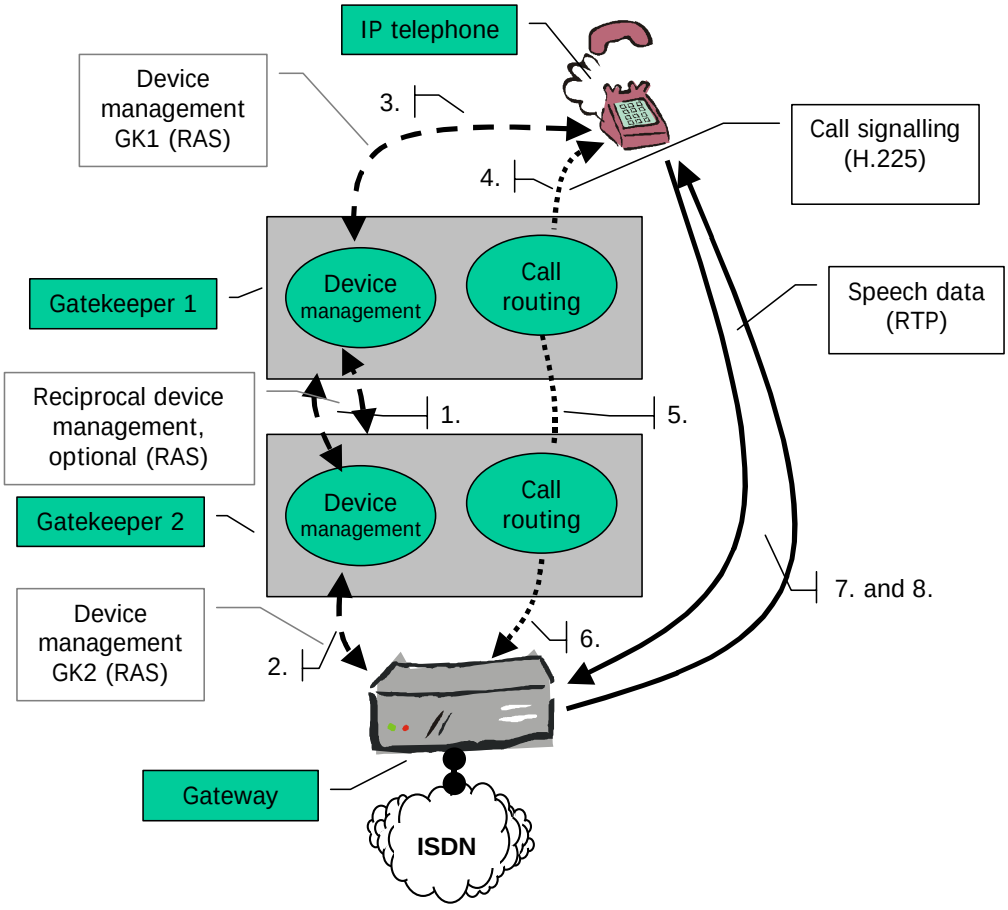
Device management is done dynamically via so-called Registration in the RAS[45] protocol. In this the registering device first of all determines the relevant

[44] in so far as they are meaningful in this connection. In fact the events can be far more complex.

[45] RAS comes from **R**egistration, **A**dmission and **S**tatus

gatekeeper. In this procedure, denoted as Gatekeeper discovery[46] , the terminal searches the network for a gatekeeper with the desired gatekeeper ID[47], a logical name for the gatekeeper. If the gatekeeper is found, the device transfers its identification[48] and IP address. If the identification is OK, the device is now ready for operation and accessible. Devices that log on with the gatekeeper using the RAS protocol are configured in GATEKEEPER CLIENT GROUP mode.

Figure 46 Call sequence with two gatekeepers and RAS



[46] Many gatekeepers and also many VoIP devices do not support the Discovery procedure. In this case the gatekeeper's IP address has to be configured in the device that is to log on. Likewise, multicasts of routers are not normally transmitted. This means that the IP address of the gatekeeper must also be recorded if it is cut off from the registering device by a router.

[47] A number of gatekeepers can be operated in a network and each found by "its" devices by means of the Gatekeeper Id. However, many third party gatekeepers do not support the Gatekeeper Id.

[48] Here this may be a logical name or a telephone number or both.

A number of VoIP devices do not support the RAS protocol. Such devices can nevertheless still be managed by configuring them statically (hence with fixed IP addresses) in the gatekeeper. Steps 1 and 2 then no longer apply in the sequence in Figure 45 Call sequence with a gatekeeper and RAS on page 101. Such devices are configured in GATEWAY or GATEWAY GROUP mode.

Of course your gateway can also register itself at another gatekeeper with the RAS protocol, as is the case in Figure 46 Call sequence with two gatekeepers and RAS on page 103. This mode of operation is configured in REGISTRATION AT GATEKEEPER AS ENDPOINT or REGISTRATION AT GATEKEEPER AS GATEWAY.

Gatekeeper Discovery

Gatekeeper discovery works via IP multicast packets, which a gatekeeper client sends out when it wants to find a suitable gatekeeper.

Normally, such packets are transmitted in the home LAN segment only and especially are not routed into other networks. Thus gatekeepers are to be found in the home LAN segment only. However, routers can be configured so as to transfer such packets onward according to certain rules. Through this it is also possible to find gatekeepers which are tied together via WAN links.

The differentiation is based on the so-called multicast addresses. The multicast address used with gatekeeper discovery is 224.0.1.41.

The Gatekeeper ID

Each gatekeeper in a network can be distinguished by its own Gatekeeper-ID. This ID allows the administrator to operate a number of gatekeepers in a network in parallel, in which every terminal device nevertheless ascertains the "correct" gatekeeper at gatekeeper discovery. The ID is defined directly in the VOIP INTERFACES area in the GATEKEEPER ID field.

Figure 47 Defining the Gatekeeper ID

If you have assigned a gatekeeper ID to your gateway, it will then answer only such RAS Discovery inquiries, in which either this ID or no gatekeeper ID at all is listed. Even if your terminal equipment has permanently configured the gatekeeper, and thus carries out no gatekeeper discovery, the RAS registrations will only be accepted if again configured into them is the correct Gatekeeper ID or none at all.

If a Gatekeeper ID is configured, then this applies for the entire gateway.

If only one gatekeeper is operated in your network or if no gatekeeper discovery is used, it generally suffices to work without a Gatekeeper ID.

H.323 protocol options

With regard to communication with other VoIP devices, your gateway supports a series of protocol options, which affect certain details of its behaviour. These options are available independent of the GATEWAY MODE used.

Table 18 H.323 protocol options

Option	Meaning
FASTSTART	The H245 Faststart procedure is authorised. Outgoing calls are implemented with Faststart, incoming calls with Faststart are answered with Faststart. If this option is deactivated, outgoing calls will be implemented without Faststart and incoming calls, with or without Faststart, will be answered without Faststart. This option is always to be recommended, unless

Option	Meaning
	compatibility problems arise with third-party products.
H245-TUNNELING	The negotiation of the voice data connection is carried out in the already available TCP signalling connection[49]. Otherwise a separate own TCP connection is set up for this negotiation. This applies for the signalling connection leading out of the gatekeeper. This saves having a separate negotiation connection, which can be advantageous in connection with NAT and Firewalls. This option is always to be recommended, unless compatibility problems arise with third-party products.
ENABLE T.38 FAX PROTOCOL	Voice connections via which a fax is transferred, are transmitted using the special Fax over IP protocol T.38. Otherwise fax transmissions are not handled separately. This option is always to be recommended, unless compatibility problems arise with third-party products.
FAKE CONNECT[50]	With this the calling end is signalled a connection set-up as soon as in-band information is received from the called end, even though no connection has yet been established. Calling tones or network fault announcements may be of concern here. Some VoIP devices only switch through the voice channel when a connection has been established. In such cases, announcements occurring before this cannot be heard by the caller. This option resolves this problem. Use this option only for VoIP devices that exhibit this problem.
SUPPRESS SENDING OF HLC	Suppresses the sending of so-called high layer compatibility (HLC) information elements. This is necessary in the event that the receiving VoIP device responds erroneously to HLCs. Otherwise the HLCs are forwarded transparently by the gatekeeper. Use this option only if a VoIP device with this kind of fault needs to be operated. In particular do not use this option

[49] Technically, no specific TCP connection will be set up for the H.245 protocol: the H.225 TCP connection will be used.

[50] In earlier versions this option was called EARLY CONNECT.

Option	Meaning
	when linking PABXs via innovaphone® gateways, since under certain circumstances important information may be lost.
SUPPRESS SENDING OF FTY	Suppresses the sending of so-called facility (FTY) messages. This is necessary in the event that the receiving VoIP device responds erroneously to FTYs. Otherwise the FTYs are forwarded transparently by the gatekeeper. Use this option only if a VoIP device with this kind of fault needs to be operated. In particular do not use this option when linking PABXs via innovaphone® gateways, since under certain circumstances important information may be lost.
GENERATE CONNECTED TIME	Causes the gatekeeper to insert a timestamp with the local gateway time in outgoing Connect messages. Use this option if the called VoIP devices are dependent on the timestamp and the call sources (e.g. the ISDN network) do not supply one

Voice transmission

Your gateway supports various methods of voice transmission in IP. You make the relevant definitions in the CODEC CONFIGURATION area for calls between an ISDN interface of your gateway and a VoIP device that is defined through this VoIP interface. Keep in mind that calls between two VoIP devices, i.e. from IP to IP, do not take account of this setting, since the negotiation of parameters takes place directly between the terminal devices and thus governs their configuration.

Voice encoding

Speech can be transmitted in various codings. Some of the available codings compress the speech, while others don't. Your gateway supports several of the common voice encoding schemes whose properties are described in the table below:

Table 19 Voice encoding schemes

Encoding	Bandwidth[51] per call	Min. delay[52]	Properties
G.711A	64kbps	20 ms	No compression, best voice quality (comparable to digital phone lines). Sound digitisation using European coding
G.711U	64kbps	20 ms	As above, US coding used[53]
G.726-16 G.726-24 G.726-32 G.726-40	16, 24, 32, 40kbps	20 ms	Intended for fax and modem data in exceptional cases only
G0.723-53	5.3kbps	30 ms	Good voice quality (comparable to analogue phone lines)
G0.723-63	6.3kbps	30 ms	Slightly better voice quality than G.723-53 with minimally greater bandwidth
G.729A	8kbps	20 ms	Best voice quality of all compression algorithms, allows minimal delay

You define the type of voice data compression in the STANDARD field. This setting is used preferentially. However if the remote VoIP device does not support the selected encoding, a commonly supported one is negotiated. Activate (check) the EXCLUSIVE checkbox if you want to force the use of the selected encoding[54].

The best trade-off between voice quality and required bandwidth is offered by G.729. Select this form of coding for remote telephony gateways that you reach via the Internet, your intranet or heavily loaded local area networks. In high-performance local area networks you should use G.711, to ensure best voice quality. You need G.723.1 for links to telephony gateways that do not support the G.729 standard. G.726 codings should be used only in cases where fax data is to be transmitted on a connection without T.38.

[51] The stated bandwidth is merely the nominal bandwidth of the encoding algorithm. Further control information accompanies the transmission of the compressed data in the network, so, depending on the configuration, the total bandwidth required may turn out to be significantly higher.

[52] Here "Delay" is understood to mean that which minimally arises through the data encoding and packet assembly. Further delays arise in connection with the transmission of the data in networks.

[53] You can use both µ-law and A-law encoding, totally independent of the particular encoding that is used on your ISDN connection. The encoding will be correctly adapted in each case on the ISDN connection.

[54] Which can of course lead to call failure if your gateway and the remote VoIP device do not support a common Coder.

Packet size

Under PACKETSIZE (MS) you specify the size of packet used for exchanging coded voice data between telephony gateways. The value you enter into the field defines the amount of time voice data is collected prior to transmission of a voice information packet. This duration causes a corresponding delay in the voice transmission. A value of 30ms is perceived by the human ear as practically immediate, whilst a value of 100ms is also not considered to be an irritation by most users.

Larger packets cause a greater delay in voice data transmission (Delay), but cause less loading on the network as the Overhead involved in transporting packets in the network is lower.

Keep in mind, that the transport overhead grows significantly with reduced Packetsize, since the per-packet transport overhead (IP protocol in LAN and additionally PPP protocol in WAN) remains the same while the voice data payload becomes less. The effective bandwidth required is therefore significantly higher (depending on the packet size) than the theoretical voice data bandwidth required by the coding algorithm indicated in Table 19 above.

If insufficient bandwidth or excessive network delay times mean voice data can no longer be transmitted quickly enough, this becomes apparent through extraneous (crackling) sounds or greatly increased delays. In such a case, you should increase the packet size for the telephony gateway concerned to alleviate the effect, or change to a more efficient coding scheme (for example, change from G.729 to G.723-53). Table 20 “Required bandwidths depending on the packet size” below shows the bandwidths required depending on the coding scheme and packet size.

Table 20 Required bandwidths depending on the packet size

Coding scheme	Effective bandwidth used (in kbps) related to packet sizes of				
	20 ms	30 ms	60 ms	90 ms	150 ms
	Possible concurrent calls on a 64kbps link				
G0.711	83 kbit/s	77 kbps	70 kbps	68 kbps	67 kbps
G0.723-53	24 kbps	18 kbps	12 kbps	9 kbps	8 kbps
	2	3	5	6	8
G0.723-63	25 kbps	19 kbps	13 kbps	10 kbps	9 kbps
	2	3	5	6	7
	27 kbps	21 kbps	14 kbps	12 kbps	11 kbps

Coding scheme	Effective bandwidth used (in kbps) related to packet sizes of				
	20 ms	30 ms	60 ms	90 ms	150 ms
	Possible concurrent calls on a 64kbps link				
G0.729	27 kbps	21 kbps	14 kbps	12 kbps	11 kbps
G.728	2	3	4	5	6
G.729	19 kbps at 120ms[55]				
	3				
G.726-24	27 kbit/s at 150ms[55]				
	2				
G.726-32	35 kbit/s at 150ms[55]				
	1				
G.726-40	43 kbit/s at 150ms[55]				
	1				
	14 kbps at 120ms[56]				
	4				

The values stated here are approximate values[57] since a precise determination of the required bandwidth depends on a number of factors. You can arrange a precise calculation for various application scenarios under: http://www.innovaphone.com/ibc.htm.

A further option for saving bandwidth consists in not transmitting any data during breaks in speech. Since only one party normally speaks at a time during a call, considerable bandwidth can be saved in this way. This function is known as SILENCE COMPRESSION and can usually be activated without any loss of quality.

At the end that is actively talking, absolute silence from the other end can be an irritation, with users often assuming that the connection has gone dead if nothing is heard from the partner in conversation. To avoid this, an artificial

[55] The G.726 codings work permanently with a packet size of 120ms regardless of the PACKETSIZE setting.

[56] Fax transmissions in the T.38 protocol work permanently with a packet size of 150ms. Strictly speaking the fax data is not compressed, the Overhead arising in the analogue transmission merely does not apply.

[57] The effective bandwidth required can vary according to conditions in the given environment. Firstly, routers used in the transmission link may employ special compression techniques (RTP Header Compression) and thus reduce the bandwidth required. And secondly, switching off the voice channels during breaks in speech similarly leads to a reduced bandwidth requirement. The values specified in the table represent the most unfavourable value with transmission over long-distance routes (PPP).

Please note though that the values stated apply per direction. The overall values for a call without silence compression are thus twice as great. Bandwidths of communications media are normally stated for each direction though anyway. Thus an ISDN connection has 64kbps per direction, so that the data in the table are intuitively comparable with the familiar bandwidths.

background noise is fed in at this end, so-called comfort noise. In order to periodically match the volume of this simulated background sound to the actual background sounds of the momentarily silent end, information is exchanged about this at regular intervals. These so-called comfort noise updates still require significantly less bandwidth than the saving through silence compression. SILENCE COMPRESSION and SEND COMFORT NOISE UPDATES should therefore be activated together and only deactivated if compatibility problems arise through third-party devices.

Defining the VoIP tracing Level

By setting the tracing level you can define for which subject areas your gateway records traces. This is done in the VOIP INTERFACES field.

Figure 48 Defining the VoIP trace level

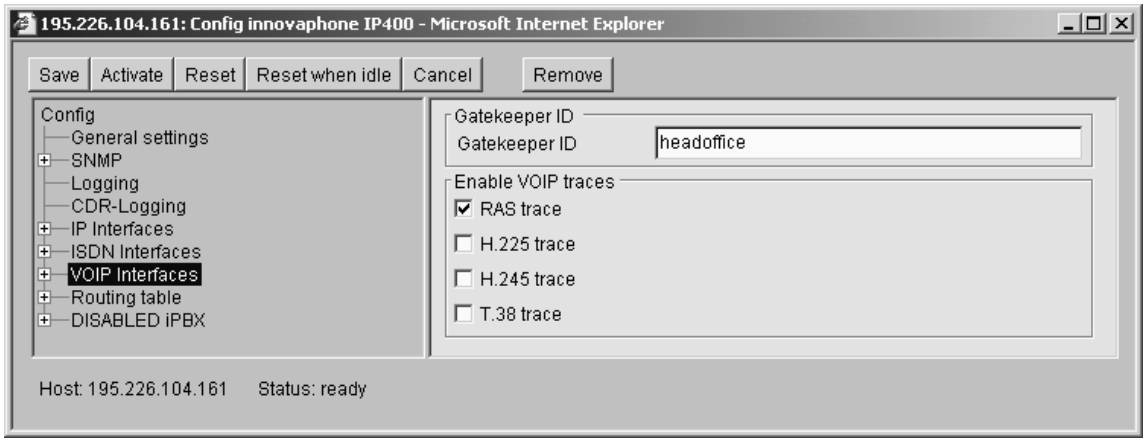


Table 21 VoIP Tracing level

Setting	Effect
RAS TRACE	Logging of the device management protocol
H.225 TRACE	Logging of the call signalling protocol
H.245 TRACE	Logging of the media channel protocol
T.38 TRACE	Fax transmission protocol

The logging of traces does not give rise to any performance problems since the entries are merely written to a special buffer in your device's main memory. A ring buffer is used here though, so new messages overwrite older ones. It may therefore be useful to mask out certain uninteresting aspects to obtain a complete trace for a particular problematic situation.

Management of VoIP devices by RAS (Gatekeeper)

Management of VoIP devices in your gateway using the RAS protocol is the recommended method of device management.

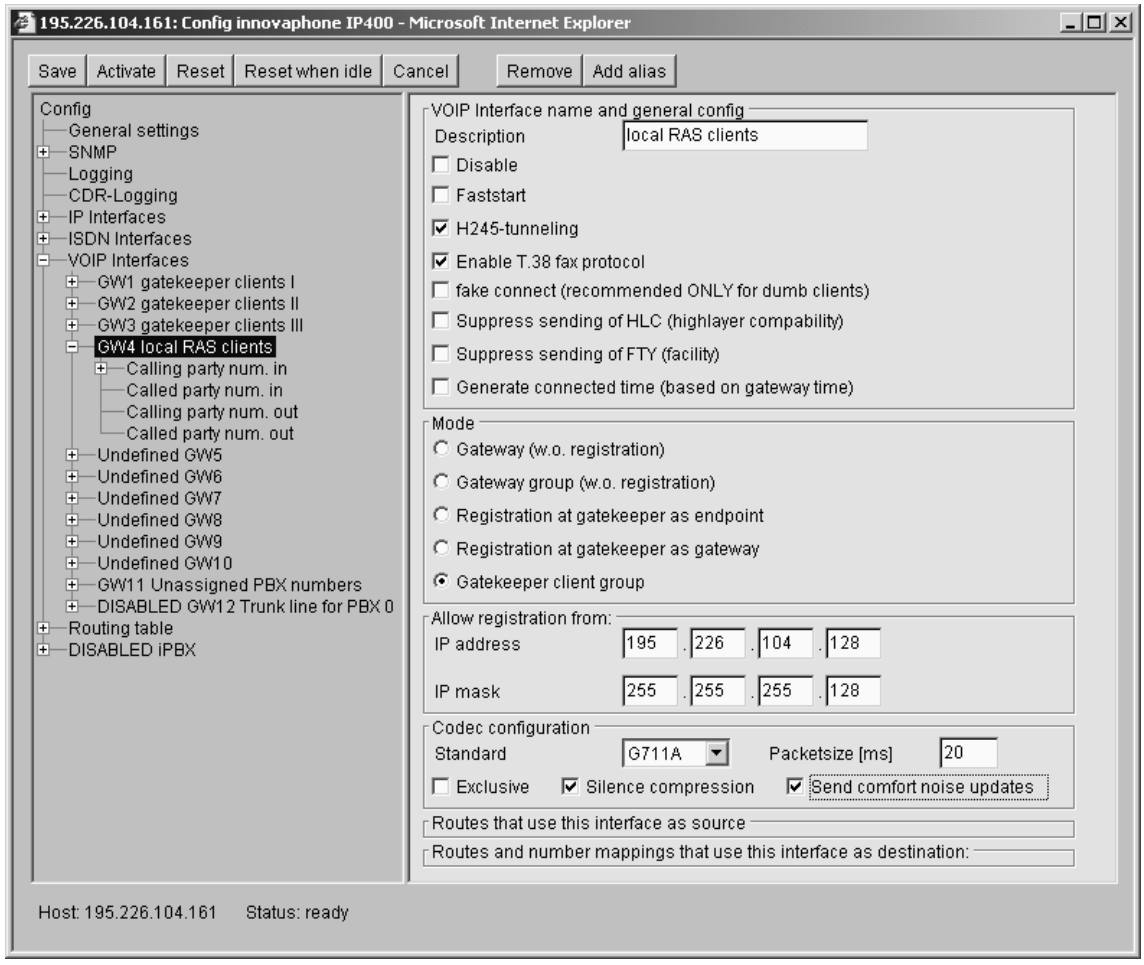
- If necessary define a Gatekeeper ID (refer to section "The Gatekeeper ID" starting page 104)
- To define the VoIP devices that are to be managed by the gatekeeper, set up a definition in mode GATEKEEPER CLIENT GROUP in the VOIP INTERFACES area under GW1 to GW12.

  If necessary, restrict the access of VoIP devices to your gateway. For this, under IP ADDRESS enter the network address of the IP network in which the authorised devices are located. Set up the network mask for the network under IP MASK.

  In this way you are able to define the sphere of authorised VoIP devices in any desired manner. In doing so, it is not necessary for the configured network to be an actual existing network. In this way you are able to define the sphere of authorised VoIP devices in any desired manner. In doing so, it is not necessary for the configured network to be an actual existing network. Figure 57 shows a definition that allows access by all VoIP devices

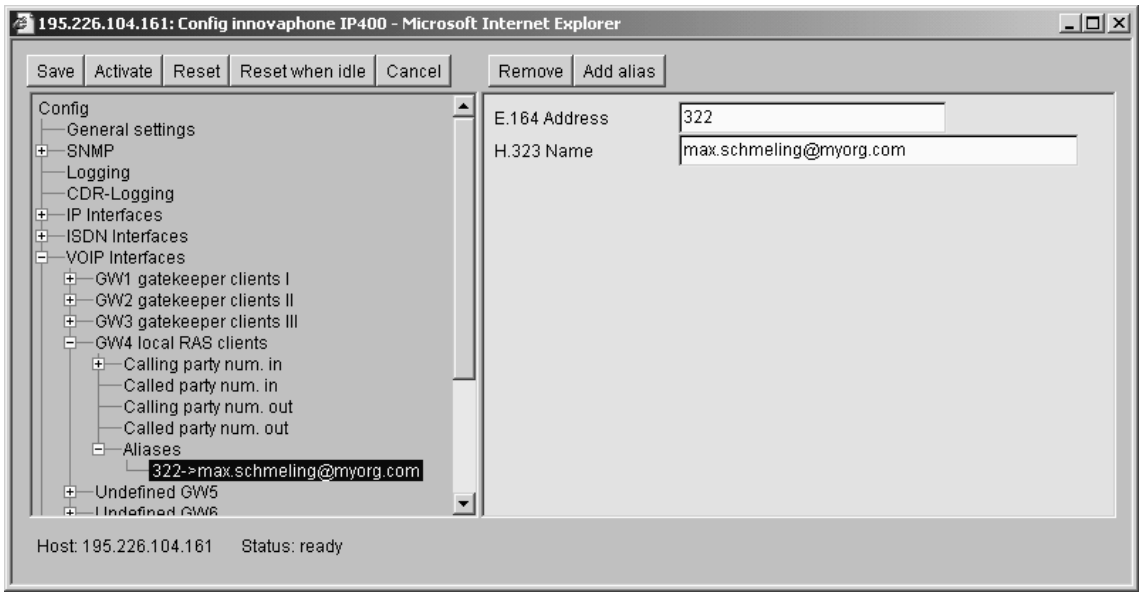
  to 120 show a definition that allows access by all VoIP devices.
- Define the H.323 protocol options for the VoIP devices to be managed (see page 105 onwards)
- Create an alias entry for every VoIP device. This is done by clicking on the ADD ALIAS button.

Figure 49 Configuration of VoIP devices registered through RAS



Here, for VoIP end points you should define the assigned direct dialling number or MSN as E.164 ADDRESS and also the name as H.323 NAME. For VoIP gateways it is sufficient to define the name.

Figure 50 Entries of a VoIP device

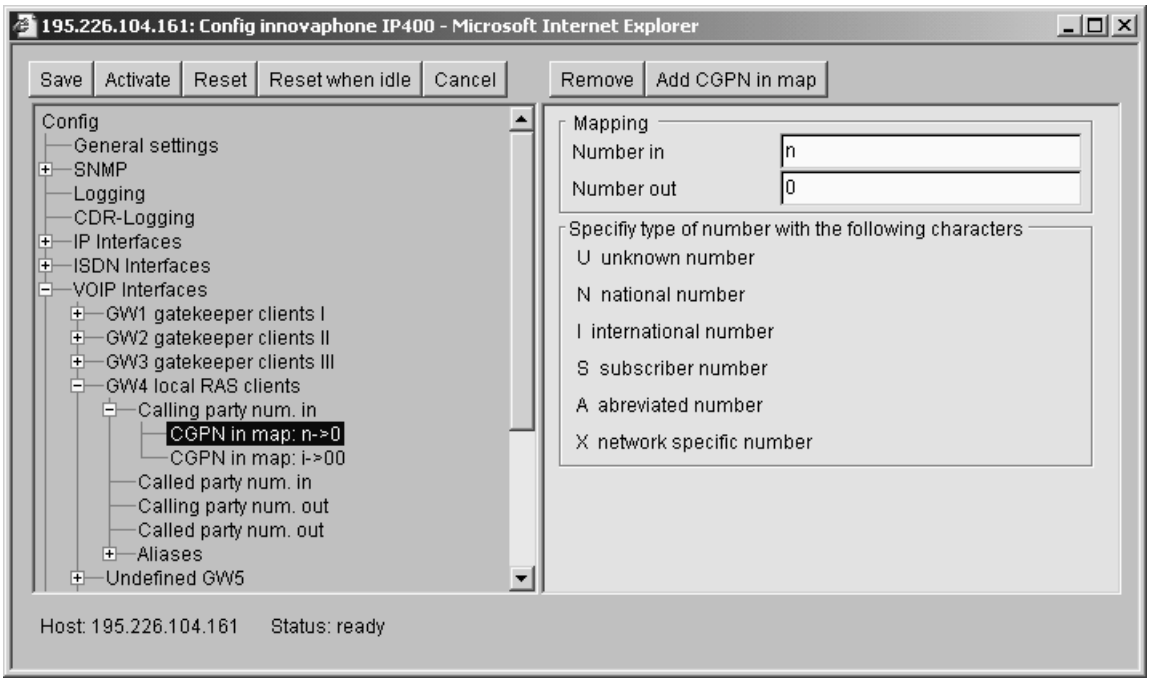


Please note that in all cases it suffices if the VoIP device registers with its name. In general, checking is done when registration occurs to see that the details contained in the registration match a configured Alias entry. If details are omitted at the registrations (the E.164 address for instance) they are not checked for this. Thus a terminal device can register with just its name, and its direct dialling number can thereby be defined solely in the gatekeeper, recorded in the alias entry with matching name and corresponding number. However if the terminal device registers with name and number, the number cannot be changed on its own in the gatekeeper, since the terminal would log on with the incorrect E.164 ADDRESS after a change.

If a VoIP device registers I with several H.323 aliases simultaneously, each separate one is checked against the one defined in its gatekeeper and the registration is done only if all aliases are defined.

▲ Should call number handling require adaptation (see page 87 onwards) then make the relevant settings by adding the appropriate entries to the CALLING / CALLED PARTY NUM. IN / OUT areas using the ADD CGPN / CDPN IN / OUT MAP button

Figure 51 Defining the interface-related number replacements



▲ If the configured VoIP devices are also to have access to ISDN interfaces of your gateway, define the voice transmission parameters (see from page 107 onwards)

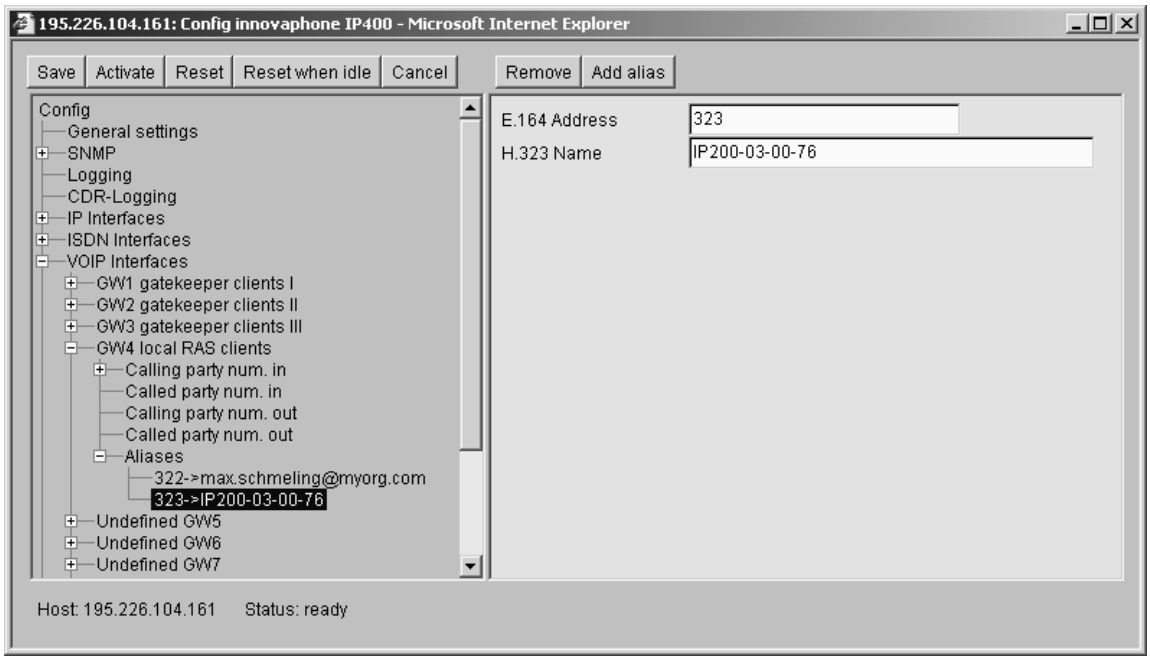
Special features in the configuration of innovaphone® devices

The innovaphone devices provide the option for registration based on their serial number. This always takes place when they are configured for use on a gatekeeper but no alias name is configured in the profile. In this case the tiptel innovaphone® 200, for example, tries to register with H.323 NAME IP200-03-***XX-XX***, where ***XX-XX*** is derived from the last four digits of the IP telephone's serial number. This allows all IP telephones to be operated with absolutely identical configuration[58].

[58] Please note that terminals that are managed with the optional iPBX components must not be configured in the VOIP INTERFACES field.

- ▲ Create an appropriate Alias entry in the gatekeeper. The serial number is entered in the H.323 NAME field and the telephone's direct dialling number is defined in the E.164 ADDRESS field.
- ▲ If the IP telephone is also to be assigned a "descriptive" name, set up a further alias text-wise with the same direct dialling number in front of the serial number alias. Enter the desired name as H.323 NAME.

Figure 52 Configuring IP 200 IP telephones

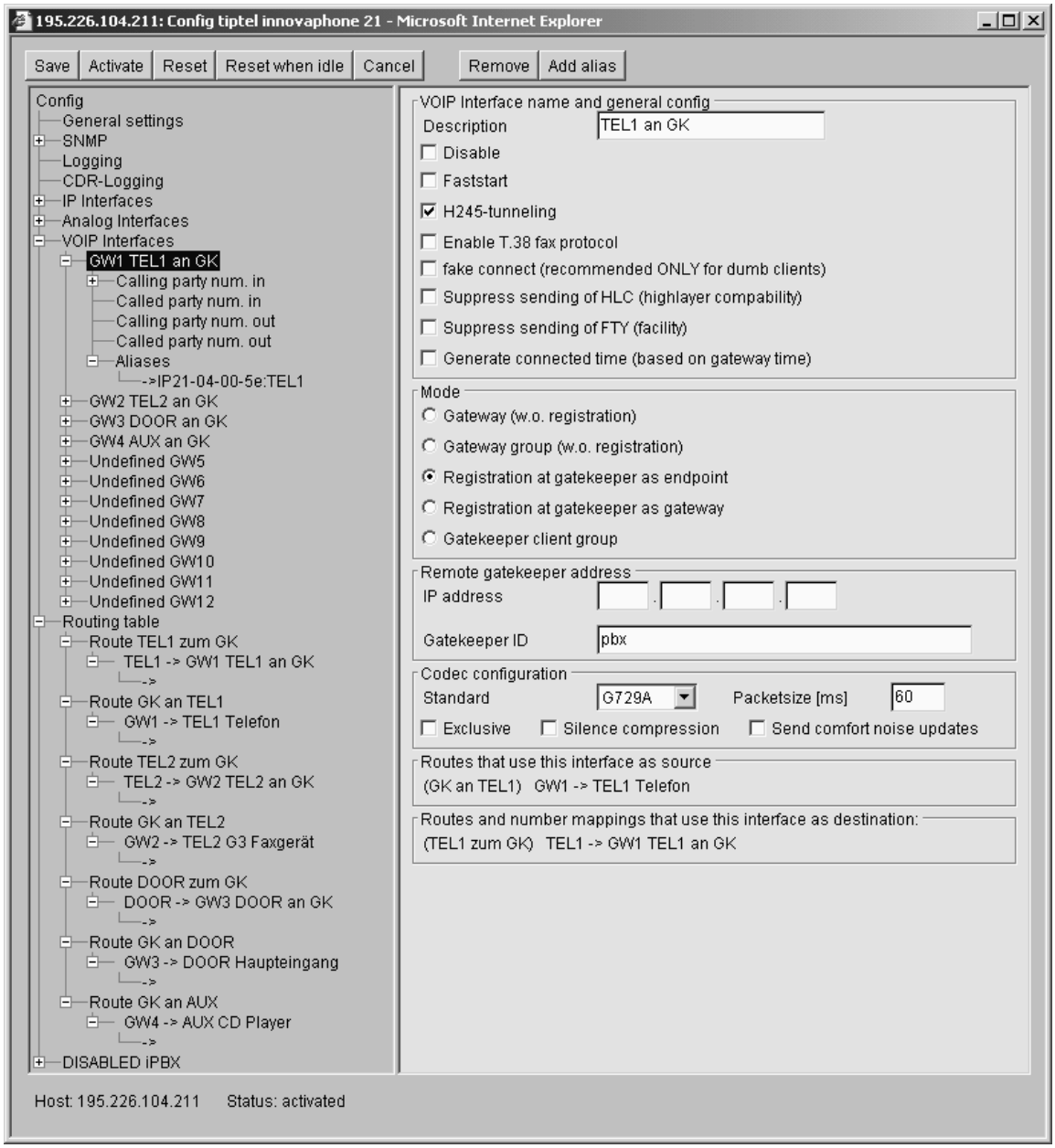


To be able to use all performance characteristics however, terminal devices should be managed with the optional iPBX components.

Registration of the interfaces of an IP 21

The IP 21 can, like the IP 400 or IP 3000, be used as a full-featured gateway, gatekeeper and iPBX. It is often desirable, however, to use the IP 21 simply like a set of terminal devices and register these terminal devices with a gatekeeper.

Figure 53 Registering IP 21 interfaces



Let us assume that an analogue telephone, a fax machine, a door intercom and a music source are connected to the IP 21. These 4 devices should be registered with a gatekeeper as independent terminals, so that the existence of the IP 21 remains hidden from the gatekeeper. From the point of view of the gatekeeper, each is in all three cases a registered H323 terminal device.

To register the individual interfaces of the IP 21 with a gatekeeper, proceed as follows:

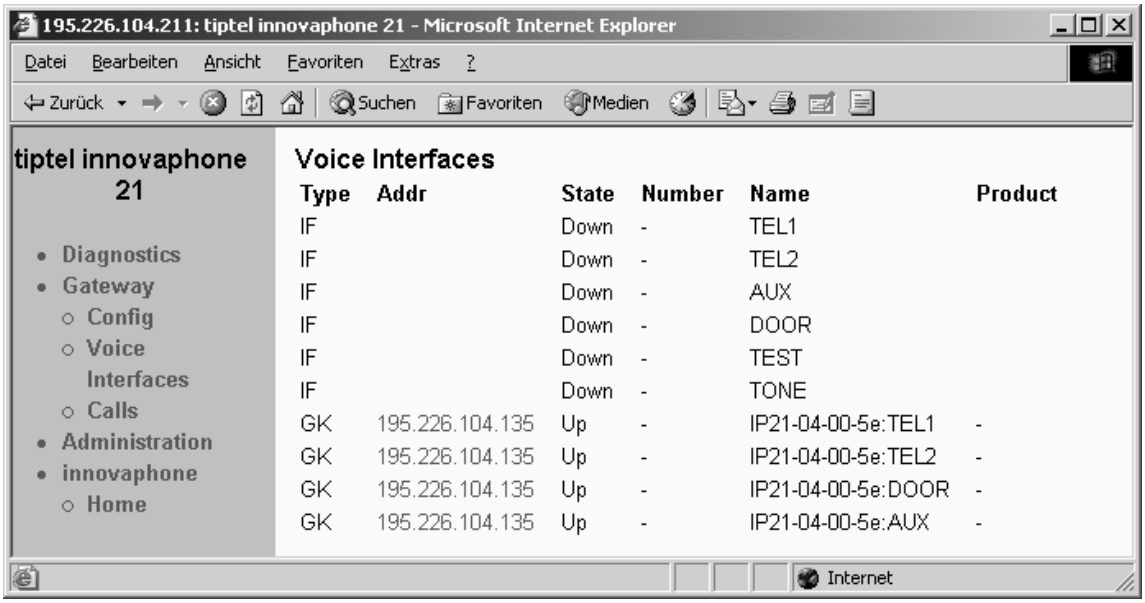
▲ Set up a gateway definition for each interface used in REGISTRATION AT GATEKEEPER AS ENDPOINT mode (see page 122f)

▲ Use a different alias for each gateway definition[59]

Set up routes between gatekeeper and interfaces (see To be able to use all performance characteristics however, terminal devices should be managed with the optional iPBX components.

▲ on page 116)

Figure 54 Registration status of the IP 21 interfaces with the gatekeeper



The individual IP 21 interfaces and the devices connected to them are now each individually registered with the gatekeeper. This allows each device to be configured independently of the others in the gatekeeper[60].

Figure 54 above above indicates the registration status of the interfaces of an IP 21 with a gatekeeper. Please note that, although all interfaces of the IP 21 can be registered with the gatekeeper, it is only possible to make as many simultaneous calls as there are DSP channels installed (see Figure 92 The browser administration interface on page 165).

[59] It is practical to use the serial number followed by the interface description, e.g., IP21-04-00-00:TEL2. Note that the automatic registration as described on page 115 does not work since all gateway definitions need to work with different aliases.

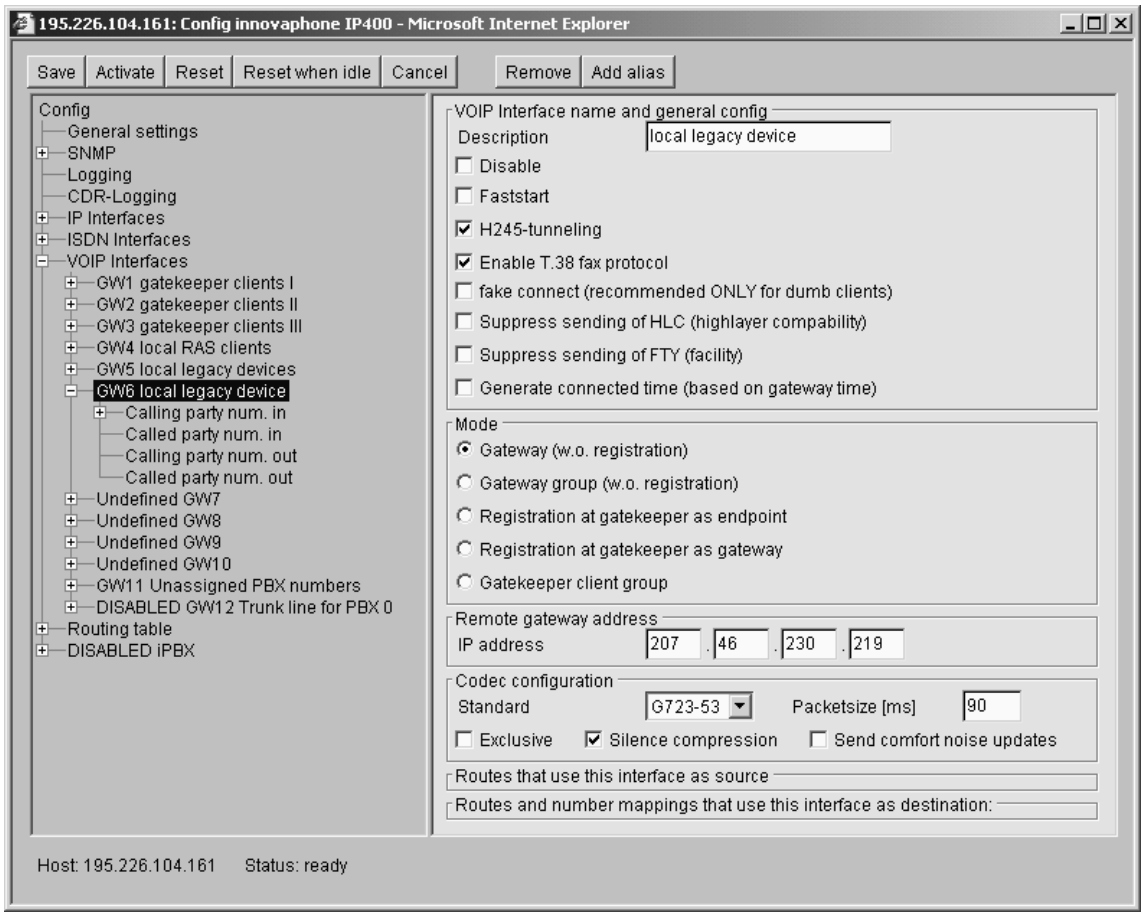
[60] This means, for example, that each terminal can be assigned its own number that is independent of all the others.

Static management of VoIP devices

If you are working with VoIP devices that do not support any dynamic registration using the RAS protocol, you have to configure the devices statically. As a consequence, the continuous checking as to whether the devices are accessible no longer applies and there is no possibility of working with variable IP addresses (i.e. with DHCP, for example). Other disadvantages do not arise though.

You can configure the VoIP devices individually or in groups. This is particularly useful in cases where a large number of VoIP clients is used that do not support any RAS.

Figure 55 Definition of an individual VoIP device



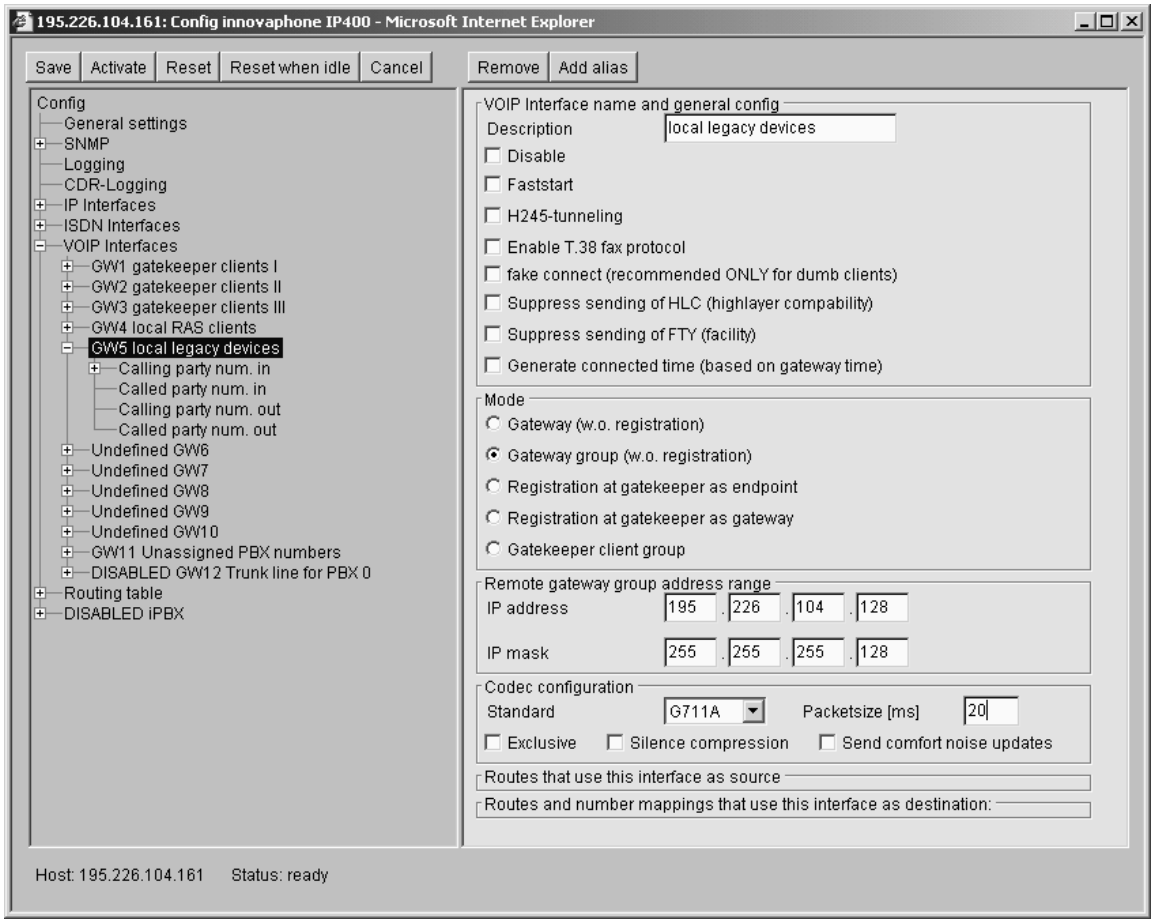
▲ To define a single VoIP device that is to be managed statically, in the VOIP INTERFACES area under GW1 to GW12 set up a definition in the GATEWAY mode

or

To define a group of VoIP devices that are to be managed statically, set up in the VoIP INTERFACES area under GW1 to GW12 a definition in the GATEWAY GROUP mode. With this you allow access to all VoIP devices located in an IP network. Proceed carefully though when setting up such gateway groups and make certain that you prevent access by unwanted devices (e.g. such as those from the Internet trying to gain access to your gateway).

▲ For a single VoIP device you enter its IP address under IP ADDRESS

Figure 56 Definition of a VoIP device group



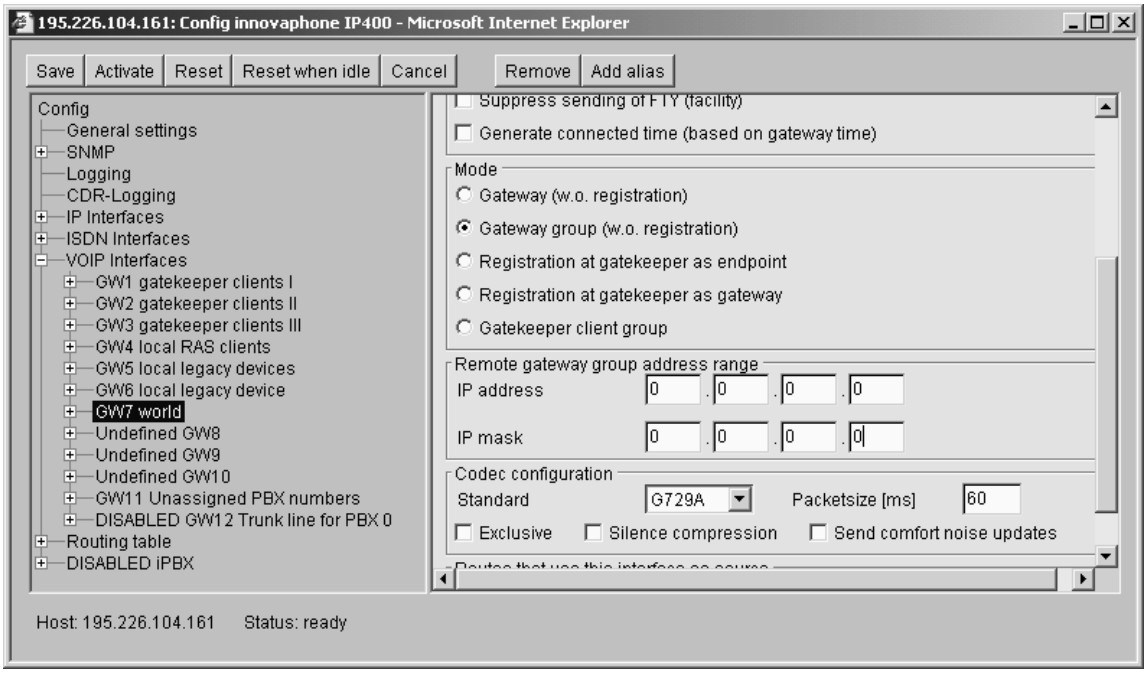
or

For a group of VoIP devices, under IP ADDRESS enter the network address of the IP network in which the authorised devices are located. Set up the network mask for the network under IP MASK.

In this way you are able to define the sphere of authorised VoIP devices in any desired manner. In doing so, it is not necessary for the configured

network to be an actual existing network. Figure 57 shows a definition that allows access by all VoIP devices

Figure 57 Authorising all VoIP devices



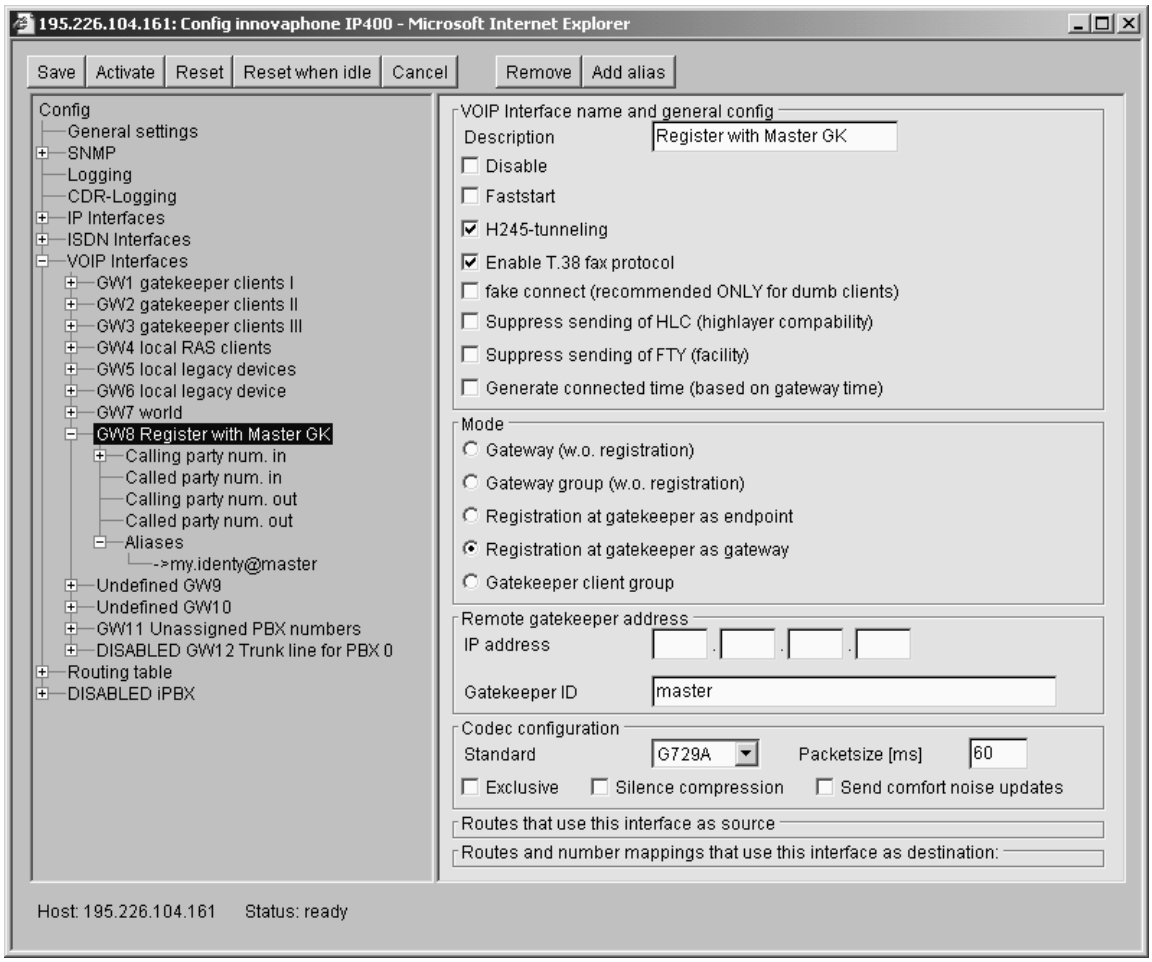
- ▲ Define the H.323 protocol options for the VoIP devices to be managed (see page 105 onwards)
- ▲ Should call number handling require adaptation (see page 87 onwards), then make the relevant settings by adding the appropriate entries to the CALLING / CALLED PARTY NUM. IN / OUT areas using the ADD CGPN / CDPN IN / OUT MAP button (refer to Figure 51 Defining the interface-related number replacements on page 115)
- ▲ If the configured VoIP devices are also to have access to ISDN interfaces of your gateway, define the voice transmission parameters (see from page 107 onwards)

Registering the gateway at another gatekeeper

If your gateway (or the gatekeeper contained therein) has to register at another gatekeeper as, for instance, is the case in the scenario shown in Figure 46 Call sequence with two gatekeepers and RAS on page 103, this can be done using a gateway definition in the REGISTER AT GATEKEEPER AS GATEWAY mode. This registers your gateway as a VoIP gateway (see page 99). This is the correct mode in most cases. However, should the gatekeeper at which the registration is to take place allow only the registration of a VoIP end point, use the REGISTER AT GATEKEEPER AS ENDPOINT mode. If the external gatekeeper on the other hand is an innovaphone® gateway, the behaviour is identical in both modes.

- To register at a gatekeeper, in the VOIP INTERFACES area under GW1 to GW12 set up a definition in the REGISTER AT GATEKEEPER AS GATEWAY or REGISTER AT GATEKEEPER AS ENDPOINT mode.
- If the determination of the gatekeeper is to be done using Gatekeeper Discovery (see page 104), you can leave the IP ADDRESS field blank. Otherwise enter the IP address of the gatekeeper there.
- If the gatekeeper works with a gatekeeper id, (see page 104) enter this in the GATEKEEPER ID field
- By clicking on the ADD ALIAS button define the H.323 Alias with which you have to identify yourself at the gatekeeper. Normally it makes the most sense if the gateway registers only with an H.323 name and not with an E.164 address (i.e. with a telephone number). With many gatekeepers this is obligatory though. Take note ,therefore, of the documentation for the gatekeeper at which you want to register
- Define the L H.323 protocol options for communication with the gatekeeper (see page 105 onwards)

Figure 58 Registering at another gatekeeper



- ▲ Should call number handling require adaptation (see page 87 onwards), then make the relevant settings by adding the appropriate entries to the CALLING / CALLED PARTY NUM. IN / OUT areas using the ADD CGPN / CDPN IN / OUT MAP button (refer to Figure 51 Defining the interface-related number replacements on page 115)
- ▲ If calls from external gatekeepers are also to have access to ISDN interfaces of your gateway, define the voice transmission parameters (see from page 107 onwards)

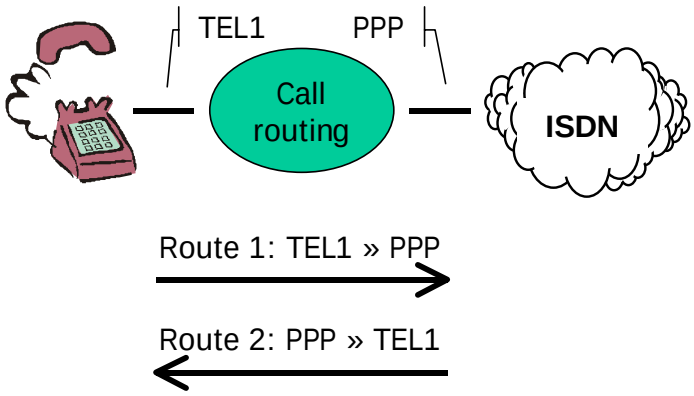
Configuring the call routing

Call routing is at the heart of gateway, determining which calls are accepted by the gateway and where they will be routed to.

General considerations for configuring the call routing

Call routing is undertaken by the gatekeeper of your gateway. It is controlled by so-called Routes[61]. Here, each route defines a permitted path of a call from the interface at which the call arrives to the interface at which the call goes out again. Here, the interface concerned may be either an ISDN interface (whose configuration is described from page 65 onwards) or a VoIP interface (see page 99 onwards).

Figure 59 Unidirectional routes



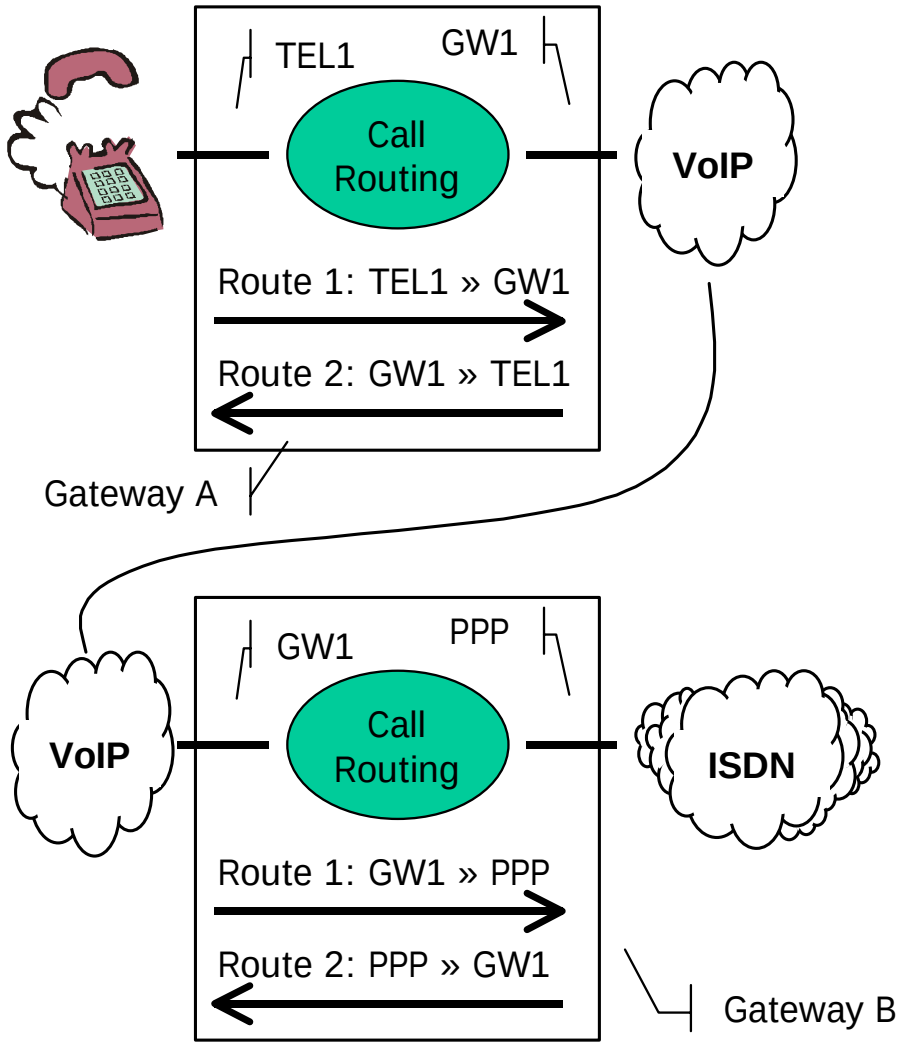
A route always defines one call direction only. Thus two routes are necessary if calls are to be possible between two interfaces in both directions, one for each direction.

[61] Here the routes concerned are voice routes, not to be confused with data or IP routes described from page 57 onwards.

Routes define the call routing within a single gateway. Should a call need to be routed through two gateways, a separate route is required in each gateway. If the calls are to be possible in both directions then four routes are required in total.

Figure 60 Routes via 2 gateways shows a scenario, in which calls are routed via VoIP between a telephone connected to gateway A and the ISDN network connected to gateway B.

Figure 60 Routes via 2 gateways

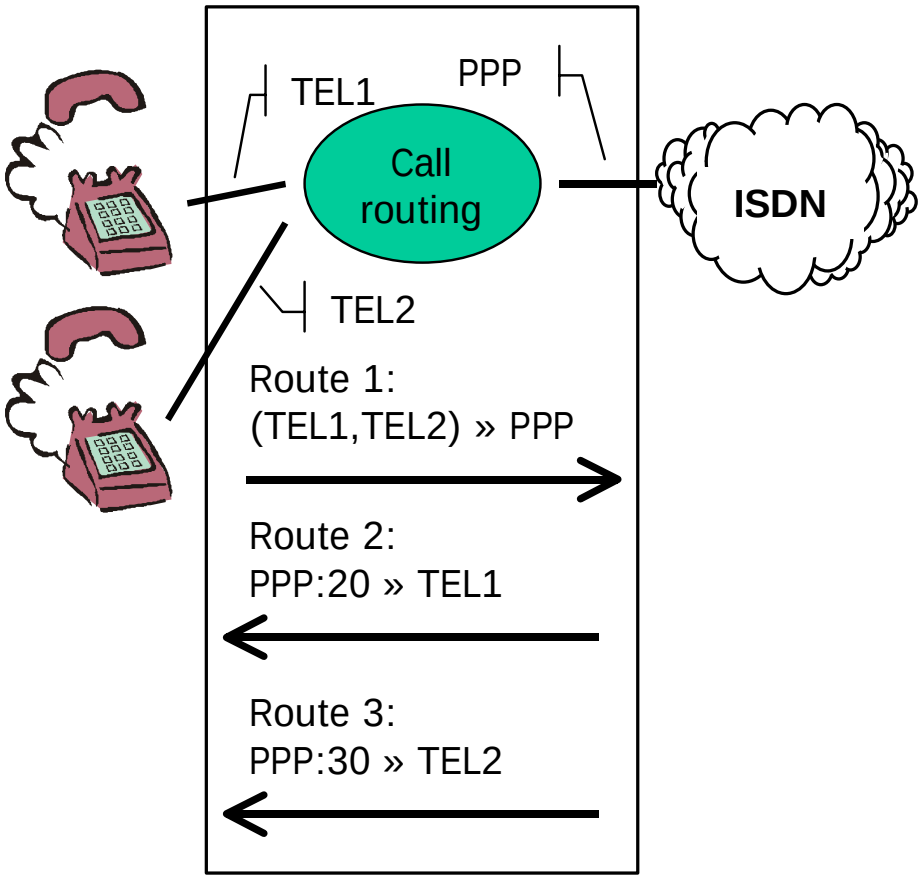


The type of call is of no relevance to the call routing. In principle, any call can be forwarded to any given interface. Thus, for instance:

- A call from your telephone via the network provider's fixed network is routed from the gateway's ISDN interface to which your ISDN telephone is attached to the ISDN interface the corresponding trunk line is connected to.
- For a call from a remote telephony gateway to your ISDN telephone, an incoming call on a VoIP interface of the gateway is put through to the ISDN interface to which your ISDN telephone is attached.

Calls from different interfaces are often handled in the same way. In the scenario shown in Figure 59 Unidirectional routes it may, for example, be desirable to allow calls from both TEL1 and TEL2. Therefore a number of interfaces can be specified as allowed sources for a route.

Figure 61 Call number dependent routes

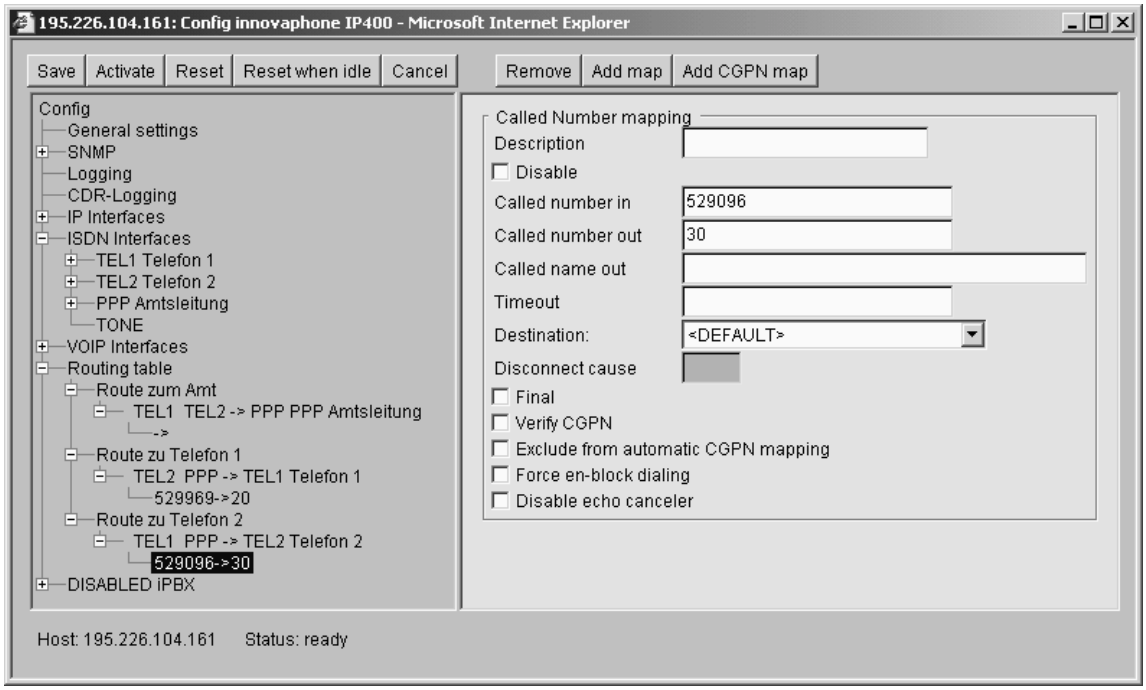


Of course the call routing often also depends on the call numbers dialled. Thus it is necessary to define the validity of routes for calls with certain destination call numbers. This is done by attaching a so-called Map entry to the route for every valid common dial prefix. Each map entry thus defines that calls from the source interfaces specified in the route, which start with the digit combination specified in the map, can be connected to the destination interface defined in

the route. Figure 61 Call number dependent routes shows a corresponding scenario.

It is sometimes useful to modify the called number in the course of the call routing. Figure 62 Routes with call number replacement shows the configuration of such a scenario in the configuration applet of your gateway. There the MSNs (529969 and 529096) assigned to a point to multipoint connection are mapped onto the internal direct dialling numbers 20 and 30.

Figure 62 Routes with call number replacement

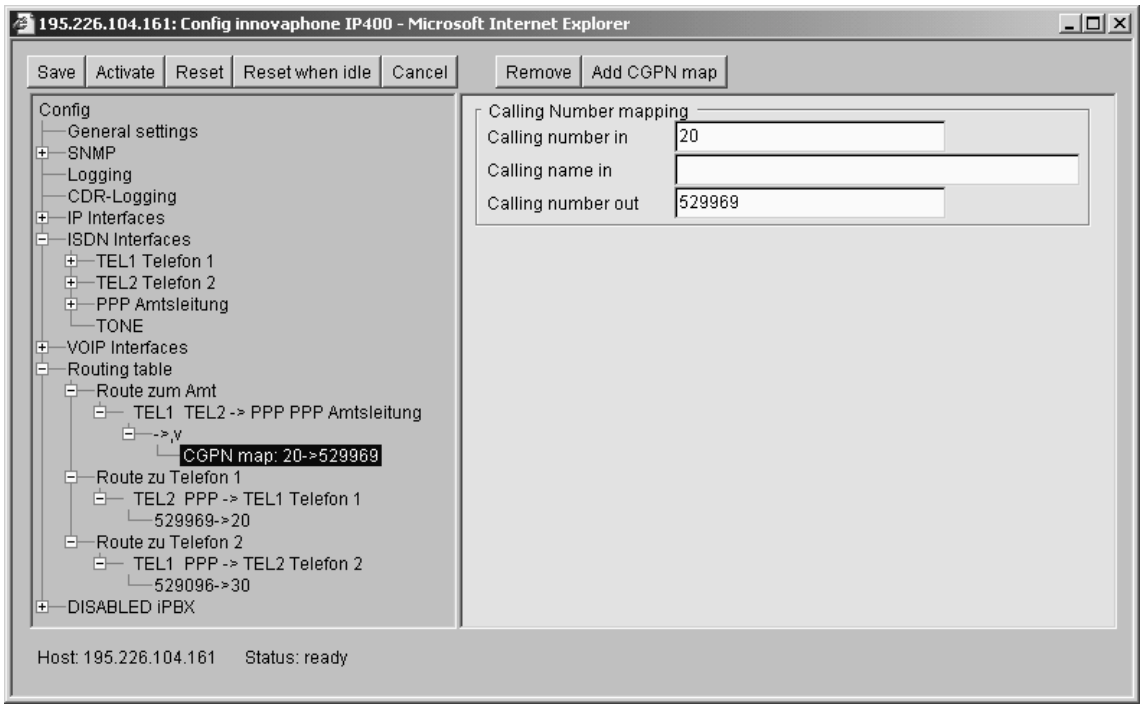


Finally, it is occasionally necessary to define routes depending on the calling number. For this, so-called CGPN Maps are attached to the Maps, very much like the Maps that are attached to the routes. This allows not only the calling numbers to be modified[62], but also the entire Map to be made dependent of the calling number.

Figure 63 shows the configuration from Figure 62 Routes with call number replacement altered in such a way that access to the trunk line is available only for the telephone with number 20 and with outgoing calls, in deviation from the incoming mapping, the call number 529096 is sent.

[62] Perhaps to suppress the direct dialling with outgoing calls.

Figure 63 Dependence on the calling number



Call routing is controlled by the gateway's routing table (in ROUTING TABLE area).

For each individual call the routing table is searched from top to bottom. If a Map is found,

- ▲ whose route cites the source interface of the current call as a permitted interface in the ENABLE CALLS FROM INTERFACES listing, and
- ▲ whose common dial prefix specified in the CALLED NUMBER IN field matches the called number of the current call, and
- ▲ whose VERIFY CGPN checkbox is not set

  or

  whose VERIFY CGPN checkbox is set and the calling number of the current call matches the CALLING NUMBER IN entry of one of the CGPN maps added to the map

then the current call is routed to the interface in the DEFAULT CALL DESTINATION field of the map's route or to the interface specified in the map's DESTINATION field.

In the process, the called number is modified such that the common dial prefix contained in the CALLED NUMBER IN field is replaced by the digit string contained in the CALLED NUMBER OUT field. The calling number is modified appropriately based on the CALLING NUMBER IN and CALLING NUMBER OUT fields if the map entry used has

a CGPN map entry on it, whose CALLING NUMBER IN field matches the start of the calling number of the current call.

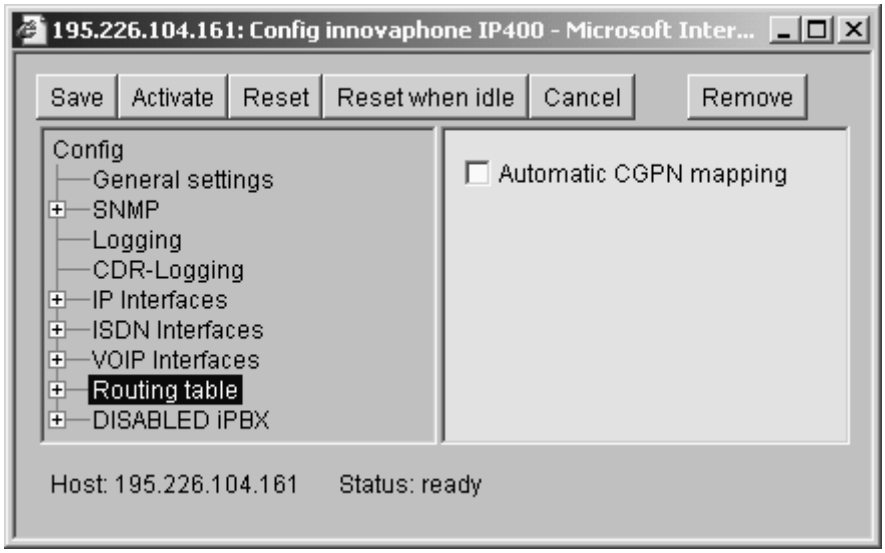
If call forwarding to the identified interface is not possible though, the next map entry in the routing table is searched, for that meets the conditions listed above.

If no suitable map entry is found in the routing table, the call is invalid and is not put through. This may be used, for example, to prevent certain sources accessing a trunk line and running up charges.

Configuring the routes

Configuration of the routing table is done in the ROUTING TABLE area of the configuration applet.

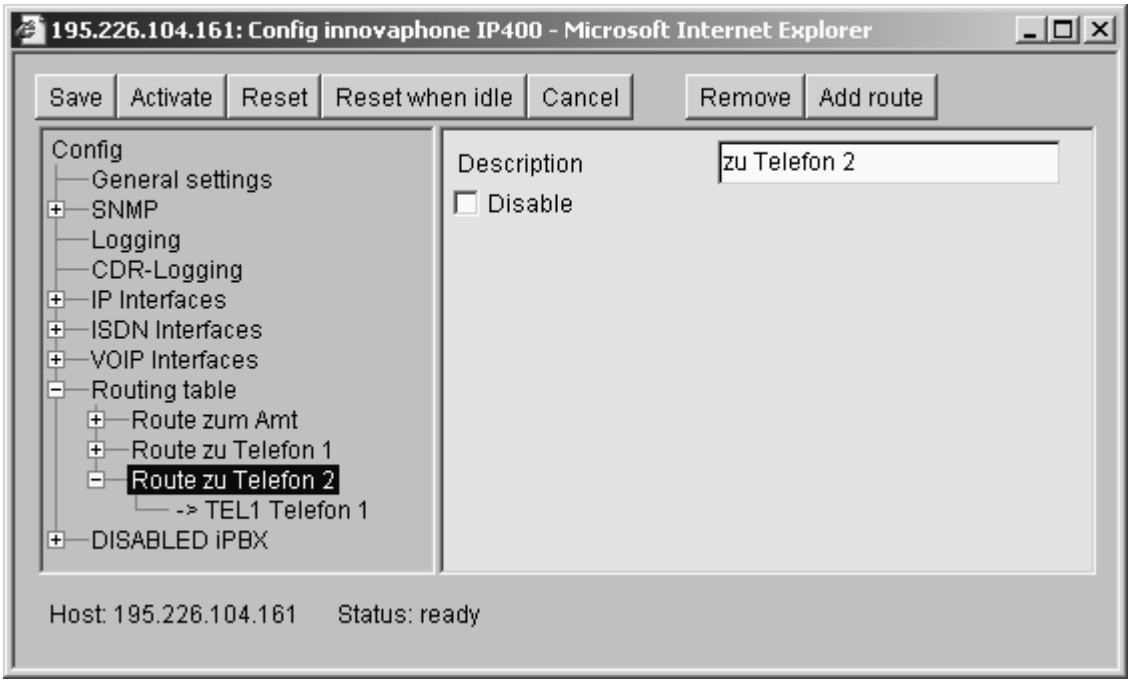
Figure 64 The ROUTING TABLE area



The definition of a new route is done by the following steps:

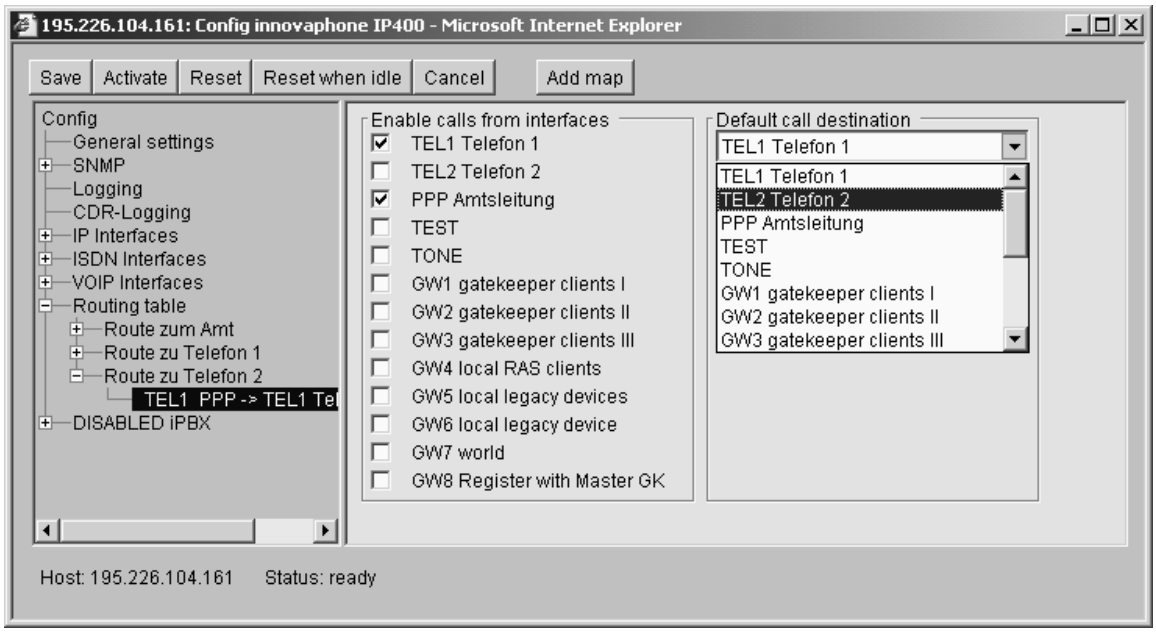
▲ Click on the ADD ROUTE button to add a further entry to the routing table. Be careful here with the order of the routes. The new route is always inserted after the current entry.

Figure 65 Inserting a new route



- ▲ Enter a name for the route in the DESCRIPTION field. This will help considerably in keeping track later on.
- ▲ Select the entry beneath the new route (the one with "->")
- ▲ In the DEFAULT CALL DESTINATION selection list, choose the destination to which the calls are to be connected
- ▲ In the ENABLE CALLS FROM INTERFACE area, check the gateways and ISDN interfaces checkbox to validate them as sources for this route. Only the interfaces that have been configured will be offered.
- ▲ Click on the ADD MAP button
- ▲ In the CALLED NUMBER IN field, enter the common dial prefix the route shall be valid for
- ▲ In the CALLED NUMBER OUT field, enter the replacement for the common dial prefix that you specified in the CALLED NUMBER IN field. If the called number should be passed unchanged, simply copy the dial prefix into this field
- ▲ If a route shall apply for a certain number and if all selection digits subsequently dialled are to be ignored, append an exclamation mark (!) to the number.

Figure 66 Definition of the source and destination interfaces



If you want to specify a number of routes for a set of sources, you can use the ADD MAP button repeatedly.

Figure 67 Parameters of a map entry

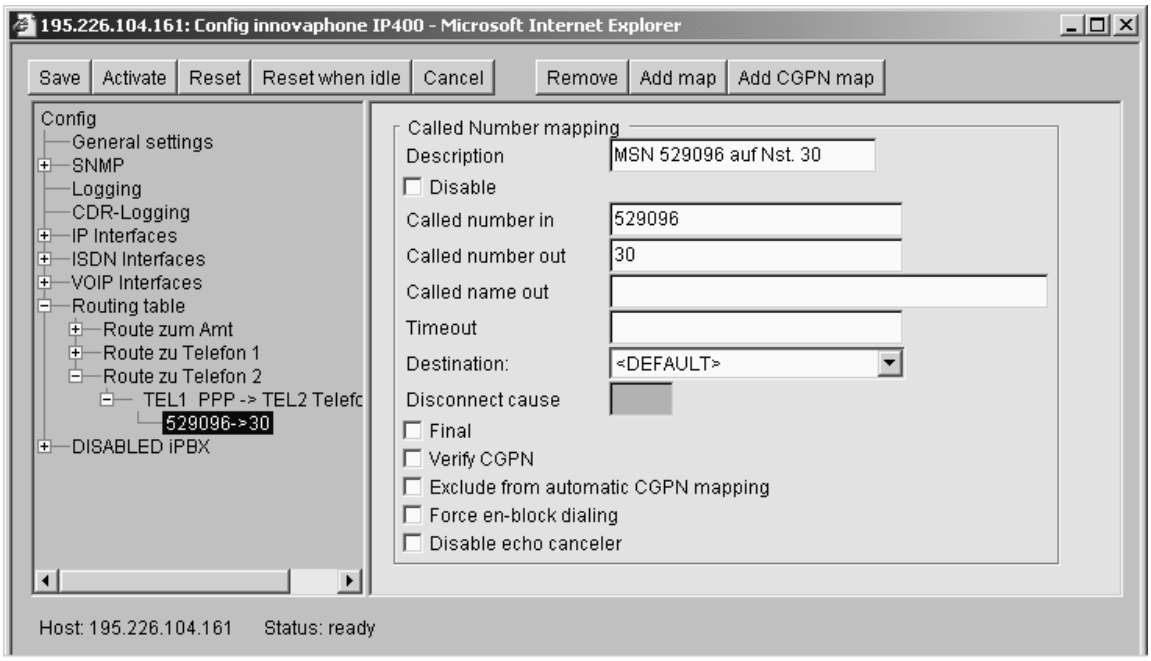
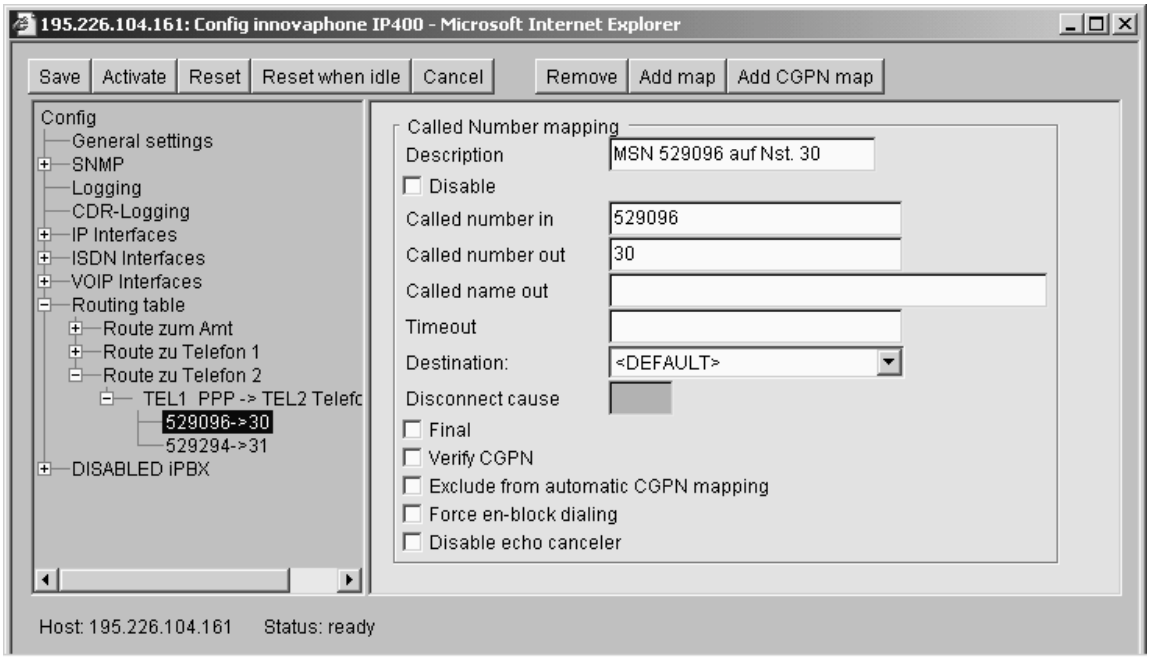


Figure 68 below gives an example. There, two MSNs (529096 and 529294) are linked on an ISDN interface and mapped there onto the MSNs (30 and

31) set up in the telephones. Both call numbers with replacements are configured as map to a route.

Figure 68 Routes with multiple maps



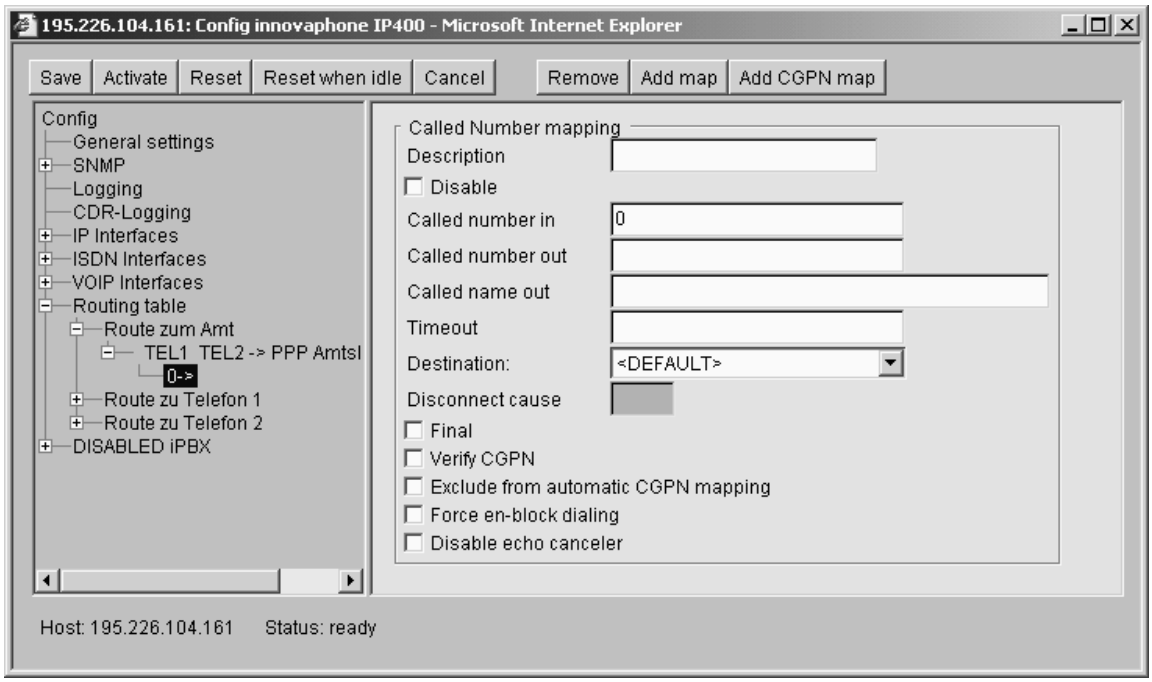
- If, for a map entry, the route exceptionally is to be configured with a different destination than that specified in the route's DEFAULT CALL DESTINATION field, select this in the map's DESTINATION field.
- Leave all the remaining fields blank in the normal case.
- To configure further routes, mark the route after which the new route is to be inserted and click on the ADD ROUTE button.

Manipulation of the calling party number (CLI)

In processing calls, it may be necessary to manipulate the calling party number, for example to ensure a correct callback.

Figure 69 Configuring a trunk access code shows configuration of "0" as access digit for a trunk line.

Figure 69 Configuring a trunk access code

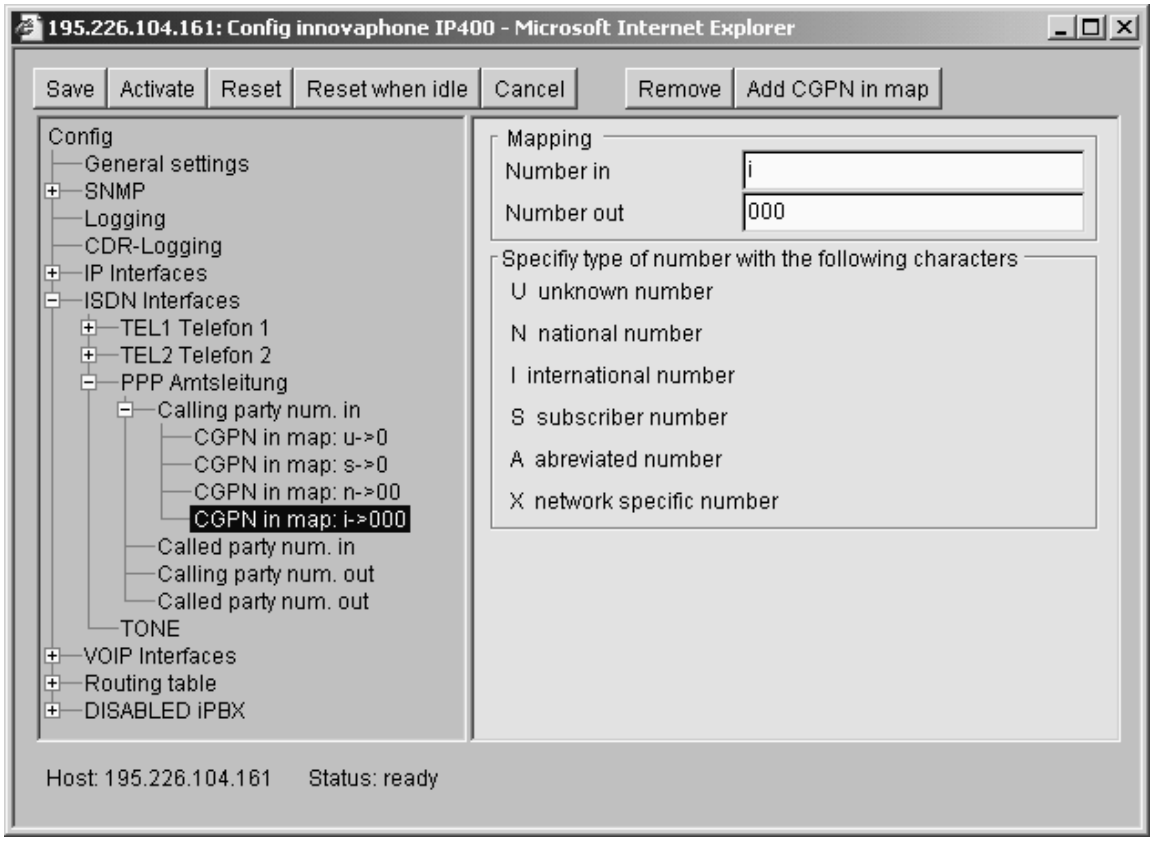


To ensure that here a trunk access digit of "0" is prefixed to the calling party number for all incoming calls via the trunk line, a CGPN (calling party number) mapping must be created for the appropriate interface.

The basic procedure for this is described in the section "Treatment of the various ISDN address types" from page 87 onwards.

Figure 70 shows how an additional "0" can be inserted as trunk access code on the PPP interface.

Figure 70 Manual insertion of trunk access code



Automatic correction of all calling numbers

With complex routing tables, the manual correction described above can be very laborious and prone to errors. The option therefore exists for the correct adjustment of all calling numbers automatically. For this you merely need to mark the AUTOMATIC CGPN MAPPING checkbox in the ROUTING TABLE area (see Figure 64 The ROUTING TABLE area).

The relevant modification of the calling party numbers is controlled by analysis of the routing table. Here a route is sought that, as it were, would make callback to the actual call possible. The number replacements of this route are then used, as it were, back to front. This automatic correction of the calling party numbers is carried out according to CGPN mappings set up if need be for ISDN interfaces or gateways.

If you want certain routes to be ignored in this process, you can mark the EXCLUDE FROM AUTOMATIC CGPN MAPPING checkbox in the relevant route.

Figure 71 Exclusion from AUTOMATIC CGPN MAPPING

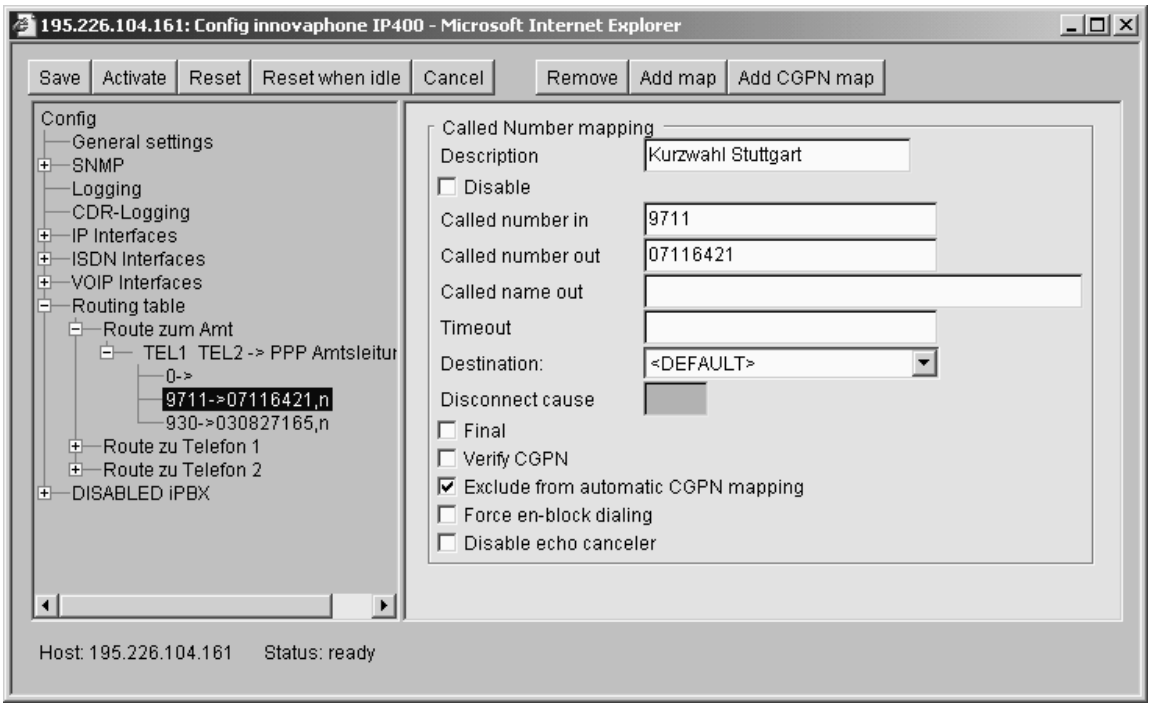


Figure 71 Exclusion from AUTOMATIC CGPN MAPPING shows two speed dial routes which are to be excluded from modification of the calling party number[63].

Selective routing depending on the calling number

In certain cases it can be useful to restrict individual routes to particular calling party numbers. By this means, access to a chargeable trunk line can be restricted to certain extensions (selective trunk authorisation) , for example.

For this proceed as follows:

- ▲ In the routing table, mark the entry that you want to restrict
- ▲ Mark the VERIFY CGPN checkbox
- ▲ Click on the ADD CGPN MAP button and append one or more entries
- ▲ Under CALLING NUMBER IN enter the common prefix that you wish to allow for this route. Omitting the entry in this case makes no sense.

[63] Otherwise calls from the Berlin branch beginning with `930` instead of `0030926` are displayed, which can be confusing for the users.

- Under CALLING NUMBER OUT enter the digit string that is to replace the above-specified prefix. Here it generally makes sense not to undertake replacement. The same digit string as under CALLING NUMBER IN is then specified
- Leave the remaining fields blank

If you have selected "Automatic correction of all calling numbers" (see page 134), checking is applied to the already corrected numbers.

Figure 63 shows the configuration from Figure 62 Routes with call number replacement altered in such a way that access to the trunk line is available only for the telephone with number 20 and with outgoing calls, in deviation from the incoming mapping, the call number 529096 is sent.

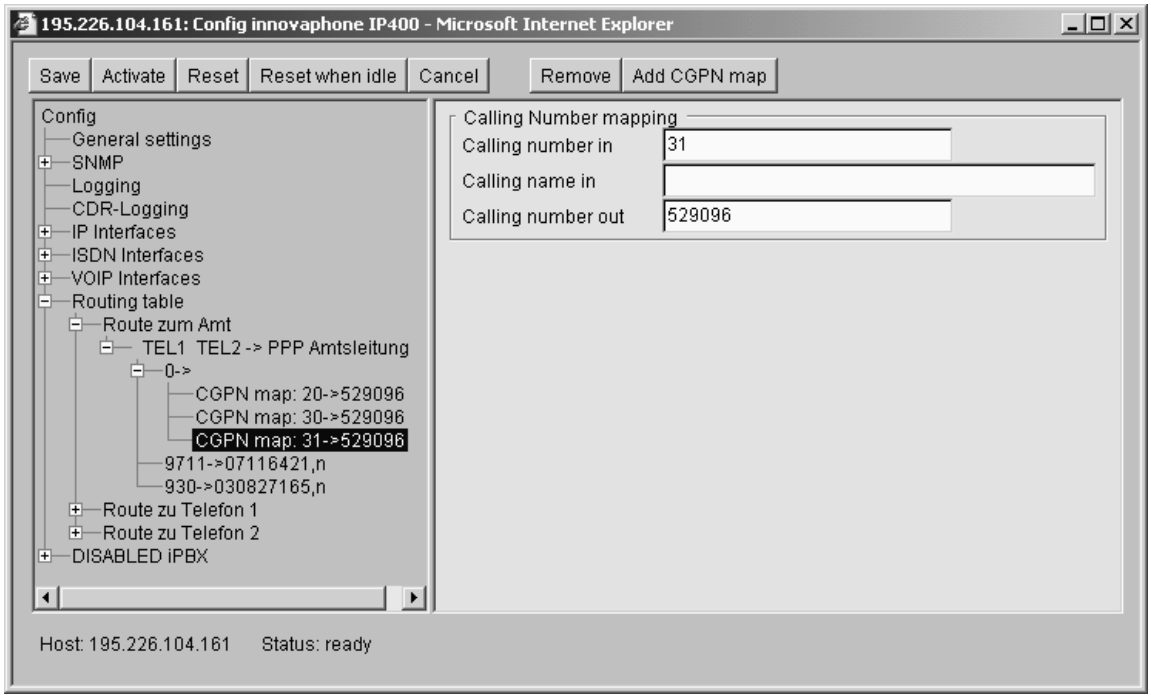
on page 127 shows such a configuration.

If you clear the CGPN Mappings again, make absolutely certain that you deactivate the VERIFY CGPN checkbox, since otherwise no calling number at all would be authorised and the Map rendered inoperative.

Altering the calling party number for specific routes

In some case it can be beneficial to modify the calling party numbers for calls routed with the aid of specific maps. For this, proceed in accordance with the description in the section “Manipulation of the calling party number (CLI)” above.

Figure 72 Altering the calling party number for specific routes



Make certain in this case that the VERIFY CGPN checkbox is not activated. Also note that during execution of a route, the calling party numbers are always interpreted independent of the address type (see section "Treatment of the various ISDN address types" from page 87 onwards), therefore no address types can be specified here.

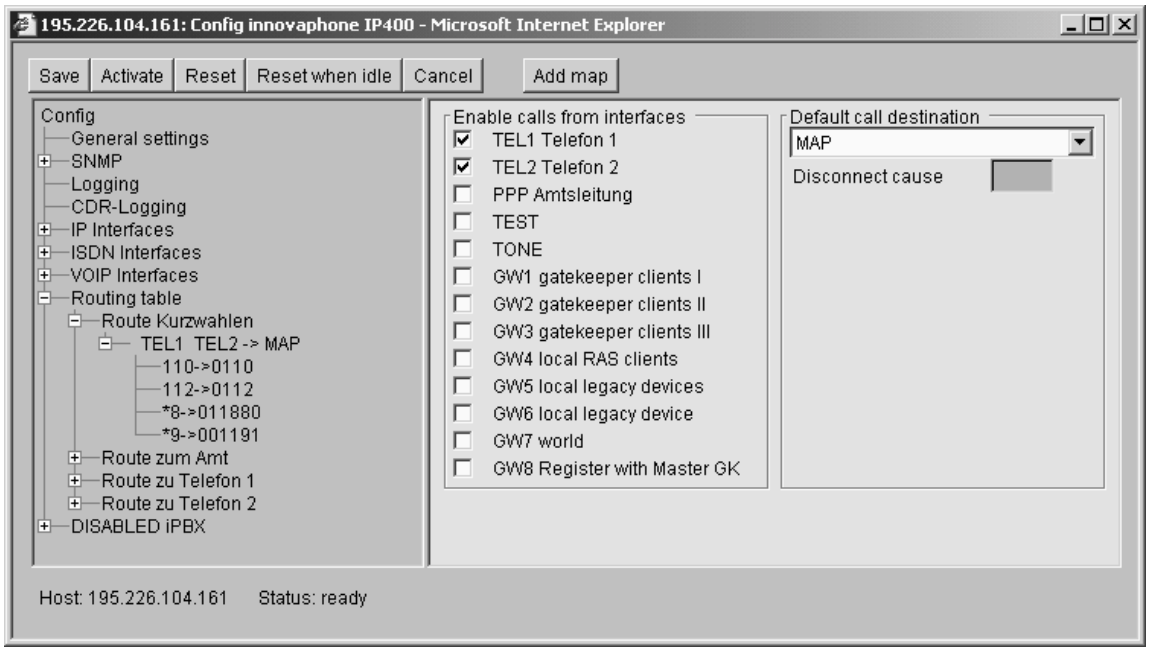
Defining call number replacements

It is often useful to replace dial prefixes, generally and independently of individual routes, e.g. to implement speed dial entries. Here the abbreviated speed dial number is replaced by the complete number and then the new routing for the complete number is performed.

This can be achieved by creating a route to the destination MAP in field DEFAULT CALL DESTINATION. Following the number replacement the call is not connected in the usual way but a suitable map is sought in the routing table with the replaced call number.

Figure 73 Speed dial implemented by MAP routes shows a configuration in which an external call number can be reached using speed dial.

Figure 73 Speed dial implemented by MAP routes



Please keep in mind, that in order to avoid infinite replacement operations only those routes will be searched that are positioned text-wise after the MAP route. MAP routes must therefore always be listed prior to the routes that define the handling of the replaced number.

Configuration of multiple routes for a single dial prefix

You can specify different routes for different call sources for one and the same dial prefix, with routing dependent on the call source and not just on the called number.

Figure 74 Call routing depending on the calling interface

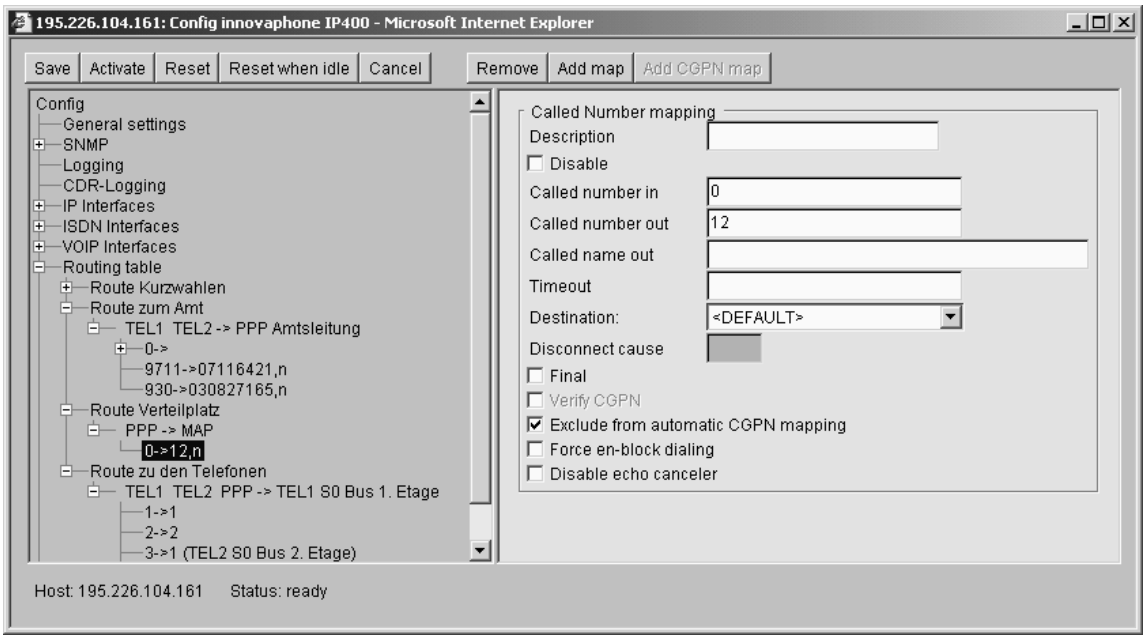


Figure 74 Call routing depending on the calling interface shows an example of such a configuration. Here call number 0 is connected to number 12 (switchboard position) for calls from the trunk line, but is connected to the trunk line for all other calls.

Call forwarding

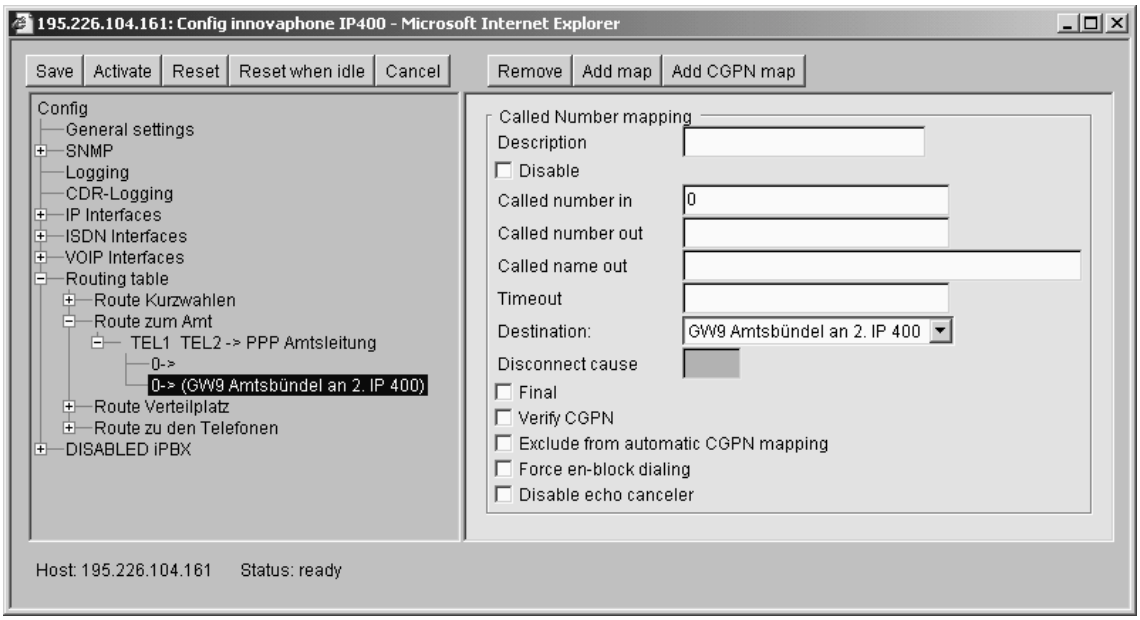
It can be useful to create routing entries with overlapping call prefixes for calls from the same call source.

The routing process in the gateway will always use the first suitable route. If a connection cannot be established using this route, subsequent routing entries can be tried. Various sorts of call forwarding can be implemented in this way.

- If a call cannot be established due to missing local resources (possibly no available trunk line, see below Table 22 "Local Problems" relating to call forwarding), a further valid route is sought immediately. Where there are several trunk lines connected to the gateway, this allows the calls to be distributed to the trunk lines in succession, for example (Figure 75 Configuration of a trunk line group shows such a configuration)

▲ If a call placement is attempted based on a route and the call could be signalled successfully to the called terminal device (device responded with an alerting message) and if for this route there is a value greater than 0 entered into the TIMEOUT field, then, if the call is not accepted within the specified number of seconds the next appropriate routing entry is sought. This implements "Call Forwarding No Answer (CFNR)". If you enter a TIMEOUT of more than 120 seconds, the Timeout cannot occur since the global Timeout for the call set-up will expire before this. However, since available alternative routes are always implemented after a failed call if a Timeout is entered , this acts like the " Call Forwarding Busy" (CFB) function.

Figure 75 Configuration of a trunk line group



If, after the attempt at a connection via a map entry, you want to prevent further routes being tried out, you can mark the FINAL checkbox in the Map entry.

You can also mark the FINAL checkbox in the Map entries for a route with destination MAP. In this case, no further MAP entries will be evaluated but other suitable routes are still searched for.

Table 22 "Local Problems" relating to call forwarding

Error code (decimal)	Description
34	No circuit/channel available
38	Network out of order

Error code (decimal)	Description
41	Temporary failure
42	Switching equipment congestion
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable

Call sequences

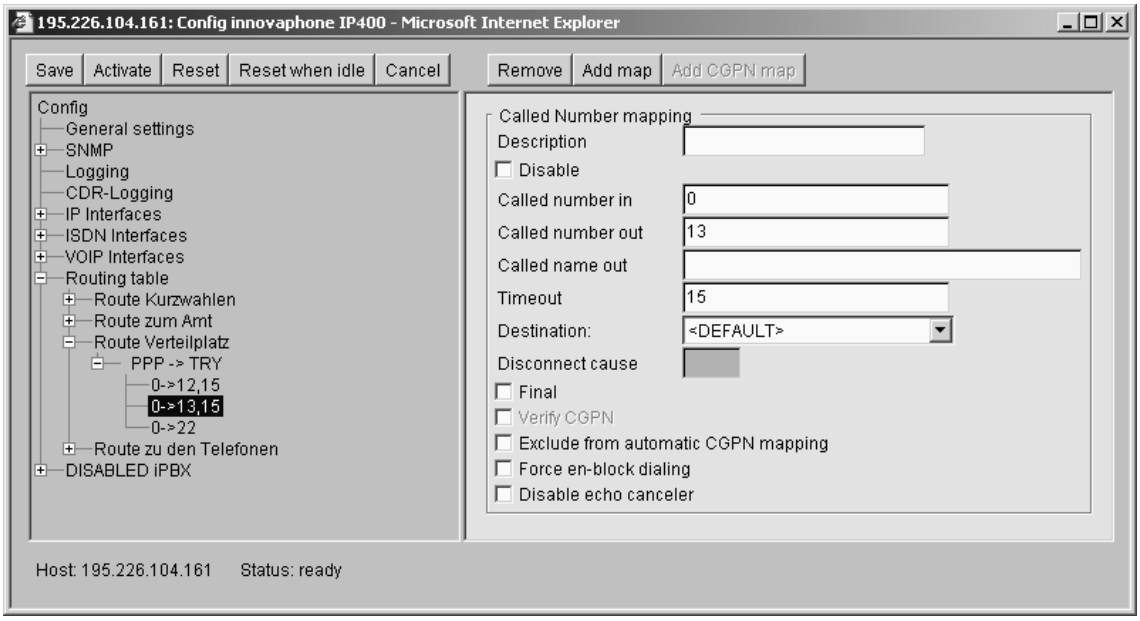
Routes with call destination TRY are a special case. If such a route is enlisted to switch calls, call number replacement is carried out and then normal routes are attempted on the result. If the call cannot be established successfully in this way a further TRY route is then attempted.

If a timeout is specified for the TRY route, this is operative on the routes attempted to connect the call.

If the FINAL checkbox is marked in the Map entry, if applicable no further TRY routes are sought.

Figure 76 Call sequences with TRY routes shows the configuration of a hub, which can be reached by the trunk line via the direct dialling 0 and internally tries extensions 12, 13 and 22 in succession.

Figure 76 Call sequences with TRY routes



Declining calls

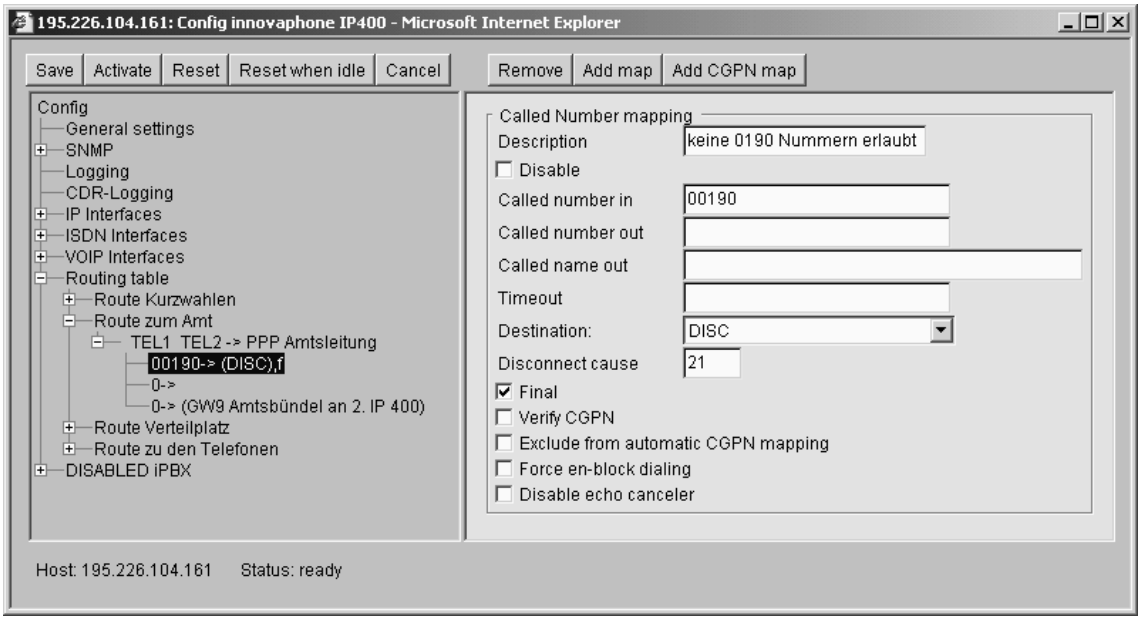
Every time it handles a call, your gateway will try to find routes with suitable Maps and to connect the call accordingly. If no suitable Map entry is found in the routing table or if all call attempts fail, the call is finally declined.

Sometimes though, it is useful to explicitly decline certain calls through an entry in the routing table. This can be done by setting up a route with DISC as the call destination. The reason for declining can then be specified in the DISCONNECT CAUSE field.

Figure shows a configuration in which the trunk access digit is configured so as to exclude the calling of certain call numbers.

A list of the defined reasons for declining calls can be found in Table 28 ISDN error values on page 192. The value specified in the "Error value (decimal)" column must be used.

Figure 77 Declining calls



Enforcing en-bloc dialling

Your gateway supports overlapped sending, i.e. continuous digit-by-digit processing of dialled digits. Thus, no explicit termination key is required to mark the completion of the dialled number. This behaviour also resembles that of traditional PABXs.

Unfortunately, most of today's H.323-compatible telephony gateways do not support this feature. When a call is initiated to such a gateway, it is not able to process the transmitted single digit and the call fails.

In such a case, a hash mark ("#") can be appended to the dial prefix, indicating that the route's destination device requires en-bloc dialling. The gateway will then first collect all digits dialled up to and excluding the hash mark. Subsequent digits dialled will be ignored. The complete number is then sent to the remote gateway.

If there is always a fixed number of digits required to complete the call destination number for a given route entry (e.g. always 3-digit direct diallings), a corresponding number of periods (".") can be appended to the dial prefix. The gateway will then expect a single digit per period and will place the call when all required digits are dialled. No hash mark is required. Subsequent digits dialled will be ignored. The complete number is then sent to the remote gateway.

If there is not always a fixed number of digits required to complete the call destination number for a given route entry, and if no explicit completion of the call is to be effected with a hash mark either, the FORCE EN-BLOC DIALING checkbox can also be marked in the appropriate Map entry. If such a map entry takes hold, the gateway collects the following digits dialled until more than 4 seconds have elapsed since the last digit selection. The call is then connected, with any digits dialled subsequently ignored.

Routes from and to fax devices

In version 2 of your gateway's firmware the option existed for assigning certain map entries to fax connections. This allowed the usage of the appropriate G.726 coder to be enforced for the transmission of Group 3 faxes.

This function (FAX (FORCE G726 40KBPS CODER)) is no longer available from version 3 of the firmware onwards, since faxes can be reliably transmitted via the T.38 protocol (refer to section "H.323 protocol options" from page 105 onwards).

If you update a version 2 configuration of this kind to version 3, you merely need to mark the ENABLE T.38 FAX PROTOCOL checkbox in the relevant gateway definitions in the VOIP INTERFACES area.

Suppressing echo compensation

Your gateway implements echo compensation for all voice connections that terminate in a local ISDN interface (echo cancellation). For data and fax connections the echo compensation is automatically not carried out. In rare cases though, it may be that a call is handled as a voice connection and nevertheless no echo compensation must be carried out. This can be the case, for example, with modem connections.

You can suppress the echo compensation by marking the DISABLE ECHO CANCELER checkbox in the relevant Map entry.

Call routing depending on device management

In principle calls from and to differently configured VoIP devices are handled in a similar way by your gateway. There are some differences in detail though which are outlined in the following sections.

Calls from and to gateway groups

In the section “Static management of VoIP devices” on page **Fehler! Textmarke nicht definiert.** it was explained how groups of VoIP devices are made known to the gateway.

In principle, routes to such gateways are configured in the same way as normal routes are. The call prefix defined for a route to a group is considered matching the dialled number if the start of the number contains the complete dial prefix *and* all digits required to complete the destination device's IP address are dialled. Subsequent digits dialled are passed on if need be to the destination device.

Table 23 Required digits for address completion

Size of host part in bits	No. of digits	Example
1 to 8	3	Class C address
9 to 16	6	Class B address
17 to 24	9	Class A address
more than 24	12	Unspecified group (0.0.0.0)

To complete an IP address 3, 6, 9 or 12 digits are required, depending on the size of the host part of the subnet mask defined in the VOIP INTERFACES definition for the gateway group. The digits are converted to bytes of the IP address in groups of three digits.

Table 23 Required digits for address completion shows the number of digits required. Complete bytes of the IP address have to be dialled in groups of three, even if less than 8 bits are missing according to the configured subnet mask. Leading zeroes must be dialled.

Assuming there is a group of VoIP devices with the network address 195.226.104.128 and the subnet mask is defined as 255.255.255.128. Hence the addresses 195.226.104.129 to 195.226.104.254 can be reached. The dial prefix 91 is configured for routing this group. To call the device with address 195.226.104.135 users then have to dial 91135.

If "Automatic correction of all calling numbers" (see page 134) is activated and a call arrives from a device defined in a group of VoIP devices, the digits required to complete the IP address of the calling device are prefixed to the calling number. This allows callback via the accompanying number.

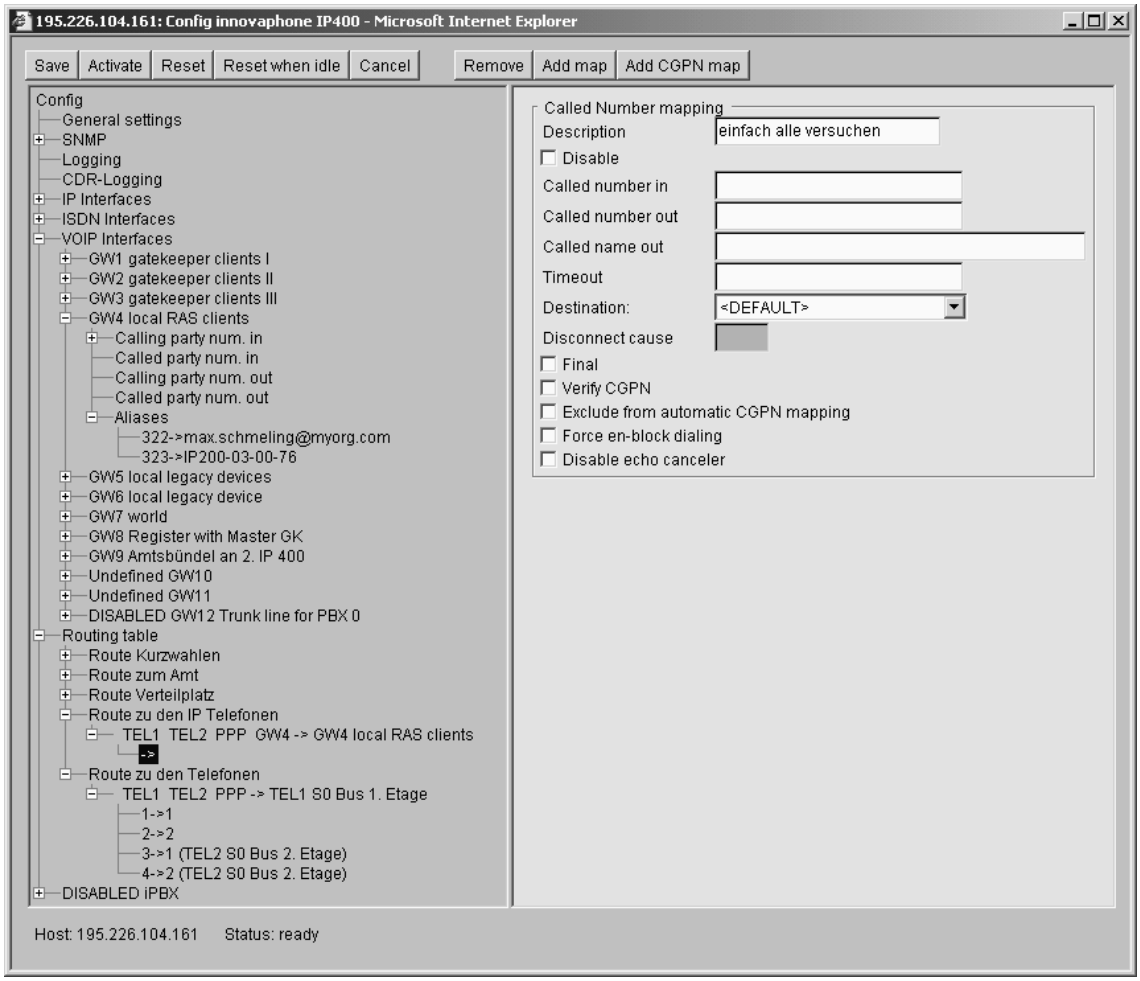
Calls from and to devices managed using RAS

Calls can be routed by call number or by name to a device registered at the gatekeeper using RAS protocol (see section "Management of VoIP devices by RAS (Gatekeeper)" from page 112 onwards. Here, calls to gateways are handled somewhat differently to calls to terminal devices (see page 99).

In principle, the call routing for a call to a VoIP device managed using RAS protocol is handled completely as normal (see section “General considerations for configuring the call routing” on page 124).

If a matching route Map entry is found for the called number and if this or the route has a VoIP INTERFACES definition as destination, which is configured as GATEKEEPER CLIENT GROUP, then all aliases are searched in this gateway and an entry is searched for with an E.164 ADDRESS that matches the called number. If such an entry is found, and if the associated device is currently registered with the gatekeeper, the call is then routed there. Otherwise the search is continued for suitable aliases. If no suitable entry is found, or if the client is not registered at the time of the call, this call will fail and an alternative route is used – if one is available (refer to "Call forwarding" on page 139).

Figure 78 Routes for terminal devices registered by RAS



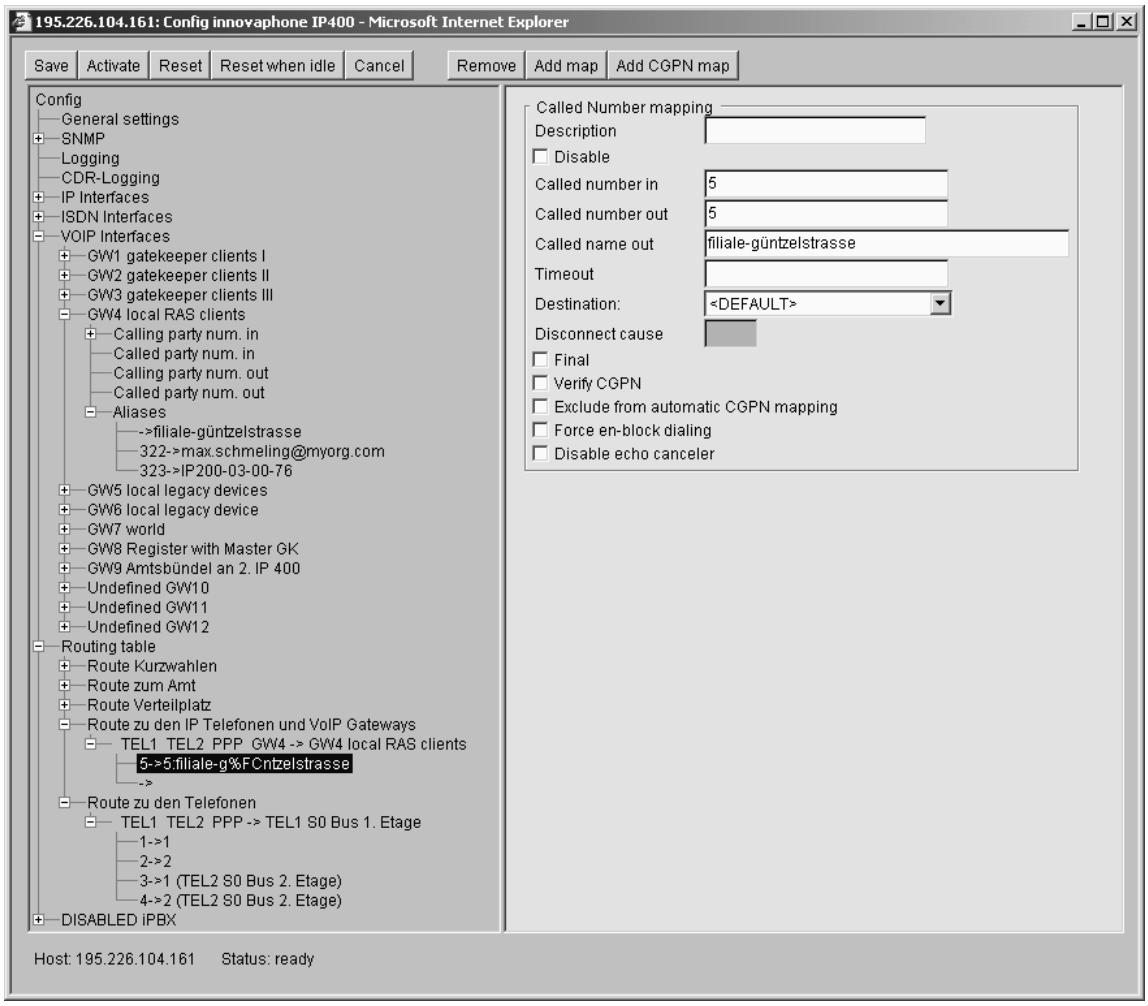
On the basis of this procedure the called number in a call is checked twice in the call routing: the first time when a route suitable for the call is searched for, and the second time when a suitable alias within the VOIP INTERFACES definition is sought. It is therefore possible and normal to configure routes of this kind very simply using blank map entries. This means that at first it will be attempted to route all calls to the devices registered using RAS. However this will quietly fail if no device with the correct number is registered.

If a matching route Map entry is found for the called number and if this or the route has a VOIP INTERFACES definition as destination, which is configured as GATEKEEPER CLIENT GROUP, then all aliases are searched in this gateway and an entry is searched for with an E.164 ADDRESS that matches the called number. If such an entry is found, and if the associated device is currently registered with the gatekeeper, the call is then routed there. Otherwise the search is continued for suitable aliases. If no suitable entry is found, or if the client is not registered at the time of the call, this call will fail and an alternative route is used – if one is available (refer to "Call forwarding" on page 139).

shows such a configuration. Two IP telephones with direct dialling numbers 22 and 36 are configured in this example as devices registered by RAS in the VoIP INTERFACES definition GW2. The remaining number range from 10 to 49 is shared between two ISDN BRI busses.

In contrast to VoIP terminal devices, which are registered in the gatekeeper with name and number, normally no number is registered for the VoIP gateways. This would not make sense anyway since the gateways implement an entire range of numbers, of course, and not just a single number. The determination of the call destination based on the called number described earlier on therefore does not work.

Figure 79 Routes for gateways registered by RAS



If gateways are registered in a VoIP INTERFACES definition and a route is to deliver a call there, specifying the gateway entry GWXX is not sufficient to identify the destination. What is also required here is thus specification of the correct H.323 name in the Map as CALLED NAME out.

Figure 79 Routes for gateways registered by RAS shows a configuration in which the call numbering plan refers from 10 to 49 to two ISDN BRI busses, from 50 to 59 to a branch linked by VoIP gateway and otherwise to IP telephones.

Calls to gatekeeper clients by H.323 name

In the VoIP domain, dialling by telephone number represents just one possibility for destination addressing. Another convenient option is to specify a name as the call destination.

If a call arrives in the gatekeeper with an H.323 name but without an E.164 address[64] , the number that belongs to the ID is first of all determined by searching in all of the VOIP INTERFACES definitions of the type GATEKEEPER CLIENT GROUP according to an alias entry with the corresponding H.323 NAME . The E.164 ADDRESS of the first matching entry is then used for further call routing, just as if from the outset the call had arrived with this number as the called number.

Mapping call numbers onto H.323 names

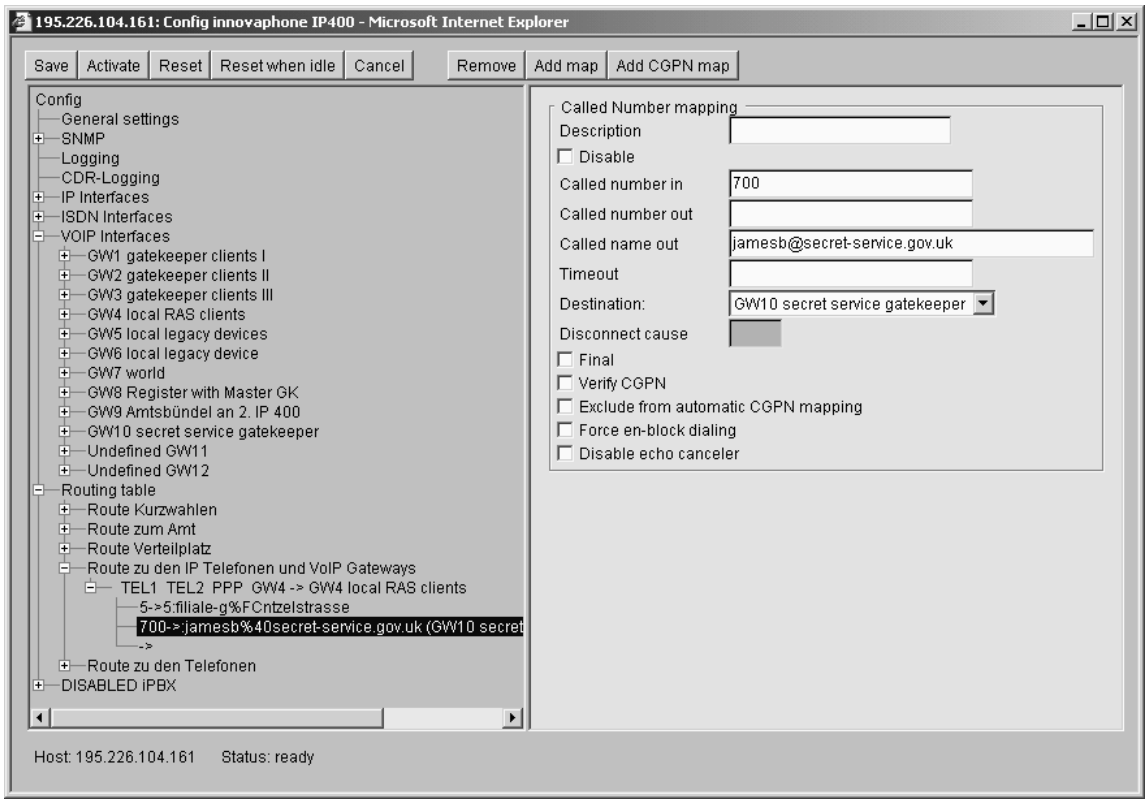
You can map telephone numbers to H.323 names in the routing table. In this way you can then undertake calls based on names to terminal equipment unable to call H.323 names (e.g. ISDN telephones).

In the normal routes enter the H.323 name as CALLED NAME OUT.

This procedure makes sense only if the VoIP terminal device is not registered directly with your gateway as gatekeeper, since then the normal methods would of course suffice.

[64] i.e. without telephone number

Figure 80 H.323 names in routing entries



Definition of various operating parameters

General settings

General parameters can be defined in the GENERAL SETTINGS area of the configuration applets.

Defining the gateway name

You can assign an appropriate name for your gateway and enter it in the NAME field. This name appears in the window title of the gateway home page and configuration applet, making it far easier to keep an overview when configuring a number of devices.

Figure 81 The gateway name

Defining the administrator account and password

In the CHANGE LOGIN PARAMETERS area you can define the administrator's user name and associated password, which secure the gateway configuration.

On saving or activating the configuration, checks are made to ensure that the newly defined password is valid. Like any other configuration change, a change in password must be activated and saved as described in section "Verifying and saving configuration changes" on page 162.

Defining the time and date source

Your gateway is not equipped with a battery-backed real-time clock. After every restart the internal time is therefore reset to 0:00 hrs, 1.1.1970.

A correct time reference is not necessary for normal operation. However, if this is important to you – for example to obtain Call Detail Records – you can specify the IP address of a time and date source in area GET TIME FROM SNTP SERVER .

Your gateway will then synchronise its internal clock to the time source at intervals specified under UPDATE INTERVAL.

If your network is not equipped with an NTP Server, you can use the following public servers listed in Table 24 “Publicly accessible time services”.

Your gateway also works simultaneously as an NTP server. If you are running additional IP21, IP 400 or IP 3000 gateways or IP 200 telephones[65], you can synchronise one of them with a time server (external if need be) and then all the others in turn from this one.

Table 24 Publicly accessible time services

Location	IP address
TU-BERLIN.DE	130.149.17.21
TU-BERLIN.DE	130.149.17.8
UNI-ERLANGEN.DE	131.188.34.75
UNI-ERLANGEN.DE	131.188.34.40
UNI-ERLANGEN.DE	131.188.34.45
UNI-ERLANGEN.DE	131.188.34.107
UNI-OSNABRUECK.DE	131.173.17.7
UNI-ERLANGEN.DE	131.188.1.45
UNI-ERLANGEN.DE	131.188.1.31
PTB.DE	194.95.250.35
PTB.DE	194.95.250.36

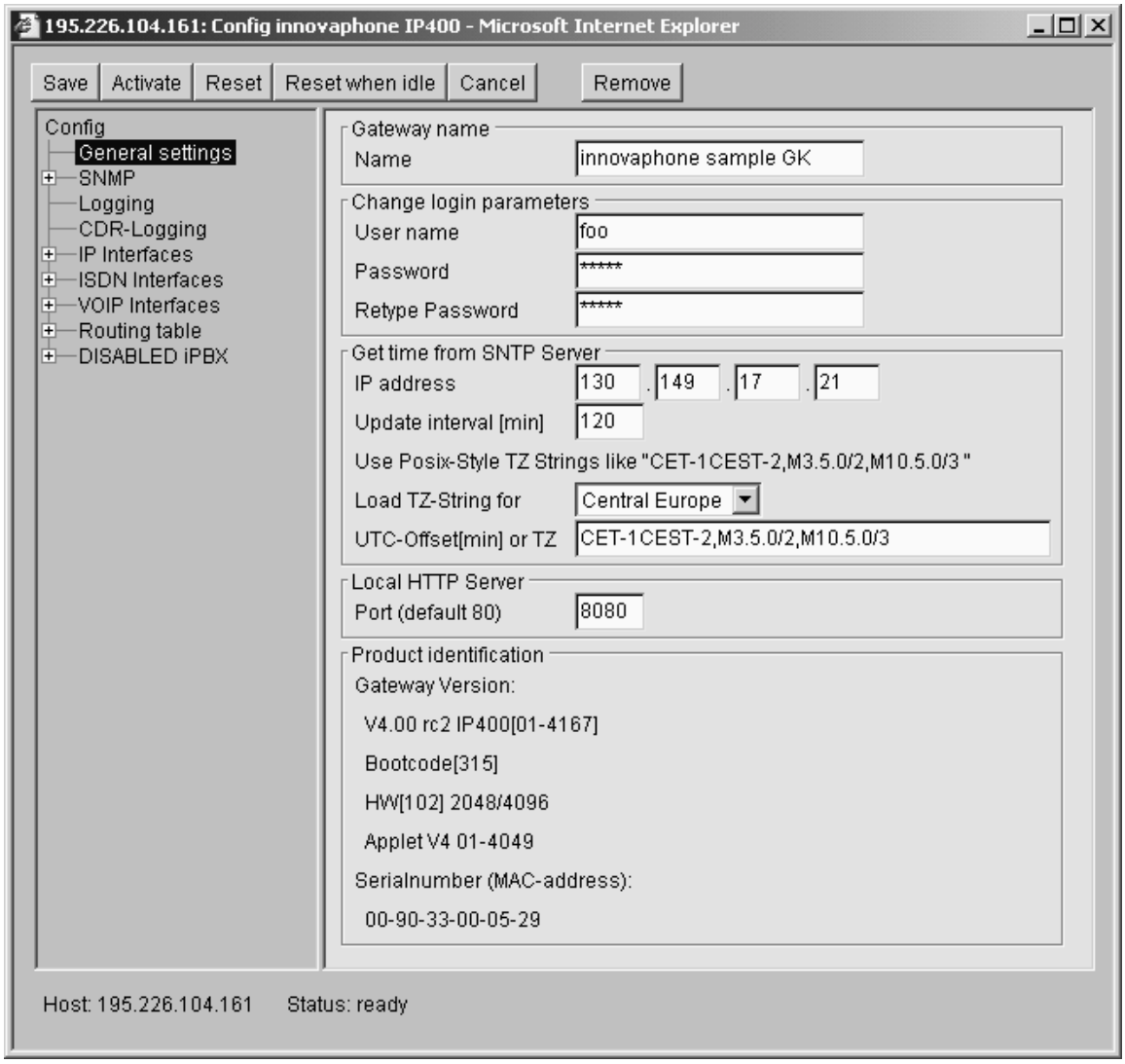
Further public time services worldwide can be found on the Internet under http://www.eecis.udel.edu/~mills/ntp/.

If you are going to operate other devices in your network that require a time server[66], then please enter there the IP address of your IP 21 / IP 400 / IP 3000. Your gateway will then itself act as a time service and report the correct time to the other devices. Avoid synchronising all of the devices to an external time service, since this results in an unnecessarily high load on this server.

[65] IP 200 telephones automatically use their gatekeeper as SNTP Server, as long as no other has been configured.

[66] For example further gateways or IP telephones

Figure 82 General settings



Time services always supply the coordinated universal time[67], and not however the correct time zone nor the summer time. You can specify the offset of your time zone from the universal coordinated time in the UTC OFFSET[MIN] OR TZ field. In the time zone GMT+1 (this is the Central European Time zone) this offset is 60 minutes. A further 60 minutes has to be added in the summer time so the overall offset is then 120 minutes. In this case you must, however, set manually the offset to switch from winter and summer time and vice versa.

This setting can be automatically carried out by the device if you specify the so-called TZ-String[68] in the UTC OFFSET[MIN] OR TZ field. In this value, the name of

[67] Universal Time Coordinated (UTC), this corresponds to Greenwich Mean Time (GMT)

[68] TZ stands for *T*ime *Z*one

the time zone, the name of the summer time zone, and their respective offsets to the UTC and the time switch points are encoded.

Since the values are somewhat complicated, the configuration applet offers a choice of edit help for making the correct entries for central Europe and Great Britain:

- In the LOAD TZ-STRING FOR field, select the Central Europe value. The TZ-String for the central European time zone will be entered in the UTC OFFSET[MIN] OR TZ field
- In the LOAD TZ-STRING FOR field, select the UK value. The TZ-String for the British time zone will be entered in the UTC OFFSET[MIN] OR TZ field
- In the LOAD TZ-STRING FOR field, select the UK value. The TZ-String will be cleared and you can then enter any value. There are various formats that are defined by the IEEE POSIX[69] standard. For most practical purpose, the following description will nonetheless suffice[70]:

  Posix TZ Strings have the following form (optional parts in square brackets):

  StdOffset[***Dst***[***Offset***],***Date*/*Time***,***Date*/*Time***]

  - ***Std*** describes the time zone (e.g., CET for central european time or MEZ for mitteleuropäische Zeit)
  - ***Offset*** gives the offset of the time zone with respect to the UTC , e.g. –1 for CET. The offset is negative if the time zone is ahead of UTC (therefore – 1 for CET). If the offset is not in whole hours, the number of minutes may be appended (e.g., -1:30).

    If no summer time is used, the TZ-String terminates here
  - ***Dst*** describes the summer time zone (e.g., CEST for central european summer time or MES for mitteleuropäische Sommerzeit)
  - The optional second ***Offset*** gives the offset of the summer time with respect to UTC. If this is not specified, an hour before the normal time is assumed
  - ***Date*/*Time***,***Date*/*Time*** define the Start and End of summer time. The format for a time entry is M***m***.***n***.***d***, signifying the ***d***-th day of the ***n***-th week of the ***m***-th month. Day 0 is Sunday. If the fifth week is specified,

[69] You can find further information about this standard at the Web address http://standards.ieee.org/catalog/olis/posix.html

[70] This description is based on a translation of the FAQ List of the Linux Samba packet

the last day (with respect to ***d***) of the month is meant. The format for a time entry is ***hh***[:***mm***[:***ss***]], in the 24-hour format.

The Central European Timezone as valid in Germany is specified as follows:

CET-1CEST-2,M3.5.0/2,M10.5.0/3

If you are going to operate other devices in your network that require a time server, then please enter there the IP address of your IP 21 / IP 400 / IP 3000. Your gateway will then itself act as a time service and report the correct time to the other devices. Avoid synchronising all of the devices to an external time service, since this results in an unnecessarily high load on this server.

above shows the configuration of an SNTP Server, which is interrogated every two hours. The gateway interprets the time in the Central European Timezone.

Defining the administration port

The administration of your gateway via the network is done via TCP ports 80 (http) and 23 (telnet). If for some reason port 80 is not to be used you can set up another port in the LOCAL HTTP SERVER PORT field. Access is then available to you via this port.

Please note that when using the applet, the telnet port (23) is required as well.

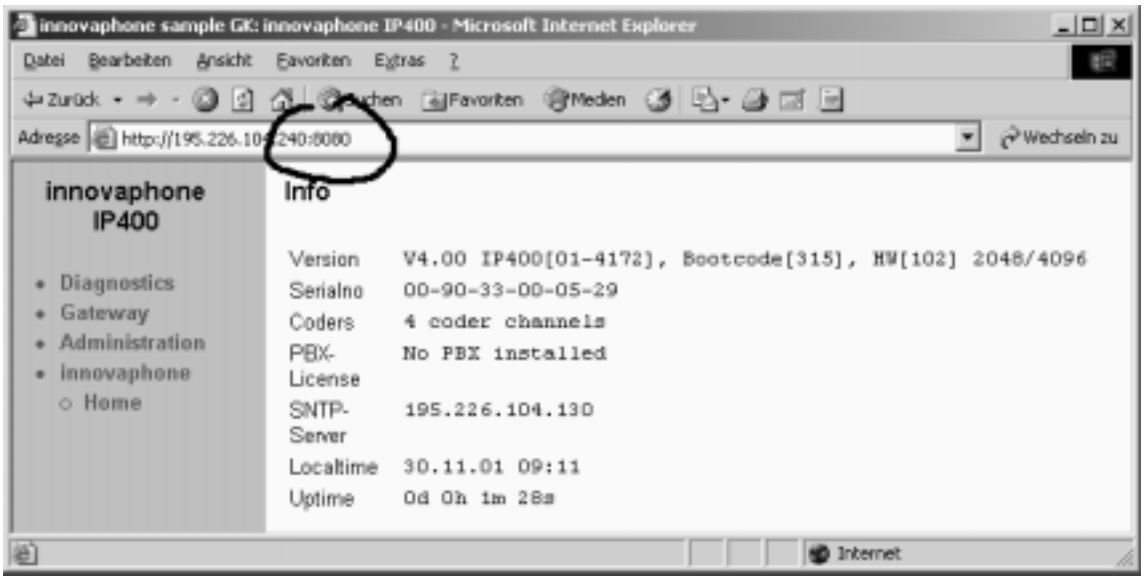
Figure 83 below shows access to a gateway in which port 8080 has been configured for administration.

Please note that when using the applet, the telnet port (23) is required as well[71].

[71] Telnet Port 23 cannot be changed using the applet. If this port needs to be modified, the followed commands need to be entered via `telnet` :

```
config change TELNET0 /port tport
config change HTTP0 /port hport
config write
reset
```

Figure 83 Access to a gateway with altered administration port 8080



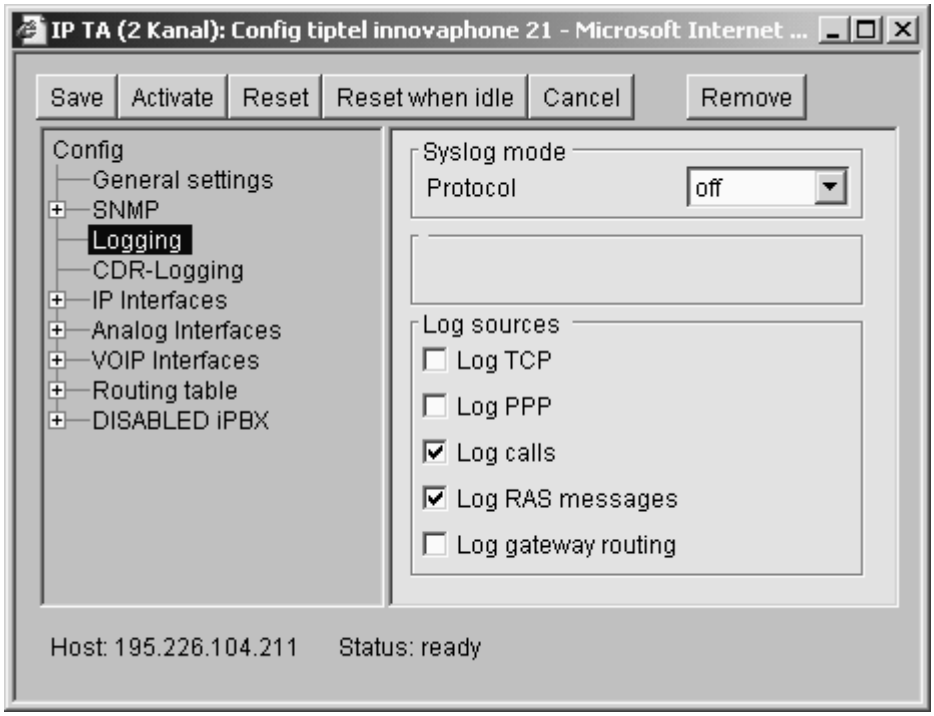
Defining the Syslog parameters

Your gateway can record significant events that occur during operation in a system log (Syslog).

The type of events to be kept in the Syslog can be configured in the LOG SOURCES field in the LOGGING area as follows:

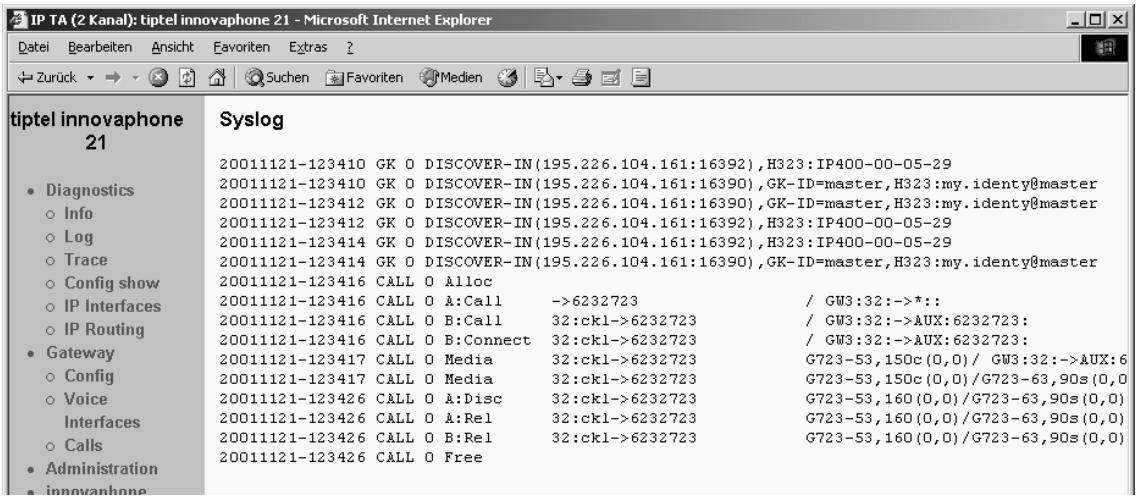
Setting	Meaning
LOG TCP	All TCP connection set-ups in the H.225 / H.245 protocol are recorded
LOG PPP	All PPP connection activities are recorded
LOG CALLS	All call routings are recorded
LOG RAS MESSAGES	Gatekeeper information relating to the logging on and off of H323 terminal devices is recorded
LOG GATEWAY ROUTING	The separate steps of the call routing in the processing of the routing table are recorded

Figure 84 Setting up Syslog events



All the current Syslog entries can be checked via the Web interface at any time via the LOG link as shown in figure 85.

Figure 85 Syslog entries in the Web interface



Syslog entries are displayed only if a Web browser displays the LOG page. Otherwise they will be lost.

If the Syslog is to be saved permanently, there are in addition three methods to choose from for achieving this.

▲ Storing the Syslog entries in a syslogd

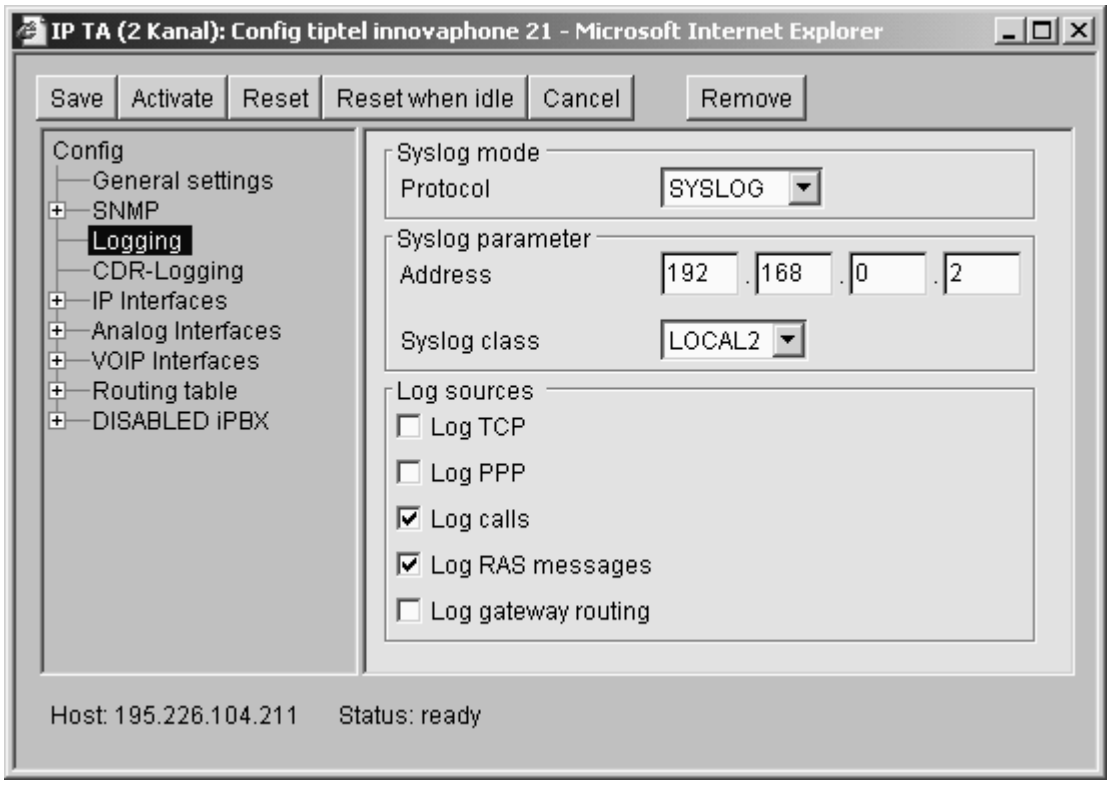
Here, the entries are logged to a syslogd server in the network. It is then responsible for further evaluation.

▲ Select SYSLOG as SYSLOG MODE

▲ Enter the IP address of your syslogd under ADDRESS in the SYSLOG PARAMETER area

▲ Select the desired syslogd message class under SYSLOG CLASS

Figure 86 Sending log messages to a syslogd



▲ Storing of Syslog entries in a Web server

In this case the Syslog entries are transferred to a Web server and can be further processed there. Each separate Syslog entry is transmitted as form data to the Web server in HTTP GET format.

▲ Select HTTP as SYSLOG MODE

▲ Enter the IP address of your Web server under ADDRESS in the HTTP PARAMETER area

- Enter the relative URL of the spreadsheet programme[72] on your Web server under URL-PATH

Figure 87 Sending log reports to a Web Server

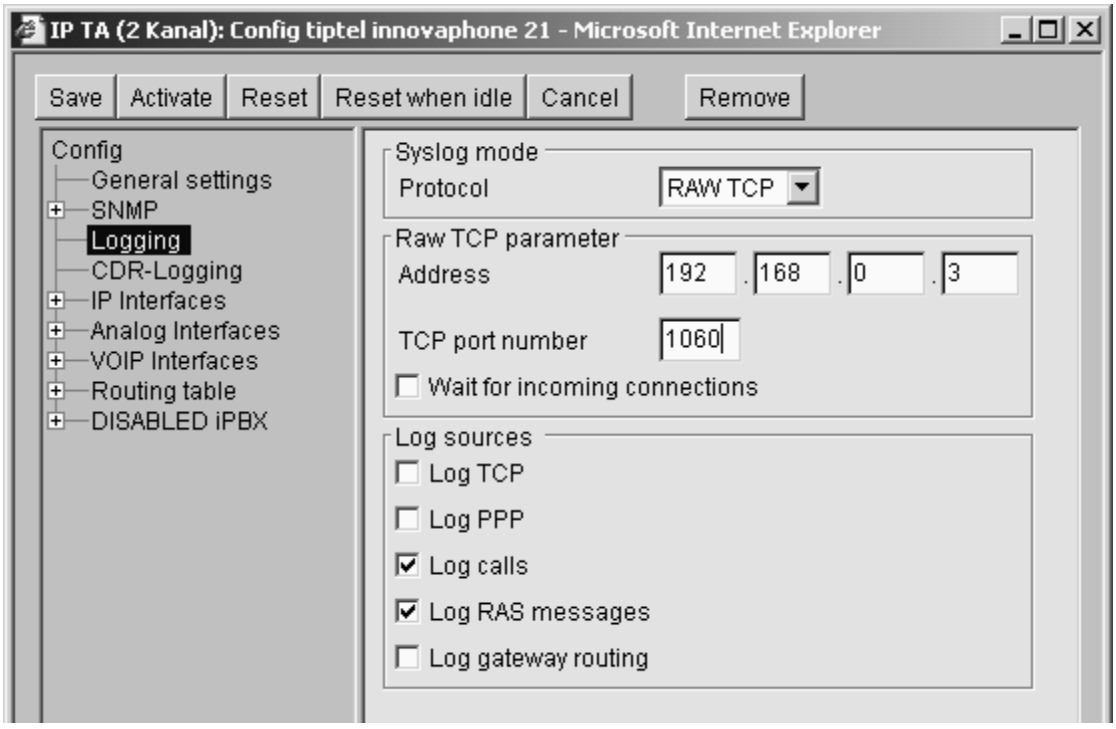
- Transfer of the Syslog entries to a TCP programme

  Here, the gateway writes the Syslog entries to a TCP link. The other end of the TCP link is then responsible for further evaluation of the entries.

  - Select RAW-TCP as SYSLOG MODE
  - Enter the TCP port number of the link under TCP PORT NUMBER in the RAW TCP PARAMETER area
  - If the gateway is to set up the TCP connection independently, enter the destination IP address under ADDRESS
  - If the gateway is to wait for an incoming TCP connection, enter the IP address from which the connection is to come under ADDRESS and mark the WAIT FOR INCOMING CONNECTIONS checkbox

[72] Your gateway will make a HTTP GET request to the Web server on the registered URL followed by the url-encoded log entry. If, for example, you have a page on your Web server with the name `/cdr/cdrwrite.asp` with a form that expects the log message in the `msg` parameter, enter the value `/cdr/cdrwrite.asp?msg=` in the URL-PATH field. Your gateway will then make a `GET /cdr/cdrwrite.asp?event=syslog&msg=`***`logmsg`*** request to the server.

Figure 88 Sending log reports to a Programme



Monitoring the Gateway by SNMP

The gateway offers the possibility of monitoring the operating condition by SNMP. The MIB-II standard is supported, along with a manufacturer-specific MIB. For details about this MIB, consult your dealer or download the MIB files from the download area of the innovaphone Web site (http://www.innovaphone.com).

Figure 89 Configuration of SNMP access

In order to access the gateway via SNMP, proceed as follows:

- ▲ Open the SNMP field of the configuration applet
- ▲ Ensure that the ACCESS parameter is set at either read-only or read-write. If it is set at read-write, certain MIB variables can also be written
- ▲ If you are not using the standard public Community-Name, enter the name in the COMMUNITY field
- ▲ The NAME, CONTACT and LOCATION entries are for information only and hence optional

The gateway can now be monitored via SNMP.

If the gateway is meant to trigger the traps defined in the manufacturer-specific innovaphone® MIB, the destinations for trap messages must also be defined.

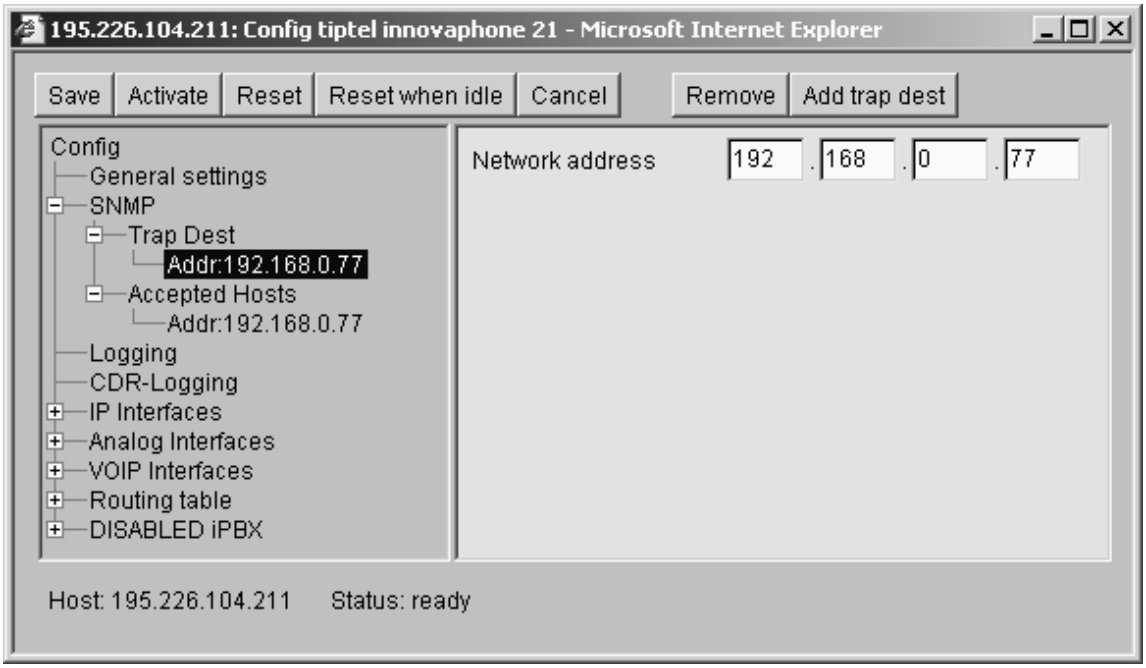
- ▲ Select the TRAP DEST field
- ▲ Click on the ADD TRAP DEST button to add a new destination You can define up to 5 destinations

To increase security, you can limit access to the gateway by limiting access via SNMP to a defined list of hosts.

- ▲ Select the ACCEPTED HOSTS field
- ▲ Click on the ADD HOST button to add the IP address of an authorised host You can define up to 5 authorized hosts

Access via SNMP is only possible if the correct Community-Name is specified . If the AUTHENTICATION TRAP has been checked in the SNMP field, a Trap is generated if access is requested with an incorrect Community-Name.

Figure 90 Adding SNMP Trap Destinations



Transmission of Call Detail Records (CDR)

Your gateway is able to transmit detailed information about calls made. Contact your dealer for further information.

Verifying and saving configuration changes

Your gateway saves the configuration information permanently in non-volatile memory, which means it is also still available after a system restart. With such a system boot the configuration is read from non-volatile memory into the

gateway RAM. This copy is evaluated on start-up and the configuration information obtained is then used during operation.

If the configuration is changed, this is operative initially on the configuration information in working memory. For the new configuration to take effect, the configuration information has to be re-evaluated like it is at system start-up.

This is done via the configuration interface by clicking on the ACTIVATE button. The new configuration is then operative and can be tested. However, the configuration is still not saved to the non-volatile RAM, and will be lost if a cold restart[73] of the gateway occurs. If, after checking, you are satisfied with the new configuration you still need to save it permanently. This is done using the SAVE button.

Figure 91 SAVE, ACTIVATE, RESET, RESET WHEN IDLE and CANCEL buttons

Most changes to the configuration – routing information changes, for example – can be carried out on the gateway without interrupting normal device operation. Some changes, however, require the gateway to perform a warm boot, which will interrupt calls in progress.

The gateway notifies you of this so that calls are not interrupted inadvertently. If you decline the restart (LATER button), you can force a warm boot later on by clicking on the RESET or RESET WHEN IDLE button.

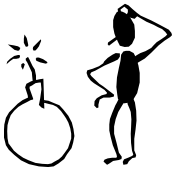
Whereas RESET initiates an immediate warm boot, with RESET WHEN IDLE a warm boot is not initiated until there are no longer any active calls. This averts calls being disconnected by the warm boot.

With improper configuration the gateway may no longer be accessible after the new configuration is activated. This is the case, for example, if an Ethernet interface parameter such as IP address or subnet mask is ill-configured. In such cases the fault can no longer be cleared using the configuration interface.

To avoid this problem, the gateway discards the activated new configuration and restores the previous configuration held in non-volatile memory if no access is made by the configuration interface or via telnet for re-connection within 60

[73] Here, a cold restart is understood to mean a restart after disconnecting the power supply and not a restart by pressing the RESET button.

seconds. After a SAVE, ACTIVATE or RESET the configuration applet automatically reconnects to the gateway. Thus, if successful, the new configuration is automatically retained.



Be aware though, that if the new configuration was stored into the non-volatile memory using the SAVE prior to its activation, there is no valid configuration any more to restore if a problem occurs. For the remote maintenance case, in particular, access to the device may no longer be possible in some instances. It is thus strongly recommended to test any configuration change first of all using ACTIVATE.

If you want to cancel all the changes made since the last SAVE, you can do this with the CANCEL button. On doing so, the current configuration is replaced by the last configuration saved in non-volatile memory.

The browser administration interface

With administration via the Web browser you can:

- monitor the operating status of the device (DIAGNOSTICS field)
- configure the gateway and the gatekeeper (GATEWAY field)
- secure the configuration and load and activate up-to-date firmware (ADMINISTRATION field)
- if installed, configure and monitor the optional iPBX components (IPBX field)

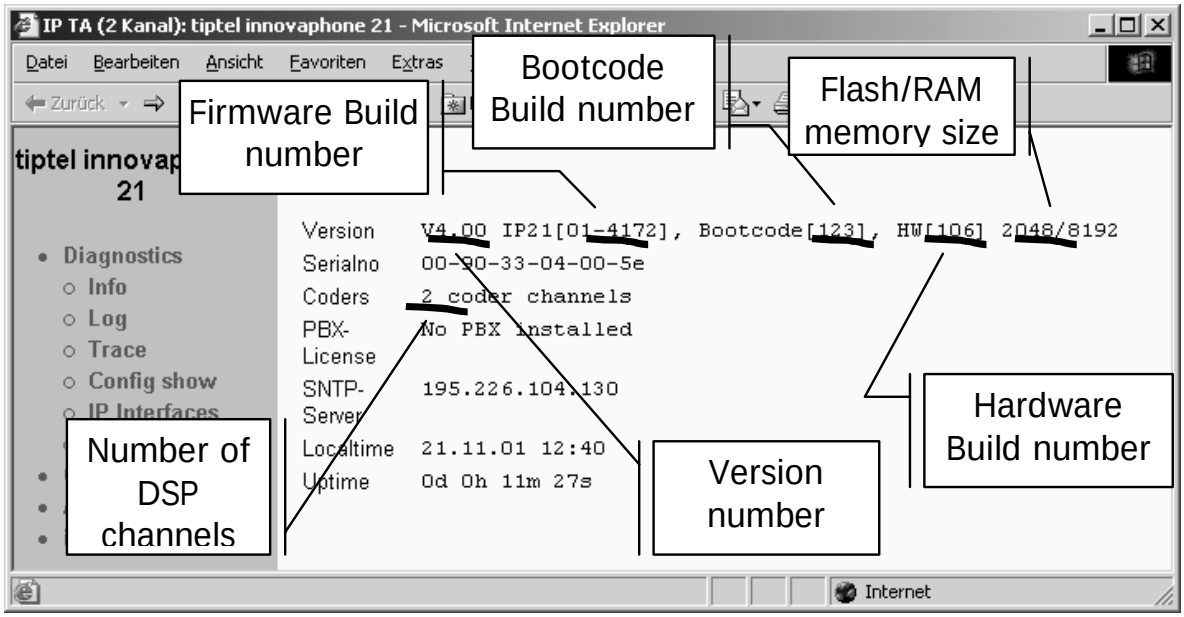
For the administration interface to work properly, your Web browser must meet the following requirements:

- HTTP1.1 protocol
- HTML4.0 protocol
- Frames
- Java Applets

▲ XML/XSL[74]

The administration interface has been tested with Internet Explorer™ 6.x, but can also be used with the Netscape browser.

Figure 92 The browser administration interface



Having connected your Web browser with the IP address of your gateway you will first see its welcome screen. The URL is

http://***xxx.xxx.xxx.xxx***

where ***xxx.xxx.xxx.xxx*** is to be replaced by the gateway's IP address.

The hyperlinks within the upper frame of the browser window allow you to navigate through the various functional areas.

Some areas require you to enter the gateway administrator's used id and password (see page 37).

[74] XML/XSL is only necessary for advanced functions, such as the sorting of lists. The gateways can be fully configured and administered without these functions.

Diagnostics

Info

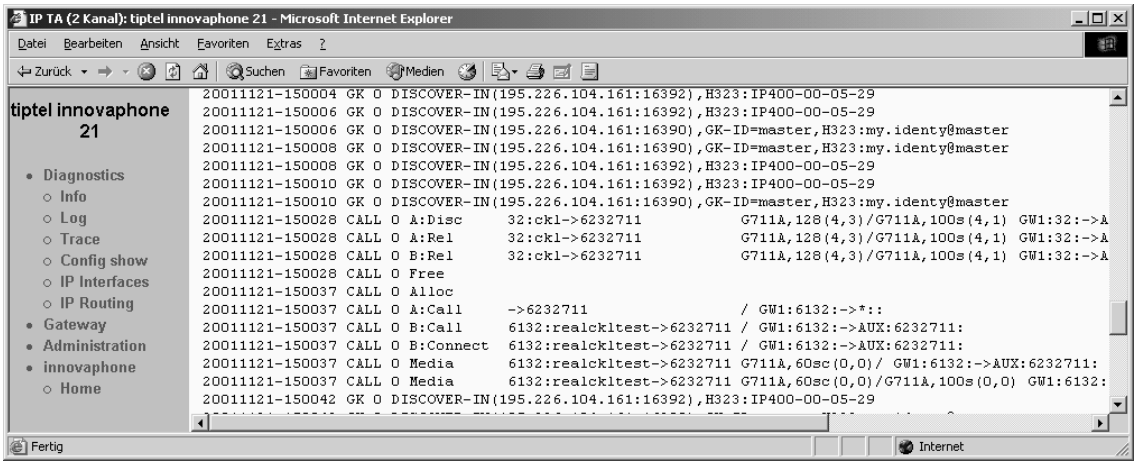
Your gateway's home page (see Figure 92 The browser administration interface) shows information about

- The device's hardware and software versions
- The serial number
- The number of voice channels
- An iPBX licence (if installed)
- The address of the SNTP server used (if configured)
- The local time of the gateway according to the SNTP server and time zone specified
- The operating time since the last cold start or warm restart

Log

This area allows you to view your gateway's log messages directly whilst it is in operation. Messages are continually updated automatically and scroll upwards out of the window.

Figure 93 Log messages display

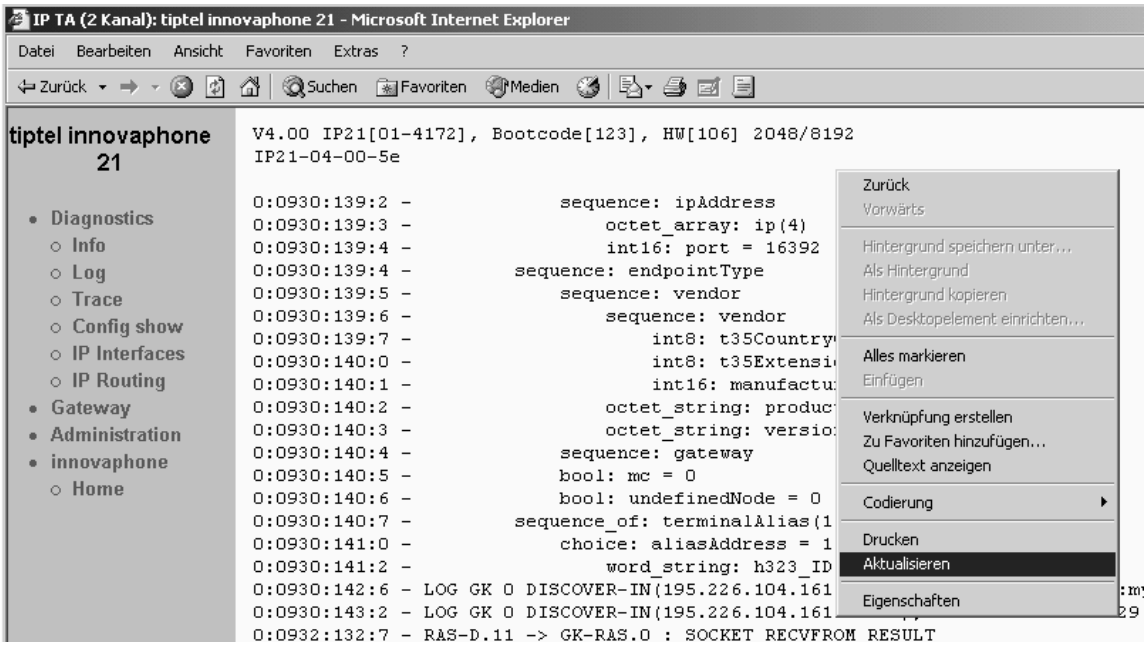


Only those messages are displayed that are configured in the LOGGING area of the configuration applet. The log messages appear here regardless of which PROTOCOL is selected under SYSLOG MODE (see Figure 84 Setting up Syslog events on page 157).

Trace

This area allows you to download trace files from your gateway. You can save the trace in files in a manner similar to the procedure described in the “Config show” section below.

Figure 94 Refreshing the trace window



Please note that the trace information is continually expanding. To obtain a continuous trace the page must be refreshed regularly. Depending on the browser's option settings, this can be done either by clicking on the TRACE link again or by updating the frame in the context menu. Figure 94 Refreshing the trace window shows how this is done in Microsoft™ Internet Explorer™.

IP interfaces

This area lists all of the IP interfaces configured for your gateway showing the current status for each one. Table 25 Entries in the IP Interfaces table below describes the meaning of the entries.

Figure 95 Display of IP interfaces

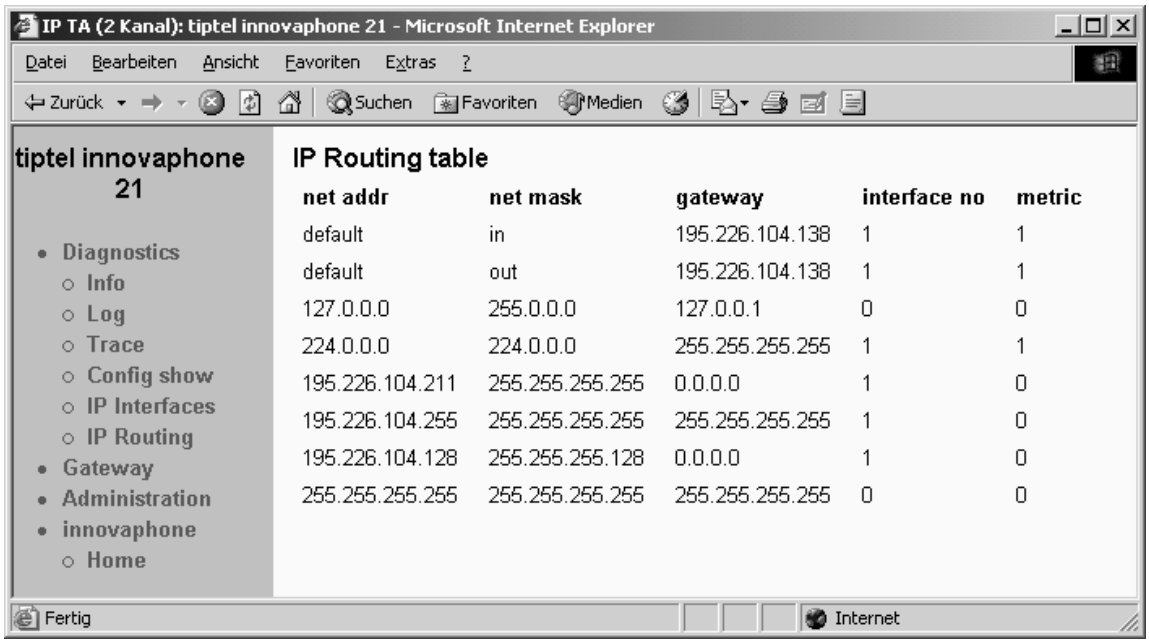
Table 25 Entries in the IP Interfaces table

Column	Meaning	Values
INTERFACE	Type of interface ▲ ETH0: Ethernet interface ▲ PPP*x*: configured logical PPP interface	ETH0, PPP0, PPP1, PPP2, PPP3
STATE	State ▲ UP: ▲ ETH0: Ethernet link is OK ▲ PPPx: the connection is set up and the IPCP protocol has run successfully ▲ Down: other	UP, DOWN
TRIGGERED BY	This column currently has no significance	
ACTION	Alters the call status ▲ CONNECT: initiates a call set-up ▲ CLEAR: closes the connection ▲ DISCONNECT: currently has no significance, please use CLEAR	CONNECT, DISCONNECT CLEAR

IP Routing

This area shows you the current IP routing table.

Figure 96 IP Routing Table



Gateway

Config

The link launches the configuration applet described starting on page 40.

Voice interfaces

This area lists all of the voice interfaces configured for your gateway showing the current status for each one.

Figure 97 Display of voice interfaces

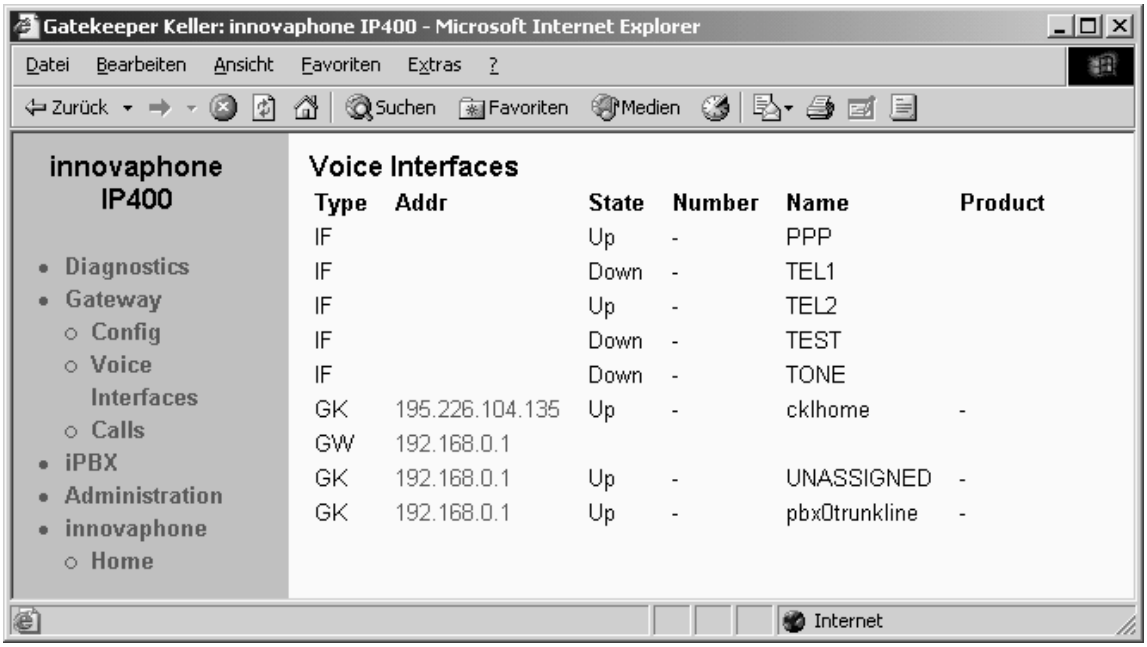


Table 25 Entries in the VOICE INTERFACES table The table below explains the meaning of the entries.

Table 25 Entries in the VOICE INTERFACES table

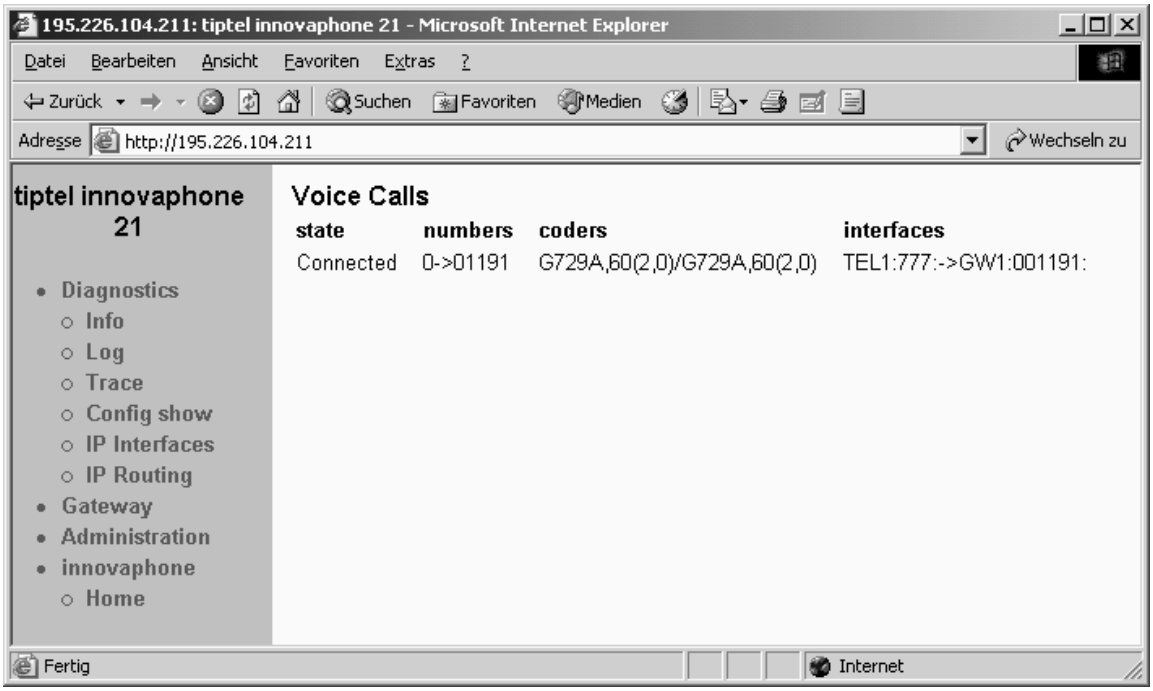
Column	Meaning	Values
TYPE	Type of interface ▲ IF: ISDN interface ▲ GW: gateway registered using RAS ▲ EP: end point registered using RAS ▲ GK: own registration at a gatekeeper	IF, GW, EP, GK
ADDR	IP address ▲ IP address of RAS client for EP and GW ▲ IP address of gatekeepers for GK	Xxx.xxx.xxx.xxx

Column	Meaning	Values
STATE	State of the interface ▲ UP: ▲ IF point to multipoint: layer 1 is set up ▲ IF point to point: layer 2 is set up ▲ IF analogue connections: call is active ▲ GW/EP: the device is registered ▲ GK: registration completed at the gatekeeper ▲ DOWN: other	UP, DOWN
NUMBER	The E.164 address (direct dialling) of the registration ▲ GW/EP: the device's configured direct dialling ▲ GK: E.164 address accompanying the registration ▲ IF: no meaning	Nnn
NAME	Name of interface ▲ IF: interface lettering ▲ GW/EP/GK: the H.323 alias of registration	TEL1, TEL2, TEL, PPP, PRI1, PRI2, DOOR, AUX, TEST, TONE Text
PRODUCT	Manufacturer's code ▲ GW/EP: manufacturer's code of registered device accompanying the registration ▲ Otherwise no meaning	

Calls

In this area you can observe the currently active calls to and from your gateway. If you have the optional iPBX components installed, please note however that internal calls between iPBX subscribers will not be indicated .

Figure 98 Indicator of current calls to and from the gateway



You can find the meaning of the individual columns in table 27.

Table 26 Entries in the CALLS List

Column	Format	Values	Meaning
State		Dialling	Dialling is underway
		Alerting	The dialled correspondent is being called
		Connected	The call is connected
		Clearing	The call has been terminated by one of the parties
Numbers	Caller->Called		
		Caller	The calling line identification of the caller as presented to the called party
		Called	The call number
Coders	ACoders/BCoders		Coder used from A->

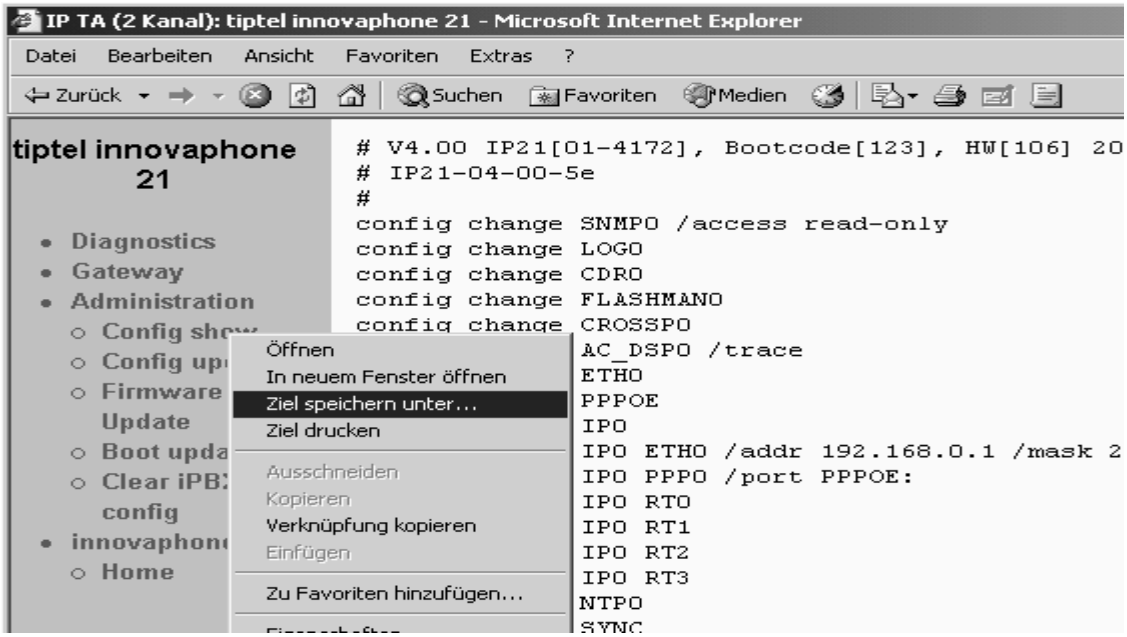
		>B or. B->
	Coder,ms(round,jitter)	Coder: speech compression used (see Speech can be transmitted in various codings. Some of the available codings compress the speech, while others don't. Your gateway supports several of the common voice encoding schemes whose properties are described in the table below: on page 107 Round: Running time in ms Jitter: Variance of running time in ms
Interfaces	sif:cgpn:cgnm->dif:cdpn:cdnm	Sif: Interface for incoming call Cgpn: calling number before routing Cgnm: calling name before routing Dif: Interface for outgoing call Cdpn: called number after routing Cdnm: called name after routing

Administration

Config show

Allows you to output your gateway's current configuration in text form.

Figure 99 Saving the configuration in the Web browser



You can also save the current configuration in a file, in which – depending on the particular browser – you use the SAVE TARGET AS... function . Figure 99 Saving the configuration in the Web browser shows how to do this in Microsoft™ Internet Explorer™.

A configuration saved in this way can be loaded back in again partly or in full using the CONFIG UPDATE link (see page 176). Using this method you can save and reinstate configurations, or create reference configurations as well, and load onto a multitude of devices.

Config update

Allows you to upload onto your gateway a configuration saved with CONFIG SHOW (see above).

Figure 100 Uploading a configuration file

Enter the path and file name of the configuration file to be loaded in the CFG-FILE field and click on the SEND FILE button.

Figure 101 Activating the loaded configuration

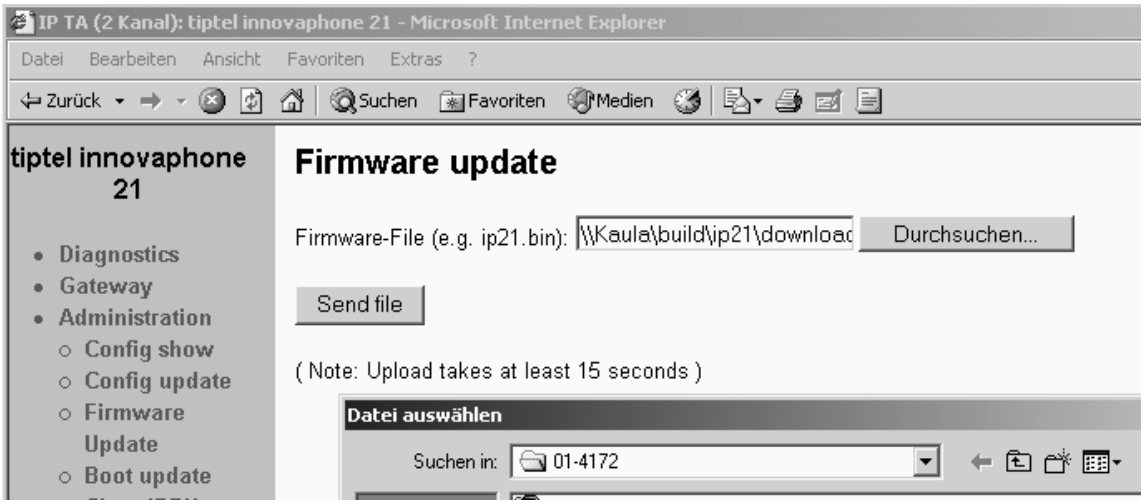
Please note that the configuration information is loaded into the gateway's volatile memory. It is then neither saved permanently nor immediately operative. Therefore, after the upload is completed, you are offered the choice shown in Figure 101 Activating the loaded configuration.

Read the section "Verifying and saving configuration changes" starting page 162, to learn how to validate and save the new configuration.

Firmware update

Allows you to upload a new version of firmware to the gateway. You can obtain new versions of firmware from your dealer.

Figure 102 Updating the firmware



Enter the path name and file name of the firmware file to be loaded in the PROTOCOL-FILE field and click on the SEND FILE button.

When loading the new firmware you will be informed not to interrupt the loading process in any circumstances.

If, despite this, the loading process is interrupted, do not in any event then switch off your gateway. On the contrary, repeat the procedure again once you have cleared the problem.

Take note of the documents that accompany the new versions to determine whether a new boot firmware also needs to be loaded. If this is the case, also take note of the required order of the boot code and firmware update, if specified.

The new firmware is not operative straight away. You have to carry out a reset to activate the new version. For this you are offered the IMMEDIATE RESET and RESET WHEN IDLE links.

Following the successful updating of the firmware, you must always close all browser and applet windows and reboot the browser. This is necessary since the new firmware can may also contain interface elements that can only be activated following reboot.

Figure 103 Resetting the gateway after a firmware upload

Boot update

Allows you to upload new version of boot code to your gateway. New versions of boot firmware can be obtained from your dealer.

Enter the path and file name of the boot firmware file to be loaded in the BOOT-FILE field and click on the SEND FILE button.

Figure 104 Updating the boot firmware

When loading the new firmware you will be informed not to interrupt the loading process in any circumstances.

If, despite this, the loading process is interrupted, do not in any event then switch off your gateway. On the contrary, repeat the procedure again once you have cleared the problem.

The new boot code is not operative straight away. You have to switch the gateway off and then back on again to activate the new version.

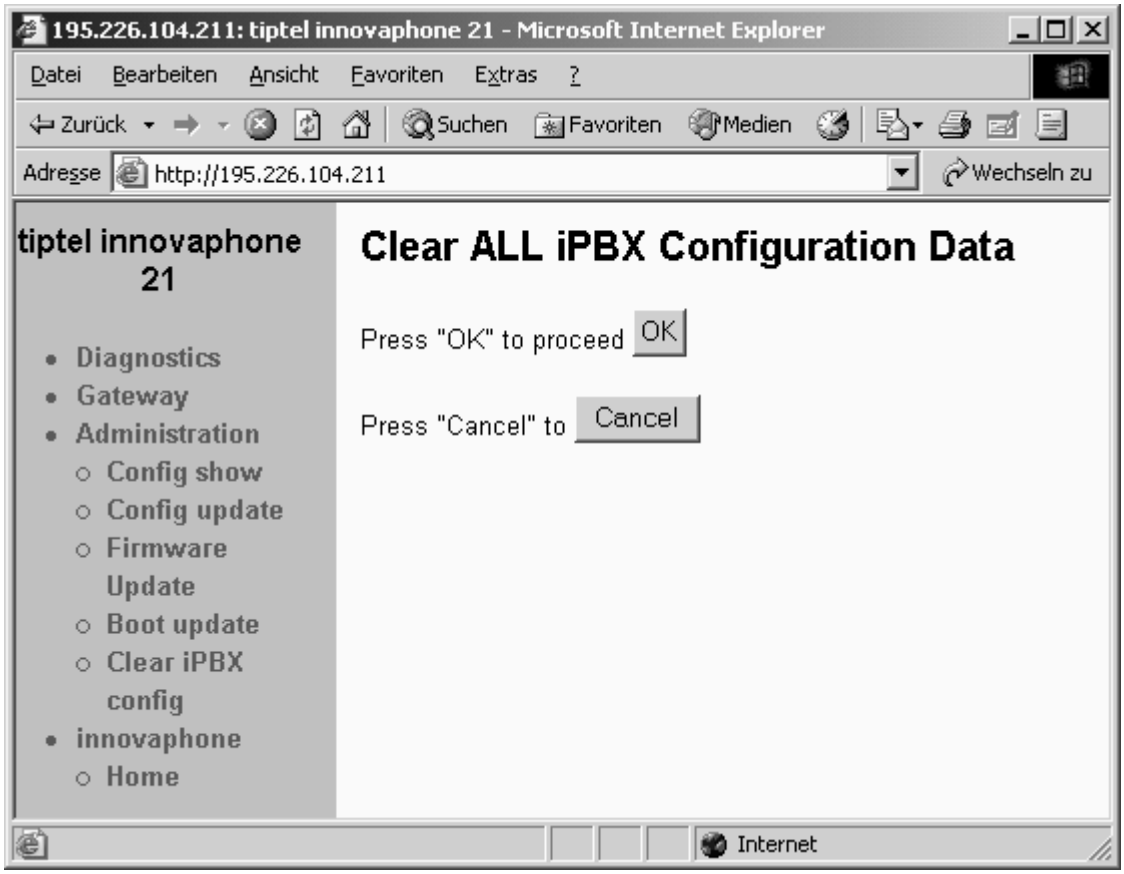
Take note of the documents that accompany the new versions to determine whether a new protocol firmware has to be loaded as well.

Clear iPBX config

This function lets you delete the entire configuration of a given installed iPBX component. This is useful, for example, following the restoration of the standard configuration (see page 30), since it means that the configuration of the iPBX components is not replaced.

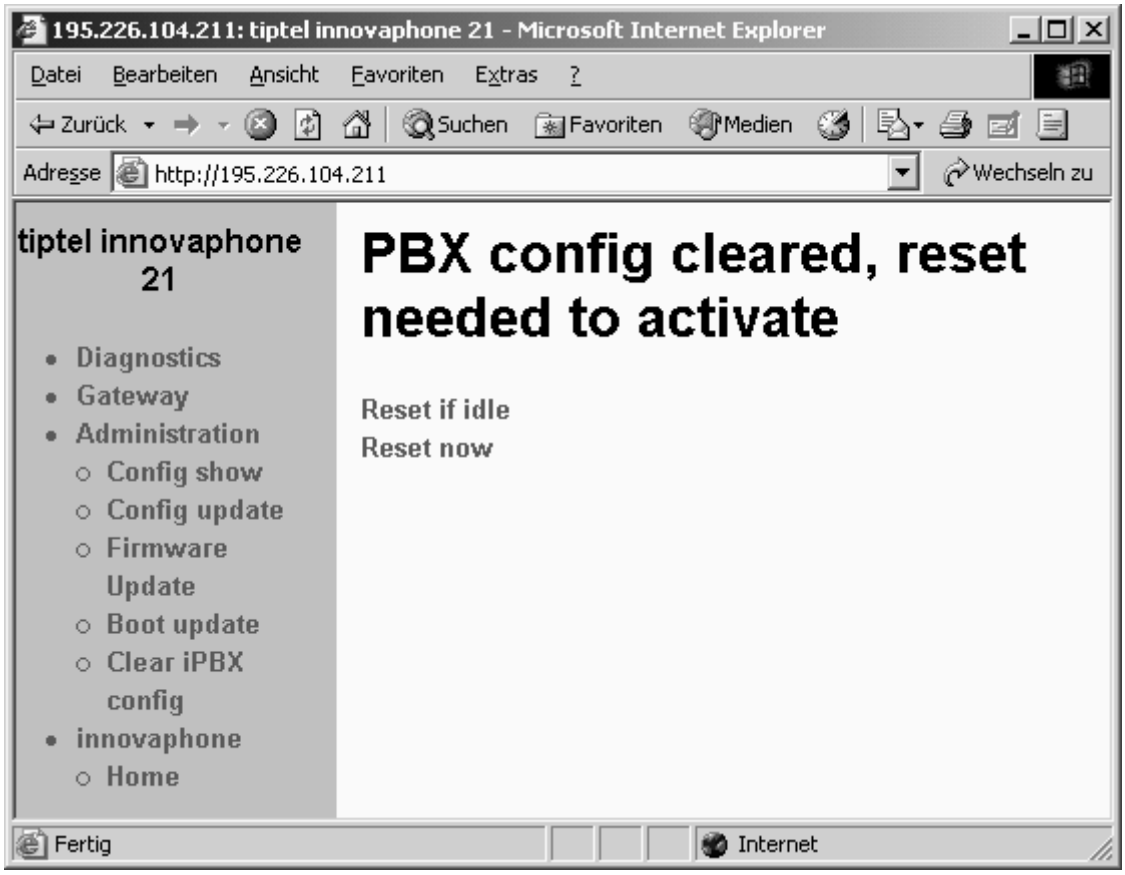
We recommend that you make a backup of the configuration before deleting (see page 175).

Figure 105 Deleting iPBX Data

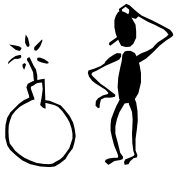


If you click on Clear iPBX you will first of all be asked if you really want to delete the entire configuration. If you confirm, the iPBX configuration will be entirely deleted. You must carry out a reset subsequently. You may choose whether this occurs straight away or only when the gateway is in idle status.

Figure 106 Reset after clearing the iPBX configuration



Safety instructions for the IP 21



For your personal safety please follow the guidelines below.

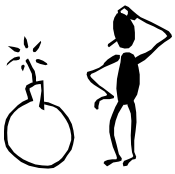
- Installation and fitting (if required) of the equipment is to be carried out by suitably qualified personnel only.
- When installing, make certain the equipment has adequate ventilation, particularly if fitting into closed cabinets.
- The equipment is suitable for operation in dry areas only.
- Use only the plug-in mains adapter supplied to run the equipment. This adapter is an integral part of the device and should not be replaced by any other.
- The device's plug-in mains adapter is designed to operate from 230V, 50Hz a.c. mains. Never attempt to run the adapter off any other electrical supply!
- The mains socket-outlet must be close to the device and easily accessible. The only way to switch off the device is to disconnect the power supply.
- The device has 2 RJ11, one RJ45, one 3.5mm jack und one strip terminal connections.
  - The RJ11 jacks are intended solely for connecting analogue terminal equipment. You should, in particular, never connect and analogue trunk line here.
  - The RJ45 jack is intended solely for connecting an Ethernet Hub or Switch.
  - The 3.5mm jack bush is intended solely for connecting an audio source.
  - The strip terminal is intended solely for connecting a door intercom according to the directions on page.

  Make sure that connections are only used as they are designed to be used!
- When used as intended and maintained as specified there is never any need to open the device. Should you decide to open the device for any reason,

however, make certain that all connecting leads have been removed beforehand.

This manual describes the innovaphone® VoIP Gateways IP 21, IP 400 and IP 3000. In terms of their design, these devices are largely identical and vary only in terms of the type and quantity of the physical interfaces. Any differences are explained in the text.

Safety instructions for the IP 400



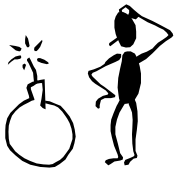
For your personal safety please follow the guidelines below.

- Installation and fitting (if required) of the equipment is to be carried out by suitably qualified personnel only.
- When installing, make certain the equipment has adequate ventilation, particularly if fitting into closed cabinets.
- The equipment is suitable for operation in dry areas only.
- Use only the plug-in mains adapter supplied to run the equipment.
- The device's plug-in mains adapter is designed to operate from 110V-240V, 50Hz a.c. mains. Never attempt to run the adapter off any other electrical supply!
- The mains socket outlet must be close to the device and easily accessible. The only way to switch off the device is to disconnect the power supply.
- The device has several RJ45 jacks. Five of them (2 * TEL1, 2 * TEL2, 1 * PPP) are intended solely for connecting ISDN terminal equipment, -trunk lines or –PABXs. One (ETHERNET) is intended solely for connecting an Ethernet hub or switch. Make certain that you do not mix up the connections, since they are compatible physically!
- Do not connect standard telephones or any other devices not mentioned to any of the RJ45 jacks!
- When used as intended and maintained as specified there is never any need to open the device. Should you decide to open the device for any reason,

however, make certain that all connecting leads have been removed beforehand.

This manual describes the innovaphone® VoIP Gateways IP 21, IP 400 and IP 3000. In terms of their design, these devices are largely identical and vary only in terms of the type and quantity of the physical interfaces. Any differences are explained in the text.

Safety instructions for the IP 3000



For your personal safety please follow the guidelines below.

- ▲ Installation and fitting (if required) of the equipment is to be carried out by suitably qualified personnel only.
- ▲ When installing, make certain the equipment has adequate ventilation, particularly if fitting into closed cabinets.
- ▲ The equipment is suitable for operation in dry areas only.
- ▲ The device is designed to operate from 110V-230V, 50Hz a.c. mains. Never attempt to run the device off any other electrical supply!
- ▲ The mains socket-outlet must be close to the device and easily accessible. The only way to switch off the device is to disconnect the power supply.
- ▲ The device has several RJ45 jacks. Three of them (PRI1, PRI2, S/T) are intended solely for connecting ISDN terminal equipment, -trunk lines or –PABXs. One (ETHERNET) is intended solely for connecting an Ethernet hub or switch. Another (CONSOLE) is intended solely for connecting a V.24 connecting cable.

  Make certain that you do not mix up the connections, since they are compatible physically!
- ▲ Do not connect standard telephones or any other devices not mentioned to any of the RJ45 jacks!!

- When used as intended and maintained as specified there is never any need to open the device. Should you decide to open the device for any reason, however, make certain that all connecting leads have been removed beforehand.
- When fitting into a 19'' cabinet using the mounting brackets, use solely the screws supplied or countersunk 6mm long M4 screws

This manual describes the innovaphone® VoIP Gateways IP 21, IP 400 and IP 3000. In terms of their design, these devices are largely identical and vary only in terms of the type and quantity of the physical interfaces. Any differences are explained in the text.

Clearing problems

Typical problems

In our experience certain problems occur more frequently than others. Table 27 below lists these problems and gives advice in how to resolve them.

Table 27 Fault clearance

Symptom	Description	Remedy
Gateway does not respond. READY, LINK and ACT. LEDs(with the IP 400) are on permanently	Gateway is waiting for a firmware download	▲ Do a quick reset by pressing the RESET button
Gateway does not respond READY LED is on, LINK LED is off	The Ethernet link does not work	▲ Check position of "CONNECT TO ..." switch (see page 14) ▲ Check the Ethernet cabling
Gateway does not	Gateway's configured	▲ Configure the IP parameters

Symptom	Description	Remedy
respond READY and LINK LEDs are on, ACT. LED flashes when access attempted	IP address is incorrect	correctly (see page 34)
In the state as shipped, gateway does not assign the PC an IP address	After switching on, the DHCP client is active	▲ Press the reset button briefly ▲ Get an IP address assigned to the PC again
A telephone attached to TEL1 or TEL2 (IP 400 only). It's display does not show anything	The telephone is lacking power from ISDN line	▲ Tick the POWER checkbox in the interface configuration
A terminal device attached to TEL1 or TEL2 does not work reliably (IP 400 only).	The bus termination is missing	▲ Verify that the ISDN bus wiring connected to the interface is correctly terminated ▲ If the termination is missing, tick the 100 OHM TERMINATION checkbox in the interface configuration (see page 76) ▲ If the termination is ok, clear the 100 OHM TERMINATION checkbox in the interface configuration (see page 76)
Incoming calls are received properly, but no callback is possible using the display calling line ID	The Calling Line ID is incomplete, because the trunk line access code is missing	▲ Configure the trunk line access code for the respective interface the call comes in on (see page 132) or activate the automatic CLI correction (see page 134)
Calls can be set up to a remote VoIP device, but no communication is possible	The required bandwidth for the voice data stream is not available	▲ Configure a more efficient speech coding scheme for the remote gateway (see page 1)
Calls can be set up to a remote VoIP device, but no speech connection comes about	The media channel cannot be set up because the two VoIP devices do not have a common voice encoder	▲ Make certain that the EXCLUSIVE checkbox is deactivated (see page 107)

Symptom	Description	Remedy
Calls can be set up to a remote VoIP device, but no speech connection comes about	The media channel cannot be set up because no IP routing is possible between the two VoIP devices	Only the media channel is set up directly between the two VoIP devices, all signalling links run via the gatekeeper. ▲ Make certain that both VoIP devices have a correct IP routing configuration, particularly subnet masks and standard gateways
Calls to a remote telephony gateway are always rejected by the gateway	The gateway does not support overlapped sending	▲ Insert a hash mark ("#") into the number prefix of the route entry that directs the call to the remote gateway. This enforces en-bloc dialling (see page **Fehler! Textmarke nicht definiert.**)
The gateway loses its configuration information after the power is disconnected	The configuration has not been saved in non-volatile memory	▲ Save the configuration to non-volatile memory after any successful change (see page 162)
A telephone attached to TEL1 or TEL2 works, but does not get a dial tone (IP 400 only)	No route is defined for the respective interface.	▲ Define at least one route entry valid for the respective interface.
Connection of the gateway to the network is behind a "Firewall", and the device cannot be accessed for configuration.	The firewall does not allow the necessary access to the gateway.	▲ Enable the services tcp/23 (telnet) and tcp/80 (http) for the gateway in the firewall.
Connection of the gateway to the network is behind a "Firewall", and no calls can be placed to other VoIP devices.	The firewall does not support the H.323 protocol.	▲ Enable "H.323 Firewalling" in your firewalling software and if necessary "H.323 NAT" as well. Consult your firewall documentation about this. ▲ Read up on this in "NAT and Firewalls" from page 189 onwards

Symptom	Description	Remedy
You are using the gwload.exe utility. Although the gateway is found, uploading of new firmware fails.	Your computer's arp-cache holds outdated information.	▲ Clear the computer's arp-cache. For this, with Windows95/98™ and Windows NT™ and its derivatives use the command arp –d ip-addr.
Fax transmissions break down	T.38 is not authorised in the gateway definition	▲ Activate the T.38 protocol (see page 105f)
Fax transmissions break down, in particular for lengthy faxes	The gateway and PABX to which the fax machine is connected do not have an asynchronous ISDN clock	▲ Implement correct clock synchronisation (see page 80)

NAT and Firewalls

If there is a firewall protecting your network from the Internet and you aim to set up calls with the gateway to remote terminals via the Internet, you need to ensure that the firewall is suitably configured.

Firewalls typically fulfil two tasks. They control access to devices and network areas within your network, and they implement the IP address translation in networks that do not have their own conventional network address (so-called "NAT", network address translation). "NAT" can also be implemented by routers.

The implementation of both functions when applied to "voice over IP" calls for detailed analysis of the data stream by your firewall or router firmware. Please refer to the respective documentation of the product you are using.

If the product you use does not support "H.323 Firewalling", there are two ways to deal with the situation:

▲ The firewall is configured such that it allows *all* required data from and to the gateway.

  While this solution is usually not well received by system administrators, it does not present a security problem in the gateway's case. This is because it is a dedicated device not performing any services other than "voice over IP".

Consequently, no security gaps in your network result from opening the path from and to the gateway.

If the H.323 devices, whose data is to cross the firewall, are solely innovaphone® devices, the number of ports to be released can be restricted. For this, however, the H.245 TUNNELLING checkbox must be ticked in the gateway definitions for all devices (see section "H.323 protocol options" from page 105 onwards).

The following ports have to be released in both directions:

- Tcp: destination port 23 (telnet), any source port, to be configured
- Tcp: destination port 80 (http), any source port, to be configured
- Tcp: destination port 1720 (h.225), any source port for VoIP calls
- Udp: destination port >= 2050, source port 5004 and 5005 (RTP), for VoIP calls

If the RAS protocol is used, the following also need to be released:

- Udp: Destination port 1718
- Udp: Destination port 1719
- Udp: Source port 1719

If the gateway has to communicate with third-party products, the number of ports to be released cannot be restricted. It is therefore necessary to release all ports from and to the gateway.

▲ The gateway is located *in front* of the firewall, which means that the data stream doe not need to pass the firewall. However, keep in mind that there is no way to establish calls from within your network to the gateway (e.g. with PCs running NetMeeting™).

If your network is operated in NAT mode and the product you use does not support any "H.323 NAT", operation across the firewall is not possible.

VoIP and heavily loaded WAN links

If voice data is transmitted over heavily loaded narrowband WAN links, there may be a drop in voice quality if the respective links can no longer ensure adequate transmission quality (see “Speech can be transmitted in various codings. Some of the available codings compress the speech, while others don't. Your gateway supports several of the common voice encoding schemes whose properties are described in the table below:

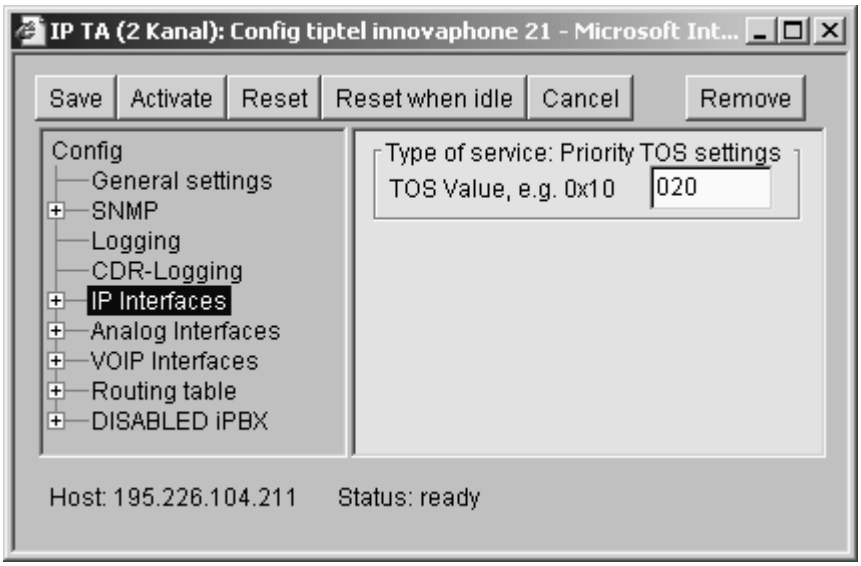
Prioritisation of voice data on the WAN links can assist here. The routers used can generally achieve this.

If your router supports "Prioritisation of voice data to H.323", direct use can be made of this.

If your router is able to prioritise based on the IP type of service (TOS) field, you can use this function. In all IP packets that the gateway sends, it sets the TOS field to 0x10. Where necessary, you can alter this value in the configuration applet in the IP INTERFACES in the TOS VALUE field[75].

If this is not the case, you can get by with the function "Prioritisation according to source- /destination address", if available. This will prioritise data packets from and to the gateway. This in effect corresponds to the prioritisation of voice data as above.

Figure 107 Setting the TOS value for voice data



In any case, the size of packets transmitted over the WAN link (often referred to as MTU Size) should be restricted to a value of less than 800 bytes. This will ensure that, in spite of prioritisation of voice data, larger data packets do not block the line for an extended period during the transmission.

Some routers, although able to prioritise, cannot interrupt the transmission of larger packets once it has started. This can lead to poor quality despite

[75] You can specify the value in hexadecimal, octal or decimal, the entries `0x10`, `020` and `16` are equal in value. Bear in mind that the value for the TOS field should be set the same on all devices.

prioritisation. In cases such as this, check whether this interruption can be connected separately[76].

If you need to call Technical Support

Whenever you need to contact your dealer for support, please be sure to have the following information to hand:

- ▲ the complete configuration as shown by CONFIG SHOW (see page 175)
- ▲ a trace which captures the error situation (see page 167)
- ▲ the complete version identifier of your gateway. You will find this on the gateway's greeting page (see page 165)
- ▲ the serial number. You will find this on the certification sticker on the bottom of the device or on the gateway's greeting page (see page 165)

ISDN error codes

The following table lists the error codes (ISDN cause codes) defined in the Q.931 standard.

Table 28 ISDN error values

Error code (hex)	Error code, Bit 8 set to 1 (hex)	Error code (decimal)	Meaning
0x1	0x81	1	Unallocated number
0x2	0x82	2	No route to specified transit network
0x3	0x83	3	No route to destination
0x6	0x86	6	Channel unacceptable
0x7	0x87	7	Call awarded and being delivered in an established channel

[76] Some routers refer to this function somewhat confusingly as interleaving.

Error code (hex)	Error code, Bit 8 set to 1 (hex)	Error code (decimal)	Meaning
0x10	0x90	16	Normal call clearing
0x11	0x91	17	User busy
0x12	0x92	18	No user responding
0x13	0x93	19	No answer from user (user alerted)
0x15	0x95	21	Call rejected
0x16	0x96	22	Number changed
0x1A	0x9A	26	Non-selected user clearing
0x1B	0x9B	27	Destination out of order
0x1C	0x9C	28	Invalid number format
0x1D	0x9D	29	Facility rejected
0x1E	0x9E	30	Response to STATUS ENQUIRY
0x1F	0x9F	31	Normal, unspecified
0x22	0xA2	34	No circuit/channel available
0x26	0xA6	38	Network out of order
0x29	0xA9	41	Temporary failure
0x2A	0xAA	42	Switching equipment congestion
0x2B	0xAB	43	Access information discarded
0x2C	0xAC	44	Requested circuit/channel not available
0x2D	0xAD	47	Resources unavailable, unspecified
0x31	0xB1	49	Quality of service unavailable
0x32	0xB2	50	Requested facility not subscribed
0x39	0xB9	57	Bearer capability not authorised
0x3A	0xBA	58	Bearer capability not presently available
0x3F	0xBF	63	Service or option not available, unspecified
0x41	0xC1	65	Bearer capability not implemented
0x42	0xC2	66	Channel type not implemented
0x45	0xC5	69	Requested facility not implemented
0x46	0xC6	70	Only restricted digital information bearer capability is available
0x4F	0xCF	79	Service or option not implemented, unspecified
0x51	0xD1	81	Invalid call reference value
0x52	0xD2	82	Identified channel does not exist
0x53	0xD3	83	A suspended call exists, but this call identity does not
0x54	0xD4	84	Call identity in use
0x55	0xD5	85	No call suspended
0x56	0xD6	86	Call having the requested call identity has been cleared
0x58	0xD8	88	Incompatible destination
0x5B	0xDB	91	Invalid transit network selection
0x5F	0xDF	95	Invalid message, unspecified
0x60	0xE0	96	Mandatory information element missing
0x61	0xE1	97	Message type non-existent or not implemented
0x62	0xE2	98	Message not compatible with call state
0x63	0xE3	99	Information element non-existent or nor implemented
0x64	0xE4	100	Invalid information element contents
0x65	0xE5	101	Message not compatible with call state
0x66	0xE6	102	Recovery on timer expiry
0x6F	0xEF	111	Protocol error, unspecified
0x7F	0xFF	127	Interworking, unspecified

Technical Data

IP 21 interfaces	
1 or 2	a/b interfaces for connecting analogue terminals
1	4+n strip terminal for connecting a door intercom
1	Ethernet 10/100-BASE-T (auto-negotiation)
1	3.5m stereo jack for connecting an analogue audio source

IP 400 interfaces	
2	Basic rate S/T interfaces with s/w configurable TE-/NT-mode as well as phantom powering (up to 4W) and bus termination. No power supply needed through a network terminator (NT)
1	Basic rate S/T interfaces in TE mode
1	Ethernet 10-BASE-T

IP 3000 interfaces	
1	Primary rate (E-1 PRI) interface, TE mode
1	Primary rate (E-1 PRI) interface, NT mode
1	Basic rate S/T interface, TE mode
1	Ethernet 10/100-BASE-TX (auto-negotiation)

IP 21 Hardware	
Enclosure	210 x 134 x32 mm
Power supply	Fixed plug-in mains adapter
	In: 230V AC 50, 75mA
Memory	8 MB DRAM,
	4 MB Flash,
	Remotely upgradeable
CPU	RISC CPU for protocol data processing

IP 21 Hardware	
	Digital signal processor (DSP) for compression of up to 2 calls concurrently
Temperature range	Operating temperature: 0 °C to +45 °C, 10% to 90% relative humidity, non-condensing
	Storage: -10 °C to +70 °C
Weight	610 g

IP 400 Hardware	
Enclosure	210 x 134 x32 mm
Power supply	Plug-in mains adapter
	In: 110V-240V AC +10%-15%, 50/60Hz, 250mA
	Out: 12V DC 800mA
Memory	1 to 4 MB DRAM,
	512 kB to 2 MB flash,
	Remotely upgradeable
CPU	RISC CPU for protocol data processing
	Digital signal processor (DSP) for compression of up to 4 calls concurrently
Temperature range	Operating temperature: 0 °C to +45 °C, 10% to 90% relative humidity, non-condensing
	Storage: -10 °C to +70 °C
Weight	680 g

IP 3000 Hardware	
Dimensions	42.4 x 29.2 x 4 cm
	19” form of construction, 1 height module
Power supply	Internal power supply unit 230V AC + 10% - 15% 47 – 62 Hz, 25 W
Memory	16MB SDRAM, 4MB Flash, remotely upgradeable

CPUs	RISC CPU for protocol data processing Digital Signal Processor (DSP) for voice processing (modular upgrades for 10, 20 or 30 channels in parallel)
Temperature	Operating temperature: 0° C to 45° C, 10% to 90% relative humidity, non-condensing storage: -10° C to 70° C
Weight	4000g

Protocols	
Internet	IP, TCP, UDP, RTP, DHCP, TFTP, ICMP, SNTP, PPP, PPPoE, LDAP
Configuration	Telnet, http, SNMP
ISDN	ETSI DSS1, Q.SIG
Voice over IP	H.323, H.225, H.245, RAS, T.38
Speech coding	G.711 A-law, G.711 µ-law, G.723.1 5.3 and 6.3 kbps with Voice Activity Detection (VAD) and Comfort Noise Generation (CNG), G.729A G0.726
Echo compensation	G.165
Special features	Overlapped or non-overlapped sending, Supports multiple MSNs, Supports presentation of calling MSN (Calling Line Identification), Conveys the sub-addressing Supports call progress tones, Supports trunk groups (pooling) Point-to-point and point-to-multipoint operation possible Static voice routing IP <-> ISDN Static data routing PPP via ISDN, dial- and permanent connection, NAT, PPTP, TOS, voice data prioritisation

Protocols	
	Operation with built-in or external gatekeeper
	Gatekeeper for H.323 third-party devices

innovaphone