VoIP Gateways

IP 400

administrator manual

innovaphone

Pure IP-Telephony

Release 5.01, 2nd edition, April 2005

PDF version available for download at:
http://www.innovaphone.com

Böblinger Str. 76 71065 Sindelfingen, Germany

Tel +49 (70 31) 7 30 09-0 Fax +49 (70 31) 7 30 09-99

http://www.innovaphone.com

VoIP Gateways

IP 400

Version 5.01
Manual

Table of contents

1 About this manual

This manual describes the innovaphone VoIP gateway IP 400.

The manual describes the operation of the equipment as a gateway and as a gatekeeper. Please refer to the innovaphone "PBX administrator's manual", supplied together with your licence, if you also wish to use the device as a telephone exchange.

This manual is an integral part of the equipment. All advice and instructions contained therein should be followed carefully and the equipment should only be used as specified. The manufacturer assumes no responsibility for any personal injury, damage to property or subsequent damage that can be attributed to improper use of the device.

Some screenshots stem from other innovaphone products. But they are of the contents the same as the IP 400 ones.

Caution

Observe the safety instructions specified in the respective manuals at all times.

1.1 Notes, tips and cautions

Note

Notes provide you with information, that you may first need to become familiar with, in order to configure the gateways properly.

Tip

Tips provide you with information on how to use the gateways in a particularly easy or convenient way.

Caution

Pay attention to these fields, to prevent damage to the gateways or other equipment, and to ensure your own safety.

2 Introduction, commissioning and installation of the VoIP gateway

2.1 Connections and user controls IP 400

2.1.1 Connections on the rear side

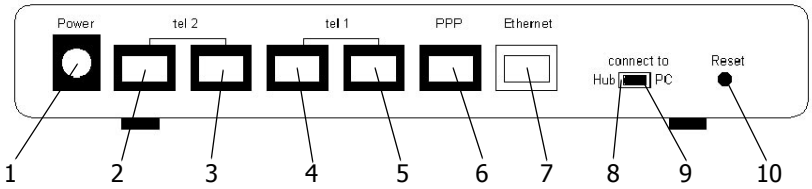

Fig. 1 The IP 400 connections

The following connectors/switches can be found on the back of the gateway (from left to right):

Pos	Name	Function
1	**Power**	For the delivered power supply, 12 V 900 mA
2	**tel2 (first socket)**	RJ 45-socket. For an ISDN-telephone, -PBX or -exchange line
3	**tel2 (second socket)**	RJ 45 -socket. For the optional connection of a second telephone to **tel2**
4	**tel1 (first socket)**	RJ 45-socket. For an ISDN -telephone, -PBX or -exchange line
5	**tel1 (second socket)**	RJ 45-socket. for the optional connection of a second telephone to **tel1**
6	**PPP**	RJ 45. To connect to an ISDN -exchange line

Pos	Name	Function
7	**Ethernet**	RJ 45-socket. To connect to 10 Mbit/s Ethernet (10_{BASE-T})
8	**connect to Hub**	Switch to the left, when connecting the IP 400 **Ethernet** interface to a hub.
9	**connect to PC**	Switch to the right, when connecting the IP 400 **Ethernet** interface directly to a PC.
10	**Reset**	Button to restart the gateway.

Table 1 Connectors and control elements of the IP 400

2.1.2 Indicators on the front

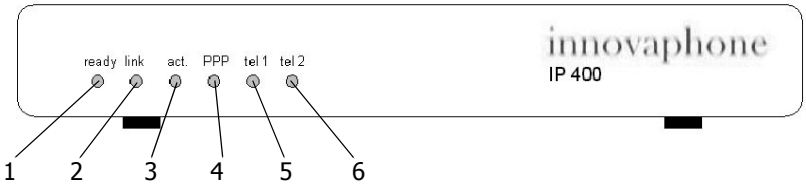

Fig. 2 IP 400 lamps

The following status LEDs can be found on the front of the gateway (from left to right):

Pos	Name	Description
1	**ready**	The LED lights red, when booting The LED lights green, when ready for operation The LED flashes, when downloading
2	**Ethernet link**	The **Ethernet** connection is ready for data transmission.
3	**Ethernet act.**	Data is being transmitted or received via the **Ethernet** connector.
4	**PPP**	The exchange line on the **PPP** connector is active.

Pos	Name	Description
5	**tel1**	The device or exchange line on the **tel1** connector is active.
6	**tel2**	The device or exchange line on the **tel2** connector is active.

Table 2 IP 400 indicators

Caution

If the **ready** LED flashes, when downloading, this process may not be interrupted. Otherwise, the equipment may be damaged.

2.1.3 The IP 400 serial number label

The serial number label is on the underside of the housing.

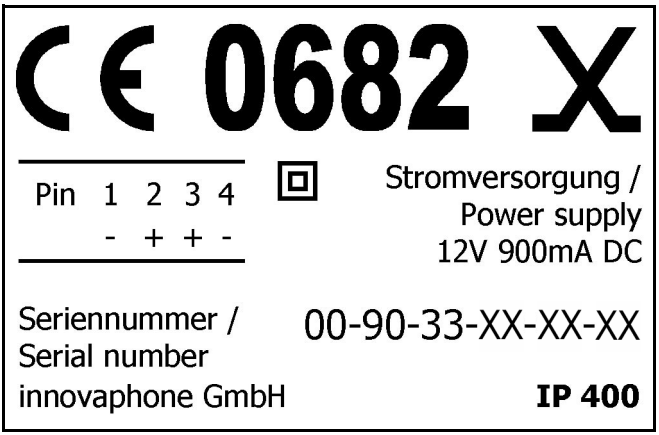

Fig. 3 The serial number label

The last three hexadecimal numbers ('XX-XX-XX' in the illustration) separated by a hyphen ('-') represent the serial number of your IP 400, while the first three hexadecimal numbers are innovaphone's, fixed, manufacturer's identification code.

The serial number is also the MAC address of your IP 400.

2.1.4 Commissioning and Installation of the IP 400

The following steps are required to commission the gateway:

- Wire up the connections as described above.
- Set the IP- interface parameters, see section 2.2 "Configuration of access to the local network" from page 11.
- To define the operational configuration, see section 4 "Configuration of the IP interfaces" from page 24.

The following sections are based on the assumption that the gateway is in the same condition as delivered and that therefore the standard configuration is loaded. We recommend restoring the standard configuration first, if you are not sure about the state of the configuration (see section 2.2.1 "Generating the standard configuration" from page 11).

Note the section "Safety instructions for the IP 400" from page 138.

The IP 400 is suitable for wall mounting. The horizontal distance between the suspension points is 12 cm. Take care not to damage the protective film of the PCB when mounting the IP 400.

The devices can be stacked. Make sure there is adequate ventilation if the gateway is to be installed in a cabinet.

For installation in a 19" cabinet, there is a special frame available which can accommodate two IP 400 gateways.

2.2 Configuration of access to the local network

The gateway is delivered with a standard configuration. In this configuration, the gateway will try to configure the IP parameters via DHCP. The installed DHCP client is thus active and the DHCP server, which is also incorporated, is deactivated.

Ask your network administrator whether your network has a DHCP server.

Refer to section 2.2.4 "Setting the IP-interface parameters without DHCP" from page 16 if there is no DHCP server in operation in your network or if, for some other reason, you do not want to have automatic configuration via DHCP. In this case your PC also needs to be provided with a twisted-pair Ethernet adapter (10 Base-T for the IP 400).

Refer to section 2.2.3 "Setting the IP-interface parameters via DHCP" from page 13, if a DHCP server is available.

In both cases you can access the gateway via Ethernet.

2.2.1 Generating the standard configuration

Tip

You can return to the standard configuration at any time by pressing the reset button, and holding it down for a few seconds. This takes about 5 seconds for the IP 400.

That will result in the gateway being re-initialised and will be put into a special reset mode. It can then be reset to normal operating mode by being switched on and off.

Tip

Press the reset button again, briefly, to return the gateway to normal operating mode. In this case however, the DHCP server mode will be activated (see from page 16 onwards), whereas the DHCP client mode (see page 13) will be activated after switching the gateway on/off.

Bear in mind though, that you will lose all of the preceding configuration data as a result of this procedure. If required, you can save the current configuration in a file, beforehand.

2.2.2 Switching on the gateway

Caution

Connect the gateway to the nearest wall socket using the supplied external power supply (IP 400, 100-240 V).

Only use the external power supply. Other power supplies could damage the gateway.

The mains socket must be close to the device and easily accessible. The only way of interrupting the power supply to the device is by removing the mains lead of the device, or of the external power supply, from the mains socket.

The equipment is now powered up and the **READY LED** is illuminated.

2.2.3 Setting the IP-interface parameters via DHCP

... for experts

- There are basically two ways of configuring an IP address for your gateway.
- When delivered from the factory, DHCP is in an automatic mode. You can force the DHCP into automatic mode with a long reset (at least 3 seconds).
- With a short reset, DHCP server mode is activated and the gateway is allocated the IP address 192.168.0.1.
- It is most definitely better to use the gateway in DHCP client mode. To do this, you need a DHCP server in the network.
- If the power supply is interrupted, while the gateway is in automatic mode, DHCP client mode will be activated. You will now be assigned an IP address by the DHCP server in the network.
- You can display the allocated IP address as follows.
  In the command line, enter `C:>` plus the following command:
  `nbtstat –R`
  `nbtstat –a ip400-YY-YY-YY`
  Where the `Y`s should be replaced with the gateway's MAC address.
- Now start the web-based configuration, using the new IP address.

Tip

The most convenient way of configuring the IP interface parameters is via DHCP, provided your network has a DHCP server.

You can ask your network administrator to reserve a fixed IP address for the gateway via DHCP. Tell your administrator the hardware address of your gateway. Please read the associated chapter about the serial number label for your gateway.

In the standard configuration, the gateway tries to configure via DHCP, each time it is switched on. The configuration mode without DHCP is activated however each time the reset button is pressed (not by switching on/off and not with the reset command) (refer here to section 2.2.4 "Setting the IP-interface parameters without DHCP" from page 16).

Now, proceed as follows:

- Set the **Ethernet switch** on the back to the "**connect to Hub**" position.
- Connect the **Ethernet RJ 45**-connector of the gateway to the RJ 45-connector of your Ethernet hub or switch using a **twisted pair** cable.
- Switch the gateway off and then on again, to activate the DHCP client.

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

- The simplest option is to ask your network administrator. They can find the assigned IP address using the DHCP server administration program.
- The other option is to consult the gateway itself. Once the configuration has been carried out successfully, the gateway registers the NetBIOS name "`ip400-XX-XX-XX`". "`XX-XX-XX`" must be replaced by the last 6 hexadecimal numerals from the serial number. Please read the associated chapter about the serial number label for your gateway.
  You can now find out which IP address has been assigned, using the command "`nbtstat`" on a Windows PC.

```
C:> nbtstat –

C:> nbtstat –a ip400-XX-XX-XX

NetBIOS remote machine name table

Name                 Type         Status
   ---------------------------------------------
   IP400-XX-XX-XX<00>  UNIQUE       Registered
   195-226-104-217<00>  UNIQUE       Registered
   IP400-XX-XX-XX<00>  UNIQUE       Registered
   MAC address = 00-90-33-XX-XX-XX
```

Tip

The IP address cannot be displayed with nbtstat, if your NetBIOS environment is configured exclusively to resolve names via WINS. Consult your network administrator to configure the NetBIOS name resolution appropriately, if the nbtstat command is unable to find your gateway.

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

Under Linux, you can use the "`nmblookup`" command for this purpose, provided the "SAMBA" package has been 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-XX-XX-XX<00>
[dvl@cobalt ~ 3] $.
```

Tip

The installation can be concluded, using your **Web Browser** or, using command lines with the help of **Telnet**. In this manual, we describe the procedure using the **Web Browser**, which is usually the most convenient one, for common application scenarios.

You can complete the definition of interface parameters using the web browser as follows:

- Start your web browser and go to the address `http://`***ipaddr.***
- Start the configuration applet via the **Config** menu in the **Gateway** menu (see section 3 "General information on configuration" from page 20). To do this, you need to log on to the device. In the standard configuration, the user name is `admin` and the password is `ip400`.
- You should change the user name and password immediately in the **General settings** area under **Change login parameters** to prevent unauthorised access (see section 8.1.2 "Defining the user administrator and -password" from page 110).
- Under **IP Interfaces / Ethernet Interface** under **DHCP**, set the **DHCP Mode** to **"Client"** (see section 4.1 "Configuration of the Ethernet interface" from page 24).
- Save the configuration permanently, using the **Save** and **Activate** buttons, (see section 3.2 "Checking and saving the configuration" from page 22).

2.2.4 Setting the IP-interface parameters without DHCP

You will have to set the IP interface parameters of the gateway yourself, if your network does not have a DHCP server.

... for experts

- If possible, configure your PC using DHCP!
- In the standard configuration, the gateway's DHCP server is only switched on 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 has been configured via DHCP, then update the IP address using `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.

Note

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

In addition, you have to deactivate the DHCP client built into the gateway and activate the built-in DHCP server. Both are done 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.

Caution

If the computer is connected to the network by a coaxial-cable (**thin Ethernet**) Remove the BNC-T-piece from the Ethernet adapter. Make sure that the network cable is not split in the process, as otherwise your network will no longer work.

If the computer is connected to the network by a **twisted pair** cable with RJ45-plugs, disconnect the cable from **Hub** or **Switch** or remove it from the wall socket, depending on where your computer is connected up.

- Set the **Ethernet Switch** on the back to "**connect to PC**". This makes the gateway operate like an **Ethernet Hub** for your computer.
- Connect the **Ethernet** RJ45-connector to the RJ45-connector of your Ethernet adapter using a **twisted pair** cable.

Your computer's Ethernet adapter will now be configured to enable it to communicate with the gateway, as it was delivered, factory default. The easiest way of doing this is for your computer's IP-details to be configured via DHCP.

You should really use DHCP, if your computer is able to deal with it. If this is not the case, the configuration can be performed manually.

- If your computer is configured to use the DHCP-protocol, the assignment of an IP address, suitable to communicate with the gateway, will now be initiated.-

Tip

Your PC must now be assigned an IP address suitable for the initial configuration of the gateway.

- Under Windows 95/98 this is done using the command
  `winipcfg`
  selecting the options "**Release all**" and "**Renew all**".
  Under Windows NT/2000/ME/XP execute the following commands:

  ```
  ipconfig /release /all
  ipconfig /renew /all
  ```

- Alternatively, you can also restart your computer.
- If your computer has been configured with fixed IP addresses, alter the settings in accordance with the following table:

Address	192.168.0.2
Network mask	255.255.255.0

Table 3 IP configuration for putting the device into service

With Windows, this is done by adjusting the settings for the TCP/IP- protocol accordingly in the **Network** area in **System control**. In this case, the computer must be restarted.

Tip

The installation can be concluded, using your **Web Browser**. In this manual, we describe the procedure using the **Web Browser**, which is usually the most convenient one, for common application scenarios.

You can complete the definition of interface parameters using the web browser as follows:

- Start your web browser and connect it to the address `http://192.168.0.1`.
- Start the configuration applet via the **Config** menu in the **Gateway** menu (see section 3 "General information on configuration" from page 20). To do this, you need to log on to the device. In the standard configuration, the user name is `admin` and the password is `ip400`.
- You should change the user name and password immediately in the **General settings** area under **Change login parameters** to prevent unauthorised access (see section 8.1.2 "Defining the user administrator and -password" from page 110).
- Under **IP Interfaces** / **Ethernet Interface** under DHCP set the **DHCP Mode** to "**off**" (see section 4.1 "Configuration of the Ethernet interface" from page 24).
- In the same place, set the parameters under **Ethernet Interface address.**
- In the same place, specify your **Default IP router**.
- Save the configuration permanently, using the **Save** and **Activate** buttons, (see section 3.2 "Checking and saving the configuration" from page 22).

The gateway is now ready to be connected to your local network.

- Set the **Ethernet Switch** on the back to "**connect to Hub**". The gateway now operates like a standard Ethernet terminal and can be connected to a **hub** or **switch**.
- Connect the gateway's **Ethernet** socket to your **Hub** or **Switch** or to the corresponding wall socket.

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

If you want to configure further gateways in the same way, you have to delete the assignment of the IP address to the hardware address first before connecting the next device to your PC.

Tip

This is necessary, as the new device has to respond to the same IP address, despite having a different hardware address.

With 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 requirements. This procedure is described in section 3 "General information on configuration" from page 20.

3 General information on configuration

Tip

Configuration is possible using a **Web Browser**. In this manual, we describe the procedure using the **Web Browser**, which is usually the most convenient one, for common application scenarios.

Please note, that your browser has to support HTML 4.0, HTTP 1.1 and Java applets. The configuration applet has been tested with Microsoft's Internet Explorer 6.x. Certain functions, such as sorting lists, require the XML and XML stylesheet functions. However, the devices can be fully operated, even without these functions.

Note

If access to the gateway is protected by a firewall, then the services `tcp/80` (http) need to be enabled. Please note, that this only enables configuration access. Please refer to section "NAT and firewalls" from page 143 if calls through the firewall are required.

To configure the equipment, go through the following steps:

- Configure the ISDN- or analogue interfaces.
  Here, you define the type of connection on the gateway's ISDN or analogue interface.
- Define other VoIP gateways and VoIP terminal equipment.
  Here, you tell the gateway which other innovaphone gateways, 3rd party VoIP gateways and VoIP terminal equipment or PC programmes you want to use.
- If necessary, configure the WAN interfaces.
  Here, you specify the parameters for your Internet or intranet access, if you also intend to use the gateway as an ISDN or a VPN router.

Tip

The innovaphone VoIP gateway IP 400 can also be used as ISDN router and as VPN router (PPPoE).

- Configure the call routing.
  Here you specify which terminal equipment is to be reached, under which number.

The configuration of the optional innovaphone PBX components is described in a separate manual, supplied together with your innovaphone PBX licence.

First, launch your **Web Browser** and enter the URL `http://`***address***`/`, where ***address*** is the IP address of the gateway to be configured. It is entered in the format *x.x.x.x*. If you have entered a host name for the gateway in the DNS name directory, you can of course also use this name, e.g. `http://h323gw.yourdomain.de`.

Now click on **Config** to start the configuration applet. You will be asked to enter the correct user ID and the password set when commissioning the gateway.

3.1 General information on the configuration user interface

The user interface, to configure the gateway, consists of two parts. The first part consists purely of HTML pages and is mainly used for calling up run-time information. These pages are used in the same way as any other web pages. The individual functions are described in more detail in section 9 "Administration via the Web Browser user interface" from page 119.

The actual configuration is performed using a separate configuration applet – a JAVA application. You start the applet by calling up **Config** from the administration user interface.

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

The applet consists of two areas. On the left-hand side, the entire configuration of the gateway is shown as a tree, in the same way as for a file browser. When you click on objects in this tree, detailed information is displayed on the right-hand side. The window on the left is used to navigate through the configuration. Entries can only be made in the right-hand window.

There is a button bar at the top of the applet window. The **Save**, **Activate**, **Reset**, **Reset when idle** and **Cancel** buttons relate to the entire configuration. Refer to section 3.2 "Checking and saving the configuration" from page 22 for the description of these functions.

The other buttons (**Add**, **Remove,** etc.) relate to the object currently selected in

the left-hand window.

Tip

You can choose names of your own for most of the configuration elements, by entering them in the **Description** field. These then appear in the tree display on the left-hand side. Make frequent use of this option, as it will help you maintain an overview later on.

Various configuration forms include 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".

3.2 Checking and saving the configuration

Your gateway saves the configuration permanently in non-volatile memory, so that it is still available after a system restart. When starting the system, the configuration is copied from the non-volatile memory into the working memory of the gateway. This copy is read during start-up and is then used during operation.

Changing the configuration firstly changes the configuration data in working memory. The new configuration only takes effect if it is re-read in the same way as during the system start-up.

In the configuration user interface, this is done by clicking on the **Activate** button. The new configuration is now effective and can be tested. However, the configuration has not yet been saved to non-volatile memory and will be lost if the gateway is cold started.

Tip

A cold start here means a restart following an interruption to the power supply, and not a restart caused by pressing the **Reset** button.

The new configuration has to be saved permanently, once you have checked it and are satisfied with it. This is done using the **Save** button.

Most of the changes to the configuration, changes to the routing information for example, are executed by the gateway without interrupting normal operation. Some changes, however, require a restart, interrupting calls in the process.

Your gateway informs you if a restart is required, to prevent calls from being acci-

dentally interrupted. If you decline the restart (**Later** button), you can enforce it later on, by clicking on the **Reset** or **Reset when idle** button.

Reset is used for an immediate restart, whereas **Reset when idle** only restarts if there are no active calls. This prevents existing calls from being disconnected by a restart.

The gateway might no longer be accessible, after activating the new configuration, if it was not performed properly. This would be the case, for example, if an Ethernet interface parameter such as an IP address or subnet mask is set incorrectly. In such a case, it would no longer be possible to fix the mistake using the configuration user interface.

If no access is made either from the configuration user interface or from **Telnet** within 60 seconds, the gateway will thus discard the activated configuration and restore the configuration held in the non-volatile memory. If **Save**, **Activate** or **Reset** is actuated, the configuration applet automatically reconnects to the gateway, with the effect that the new configuration is automatically saved, if successful.

Caution

Please bear in mind, that it's not possible to restore a useable configuration if a problem occurs after a **Save**. For remote maintenance in particular, under certain circumstances, access to the device may be no longer possible. We thus strongly recommended that you first check any changes to the configuration, using **Activate**.

You can cancel all changes made since the last **Save** by using the **Cancel** button. The current configuration will then be replaced by the last configuration saved in the non-volatile memory.

4 Configuration of the IP interfaces

4.1 Configuration of the Ethernet interface

The Ethernet IP interface is usually configured when the gateway is commissioned and does normally not need to be changed again. If this does need changing, you can adjust the settings in the **IP Interfaces > Ethernet Interface** configuration applet.

The gateway's DHCP function has a total of four operating modes:

Mode	Function	Use
Off	No DHCP function	When you want to configure fixed IP parameters.
Server	DHCP server[1] active	Connected devices are assigned an IP address by the gateway.
Client	DHCP client active	The gateway gets its IP configuration from a DHCP server in the network, section 4.1.1 "DHCP configuration options" from page 26 lists the DHCP options used.
Automatic	The DHCP client is active after switching on, after a reset of the DHCP server.	The gateway is thus as delivered in this condition (as also after a long reset)[2].

1.This setting only makes sense in exceptional cases, since the gateways do not incorporate complete DHCP servers. It is used primarily in tests or for demonstrations.
2.This setting only makes sense at the start. During commissioning, it must be replaced by the setting "off" or "Client".

Table 4

- To configure the Ethernet interface completely, it might be necessary to register the standard gateway of your network as the **Default IP Router**.
- If more routes have to be added on the other side of the standard gateway, this can be done via the **Add IP route** button.

  For network routes, enter the **Network address** with the host part as 0, and enter the correct **Network mask**.

  For host routes enter the complete IP address of the host and enter `255.255.255.255` in the **Network mask**.

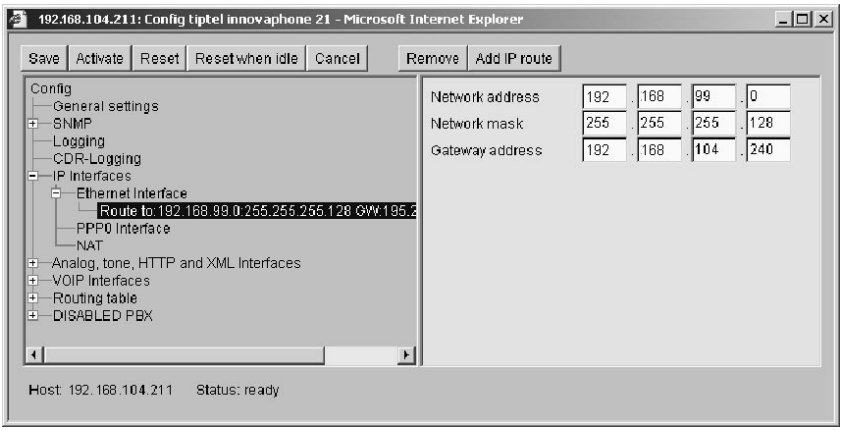

Fig. 4 Adding routes to the Ethernet interface

- If your gateway is not to also serve as a WAN router, leave the **DNS server address** field empty and deactivate the **Do proxy-ARP** checkbox.
- The **Full duplex** checkbox is usually not activated.

Tip

This option is only necessary with the IP 400. The IP 3000, IP 3000DD, IP 800, IP 202 and the IP 21 negotiate the full duplex mode automatically with the switch or hub.

- Check the 802.1p box, if the equipment's Ethernet packets need to be prioritised in the switch.

4.1.1 DHCP configuration options

Besides the IP address actually assigned, your gateway's DHCP client processes the DHCP options specified in Table 5, provided that they were supplied when the DHCP lease was granted.

Options supplied via DHCP always overwrite any parameters defined in the gateway configuration.

DHCP #	DHCP name	Overwritten configuration parameters	Description
001	Subnet mask	**IP address mask**	The registered network mask is used.
002	Time offset	**Offset to UTC**	Time difference to Universal Time, in seconds.
003	Routers	**Default Gateway**	The first entry in the list of registered routers will be used as the standard IP-gateway.
006	Domain name servers	**DNS server address**	The first two entries from the list of registered DNS servers are used as DNS servers.
042	NTP servers	**SNTP server IP address**	The first entry, from the list of registered NTP servers, is used as the NTP server.

Table 5 DHCP configuration options

4.1.2 Full duplex Ethernet

The IP 400 Ethernet controller can be set to full-duplex operating mode. Normally the IP 400 is operated in half-duplex mode.

For full-duplex operation:

- Go to **IP Interfaces > Ethernet Interface** in the configuration applet.
- Check **Full duplex** on the **Ethernet Interface** form.
- Set your Ethernet switch to always run in full duplex mode, for the port to which the IP 400 is connected. This is necessary, as the operating mode of the IP 400 is not negotiated. Faults will occur if the IP 400 settings do not correspond to those of the Ethernet switch.

4.1.3 Priority on Ethernet

The Ethernet packets sent by the equipment can be prioritised, at level 2, in the switch. To do this, the packets must be marked accordingly, during transmission. This function must be supported by the switch used.

- Select **IP Interfaces > Ethernet Interface** in the configuration applet.
- Tick **Use 802.1p for Quality of Service** to mark the packets sent with VLAN ID 0 and priority 7.
- The VLAN ID with the value 0 switches QoS off, following 802.1Q. The value 0 is assumed if the **802.1 Q VLAN ID** field is empty. If your switch port, connected to the innovaphone gateway, is configured to a different VLAN ID, you have to use the same value here, to enable the prioritisation of the Ethernet packets.

Caution

Note the configuration of the switch, before setting the **VLAN ID**.

innovaphone equipment can access the VLAN ID and the VLAN priority using DHCP. See Appendix D: "The innovaphone DHCP Client" from page 152 for more information on the DHCP client, the VLAN ID and the VLAN priority.

4.2 Configuration of the WAN interfaces

Your gateway can also be used as an ISDN or PPPoE (PPP over Ethernet) router. In this case it deals with the transmission of TCP/IP data between your local network and the WAN connection, regardless of whether this concerns voice or other data.

The equipment provide various options for routing in the WAN. To use ISDN as a WAN interface is a standard feature of the IP 400. The IP 400 supports PPPoE on the WAN interface.

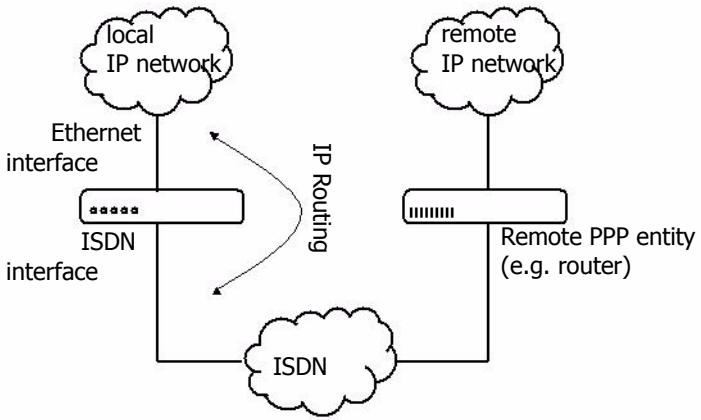

Fig. 5 Using the gateway as an ISDN router

Any ISDN or PPPoE router with PPP capability can serve as a PPP remote entity. Fig. 5 on page 28 illustrates accessing a remote IP network using an IP 400 as an ISDN router. Fig. 6 on page 29 illustrates accessing the Internet via a DSL connection.

The IP 400 has 4 configurable PPP interfaces available.

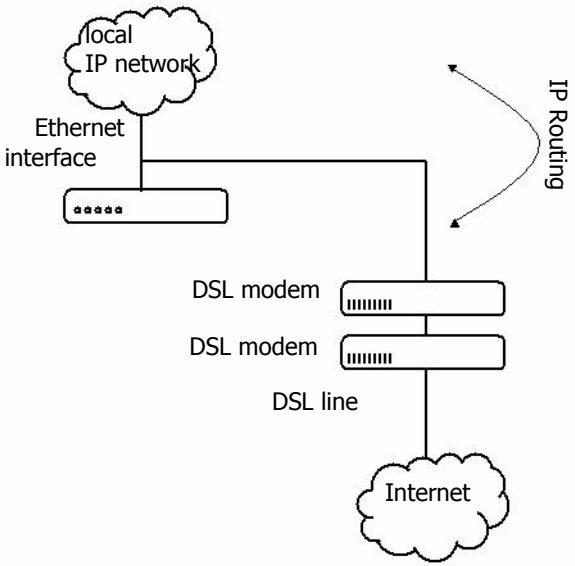

Fig. 6 Connection to a DSL line using PPPoE

The connection can also be established directly between two gateways, for example as part of a PBX link-up between two locations via a permanent ISDN connection (leased line). Fig. 7 on page 29 shows such a configuration.

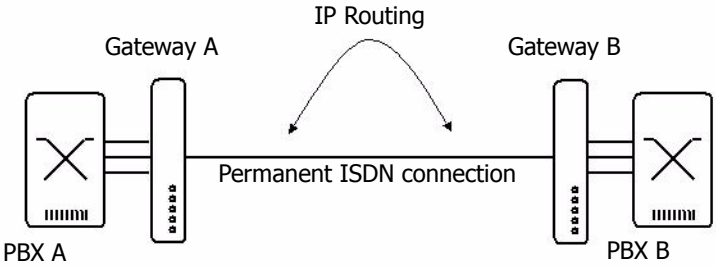

Fig. 7 Linking gateways with a permanent ISDN connection

One specific application of the ISDN WAN interface is to dial-in to the gateway for maintenance purposes. This enables remote maintenance of the gateway, without necessarily having access to the local IP network, as illustrated by Fig. 8 on page 30.

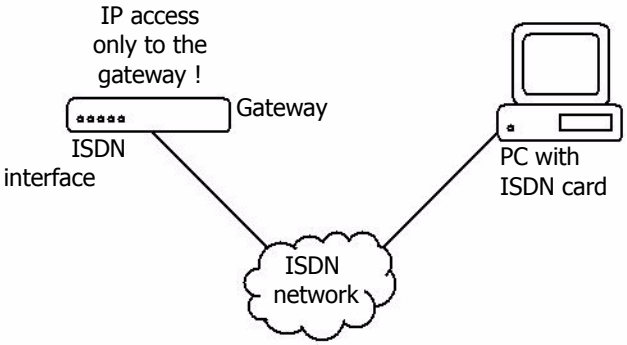

Fig. 8 Remote maintenance access via ISDN

4.2.1 General considerations on the configuration of the PPP connections

Opening a connection

The gateways do not usually establish any connections automatically, when using dial-up lines. In these cases a PPoE connection is treated as a dial-up line. PPP connections are thus only established, if an incoming data call is received for a configured PPP interface, or if the connection is established explicitly via the **IP Interfaces** area of the administration user interface. As a result, full control is maintained over cost-generating data connections and, in particular, events in the local network cannot cause any unwanted connection set-ups (no **dial on demand**).

Caution

In some cases though, it may be wanted to keep a dial-up line permanently open. This is achieved by means of the "Automatic dial after boot" setting. It results in the corresponding PPP connection being established and kept permanently open, immediately after starting the gateway. Use this setting with appropriate caution.

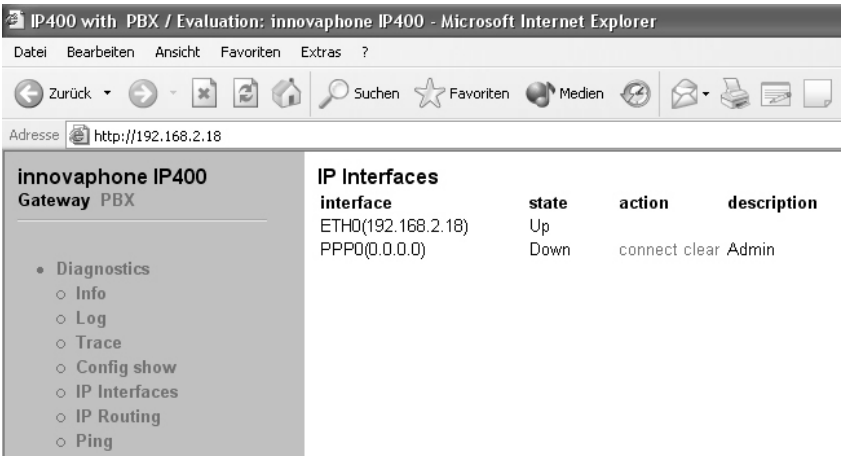

Fig. 9 Connection control on the administration user interface

The **connect** link is used to establish the selected connection. The **clear** link, by contrast, is used to clear the connection.

Channel bundling (multi link)

The gateways support channel bundling on two ISDN B channels (128 kbit/s).

WAN interface addresses

The WAN interfaces of a router are usually assigned their own IP addresses (usually from a special transfer network). This is not necessary with the gateways. You thus do not require any particular IP addresses, apart from those for your own IP network.

Compression of voice data on the PPP link

The gateways support the compression of voice data along the PPP link using the **RTP Header Compression** method (to RFC 2508 / 2509). This drastically reduces the required bandwidth for VoIP calls.

Compatibility problems may arise in practice, if the distant PPP entity used is not an innovaphone gateway. Try the option **Adjust for Cisco's PPP implementation** if a Cisco router is used at the remote location and problems arise in the transmission of voice data.

Configuration of the IP routes

You can add separate IP routes for each PPP interface using the **Add IP route** button. The routes are configured in the same way as those for the Ethernet interface (see section 4.1 "Configuration of the Ethernet interface" from page 24). All IP routes must be defined explicitly. No data is routed via PPP interfaces, for which no IP routes have been defined.

Please note however, that the configured IP routes are static routes, which are always active. This is true, even if the corresponding PPP interface is not connected. Overlapping IP routes on different PPP interfaces (several **Default Routes** for example) are thus not possible.

4.2.2 Settings for outgoing ISDN PPP dial-up connections

The following steps are used to configure your gateway for an outgoing PPP data connection:

- In the configuration applet, select **IP Interfaces > PPPn Interface**, where n corresponds to each PPP interface to be configured.
- Uncheck the **Automatic dial after boot** box.
- Uncheck the **Multilink** box.
- Uncheck the **Permanent connection** box.
- Select the ISDN interface(s) that you want to use for the outgoing call from the **Port** field.
- The **Channel** field is significant for permanent connections only and thus can't be changed here.
- In the **Subscriber number** field, enter the calling MSN (multiple subscriber number) to be used for the call. It can usually remain empty.
- Uncheck the **Allow incoming calls** box.
- Uncheck the **Assign remote IP address** BOX.

Tip

As a result, the called party will not be assigned an IP address whilst the PPP connection is being established. This is unusual for outgoing calls.

- Leave the **Check remote number** field empty.
- Enter the appropriate data in the **User** and **Password** fields in the **Incoming calls** area, if the called distant PPP entity is to provide authentica-

tion at your gateway.

- Enter the call number of the remote PPP entity to be called in the **Dial remote number** field.
- Enter the appropriate data in the **User** and **Password** fields in the **Outgoing calls** area, if your gateway is to provide authentication at the called distant PPP terminal.
- Configure the IP routes as described in section "Configuration of the IP routes" from page 32.

Extension to multilink

You can also configure a **multilink** connection via two bundled channels instead of a connection via one B channel.

- In the configuration applet, select **IP Interfaces > PPPn Interface**, where **n** corresponds to each PPP interface to be configured.
- Tick **Multilink (128K ISDN) in the ports group for PPP.**
- If a different call number has to be used for the second channel to the remote PPP entity to be called, enter it in the **Dial remote number** field in the **Numbers for 2nd Multilink channel** area. Leave this field empty 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. It can usually remain empty.

4.2.3 Settings for incoming ISDN PPP dial-up connections

Use the following steps to configure your gateway for an incoming PPP data connection:

- In the configuration applet, select the **IP Interfaces > PPPn Interface** path of the PPP interface to be configured.
- Uncheck the **Automatic dial after boot** box.
- Uncheck the **Multilink** box.
- Uncheck the **Permanent connection** box.
- Select the ISDN interface(s) in the **Port** field, that you want to use to accept incoming calls.
- The **Channel** field is significant for permanent connections only and thus can't be changed here.
- Enter the number to accept incoming calls in the **Subscriber number** field. It should not remain empty.

Tip

If this field remains empty, all data calls will be accepted at the selected ISDN interfaces. In this case however, it is not possible to assign these calls to the various PPP interfaces. Such configurations should thus be avoided.

- Check the **Allow incoming calls** box.
- Uncheck **Assign remote IP address**, if the calling distant PPP entity has a permanent IP address. As a result, the called party will not be assigned an IP address whilst the PPP connection is being established. This is unusual for outgoing calls. Tick **Assign remote IP address** if the device in question at the calling PPP remote entity requires a dynamically assigned IP address. This is the case, for example, with a Windows PC that dials up a gateway via the remote data transmission network. In this case enter the IP address that is to be assigned in the **IP address** field and add an IP route to the PPP interface with precisely this IP address (see section "Configuration of the IP routes" from page 32).
- If the dial-in is to be restricted to a single PPP remote terminal, enter its number in the **Check remote number** field. The last part of the calling party's number is compared to the contents of this field and must match it, otherwise the call will be rejected. If, for example, the number `7031730090` is entered there, calls are accepted from both `07031730090` as well as `004907031730090`.
- Enter the appropriate data in the **User** and **Password** fields in the **Incoming calls** area if the calling remote PPP entity is to provide authentication to your gateway.
- Leave the **Dial remote number** field empty.
- Enter the appropriate data in the **User** and **Password** fields in the **Outgoing calls** area, if your gateway is to provide authentication to the calling remote PPP entity.
- Configure the IP routes as described in section "Configuration of the IP routes" from page 32.

Expansion to Multilink

You can accept a **multilink** connection via two bundled channels instead of a connection via a single B channel.

- Check the **Multilink** box.
- Leave the **Dial remote number** and **Local subscriber number** fields empty in the **Numbers for 2nd Multilink channel** area. Your gateway will accept calls for both channels on the same number, configured in the **Subscriber number** field.

4.2.4 Settings for incoming and outgoing ISDN PPP dial-up connections

You can also configure a PPP interface for incoming and outgoing calls. To do this, combine the previously described settings for incoming and outgoing calls.

4.2.5 Special features of WAN connections via Ethernet (PPPoE)

Using PPPoE over WAN connections, for example with a DSL modem, is very straightforward. Note however, that only outgoing calls are possible in this operating mode.

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

PPPoE connections are basically dial-up connections, just like ISDN connections. However, a number of providers offer **Flat Rates** with charges which are independent of the call duration. In such cases, it is possible and also makes sense to keep the PPPoE connection open permanently.

Network address translation (NAT) is not required if the connection is operated with unofficial, but known, IP addresses. To deactivate NAT, set the option **Exclude from NAT**. NAT only needs to be active on networks requiring official IP addresses.

- Check the **Automatic dial after boot** box, if you want to keep the PPPoE connection permanently open. Otherwise, or if you are uncertain about the incidental costs, remove this check.
- Uncheck the **Multilink** box.
- Uncheck the **Permanent connection** box.
- Select the **PPPOE** setting from the **Port** field.
- The **Channel** field is only significant for permanent ISDN connections and

thus can't be changed here.

- Leave the **Subscriber number** field empty, since it has no significance.
- Only outgoing PPPoE connections are possible, so uncheck the **Allow incoming calls** box.
- Uncheck the **Assign remote IP address** box.

Tip

As a result, the called party is not assigned an IP address while the PPP connection is being established. This is unusual for outgoing calls.

- Leave the **Check remote number** field blank, since it has no significance.
- Leave the **User** and **Password** fields empty in the **Incoming calls** area, since they are of no significance.
- Leave the **Check remote number** field empty, since it has no significance.
- Enter the appropriate data in the **User** and **Password** fields in the **Outgoing calls** area, if your gateway is to provide authentication at the called distant PPP terminal.
- Configure the IP routes as described in section "Configuration of the IP routes" from page 32.

4.2.6 Settings for VPN connections with PPTP

The point-to-point tunnelling protocol (PPTP) implements virtual, private network (VPN) connections via the Internet or other networks using the Internet protocol.

The PPTP connections are always dial-up connections. An IP address is dialled. Authentication is performed by means of the user name and password. In addition, the transmitted voice data can be encrypted using Microsoft Point-to-Point Encryption (MPPE). This is based on the requirement that the distant entity also supports this process.

Since encoding and decoding always takes time, there may be some delay in voice transmission, affecting the quality of the transmission. If quality loss is apparent, you will have to decide for yourself between security or voice quality.

The innovaphone VoIP gateways can dial up to a remote server as PPTP client as well as providing a dial-up access point themselves. PPTP is ideal to link up two innovaphone VoIP gateways via the Internet.

Network address translation (NAT) is not required if both parties operate a net-

work with unofficial IP addresses which are known to both parties. To deactivate NAT, set the option **Exclude from NAT**. NAT is only required if a tunnel is set up to a network requiring official IP addresses.

Dial-up of the VoIP gateway (client) to a PPTP server

- In the configuration applet, select the **IP Interfaces > PPPn Interface** path of the PPP interface to be configured.
- Select the **PPTP** protocol from the **Port** menu.
- Enter the IP address of the remote PPTP server, with which you wish to set up the VPN, under **PPTP-IP address**.
- Switch off the option **Allow incoming calls**.
- Set **Enable Encryption**, **Exclude from NAT** and **No DNS on this port** as required.
- Enter the **user** and the **password** with which you would like to log on to the remote PPTP server in the **Outgoing calls** group.

Setting up a PPTP server

- In the configuration applet, select the **IP Interfaces > PPPn Interface** path of the PPP interface to be configured.
- Select the **PPTP** protocol from the **Port** menu.
- Do not enter an IP address under **PPTP-IP address**.
- Switch on the option **Allow incoming calls**.
- Set **Enable Encryption**, **Exclude from NAT** and **No DNS on this port** as required.
- Set the **Assign remote IP address** option to assign an IP address from your network to the distant entity dialling-in. Enter this IP address in the **IP address** field.
- In the **Incoming calls** group, enter the **user** and the **password** with which the remote PPTP client is to register.

4.2.7 The remote maintenance facility in the standard configuration

In the standard configuration, the **PPP** ISDN interface is configured to dial-up up for remote maintenance. This allows the gateway to be configured remotely from any PC with an ISDN card and a PPP remote data transmission programme (e.g. Windows DUN).

Tip

The standard setting for this is disabled. To activate the preconfigured remote maintenance facility, uncheck the "Disable" option in the configuration applet under **IP Interfaces > PPP0 Interface > Interface name and general config**.

The settings for this are configured in the logical interface PPP0, which you can view and modify as desired under **IP Interfaces > PPP0 Interface**.

- Calls are answered on the **PPP** interface (**ISDN port** is **PPP**, **Allow incoming calls** checkbox is ticked).
- Calls are accepted to every MSN (**Subscriber number** is empty).
- The calling party is assigned an IP address (`192.168.0.253`) (the **Assign remote IP address** checkbox is ticked).
- Calls are accepted from all remote entities (**Check remote Number** is blank).
- As **User** `admin` is used and as **Password** `ip400`.
- Reverse authentification does not take place (the fields under **Outgoing calls** are blank).
- The called gateway itself is assigned the IP address `192.168.0.254`.

Tip

Under normal circumstances this IP address should not overlap with the address of a device on the LAN. If however, there is a device on the network with the IP address `192.168.0.254`, the gateway itself will not be able to communicate with this device. This address is programmed permanently into the gateway. This ensures that a gateway can always be addressed, under this IP address, via the remote maintenance facility, regardless of which IP address is set on the Ethernet interface of the gateway.

This configuration means that by plugging in an ISDN BRI point-to-multipoint exchange connection (e.g. a BRI connection to the exchange or a BRI line from a PBX) to the **PPP** interface, the gateway can be configured from any PC with a PPP dial up application.

Of course, this configuration can be adapted to the local circumstances. Refer here to the instructions in section 4.2.3 "Settings for incoming ISDN PPP dial-up connections" from page 33.

4.2.8 Allowing dial-up access to the entire network

For IP packets which have to be routed from Ethernet to logical PPP interfaces via the gateway, to the local network, the gateway appears as if it were itself the addressed terminal equipment. This allows IP terminal equipment on the same Ethernet segment, which does not have a correct routing entry, to also communicate beyond the gateway and make use of the WAN connection. This function referred to as **proxy arp** is activated by ticking the **Do proxy-ARP** checkbox in the **Ethernet Interface** area of the configuration applet.

For this purpose, the remote entity, connected via ISDN, has to be assigned an IP address from the same subnet as the gateway. This is done by making an appropriate entry in the **Remote IP address** area and ticking the **Assign remote IP address** checkbox.

Note however, that this makes your entire network accessible to the dialling-up party, which could be a security problem, under certain circumstances.

4.2.9 The ENUM protocol

ENUM stands for a protocol, which has to do with mapping so-called E.164 numbers to Uniform Resource Identifiers (URI). It defines rules to uniquely map a telephone number to a domain. This domain can then be used, for example, to identify addresses for IP telephony.

ENUM uses the Domain Name System (DNS) to do that. One of DNS's jobs is to create a logical connection between the addresses of computers attached to the Internet (which are identified by pure numeric IP addresses) and domains, which have the advantage of being easier to remember. Most Internet users probably only know of domains in connection with E-mail addresses or web-sites. The DNS infrastructure and the ENUM protocol enable telecommunications services to be requested and addressed via domains. In contrast to web domains, users of ENUM domains don't have a free choice, as there are fixed rules about mapping a telephone number to a corresponding ENUM domain. The corresponding ENUM domain can thus only be registered by the owner of the associated telephone number. The ENUM protocol has to be supported by the Internet Service Provider (ISP).

By linking telephone numbers and Internet resources, brand new services result. A basic service is to find an Internet terminal capable of telephony, from a traditional telephone. ENUM can optionally, also supply details of additional communications options. If no Internet terminal is reachable, which is capable of telephony, another means of communication can be selected from the list of alternative applications.

An example should illustrate the principle: After entering a telephone number, for which ENUM information is available, the call is first switched to a conventional network connection. If no-one answers, the call is forwarded to the registered mobile telephone number. If no connection can be made here, the message can be recorded and sent to an E-mail address as an audio file. It is also conceivable that a web site could be addressed, which could then supply information about any other communications options.

This example makes the advantage of the new system clear: Instead of a multitude of telephone numbers for the various applications, one number will do. The entries in the ENUM name server deal with the allocation to the matching output devices. An incoming fax is thus automatically directed to the correct piece of terminal equipment.

The use of ENUM in modern communications scenarios offers a lot of options, with a correspondingly large potential for use, in very different areas. For example, when routing: here PSTN networks and VoIP networks can be linked.

4.2.10 To set up the ENUM protocol on an innovaphone gateway

To be able to use the ENUM protocol, 3 VoIP interfaces have to be set up. To transmit the ENUM calls via the innovaphone PBX, to receive incoming ENUM calls and to forward these incoming calls to the innovaphone PBX.

To set up the ENUM protocol on your innovaphone gateway, proceed as follows:

- Start your gateway's configuration applet (see section 3.1 "General information on the configuration user interface" from page 21).
- In the configuration applet, select the path **Config > VoIP Interfaces > GWn**, where n corresponds to the VoIP interface to be configured, e. g. **GW1**.
- In the area **VoIP Interface name and general config** in the field **Description** enter a brief description, e. g. `ENUM`.
- In the **Mode** area, enter the correct mode **Enum Gateway**.
- In the **Enum** area, you can make an entry in the **Suffix** field. Generally, no entry is necessary. If the field is empty, the internal preset `e164.arpa` will be used.

With that, the configuration of the ENUM interface for outgoing calls is finished. Configuring the router will be explained later. In the next step we will configure an innovaphone PBX interface, if this hasn't already been done. In the following example, we presume that **GW2** is our gateway to the public exchange for the PBX and is registered with the alias `Exc` or `PBX` and the number `0` in the PBX `127.0.0.1`:

- In the configuration applet, select the path **Config > VoIP Interfaces > GWn**, where n corresponds to the VoIP interface to be configured, e. g. **GW2**.
- In the area **VoIP Interface name and general config** in the field **Description** enter a brief description, e. g. `PBX`.
- In the **Mode** area, enter the correct mode **Registration at gatekeeper as gateway**.
- In the area **Remote gatekeeper address** in the field **IP address**, enter the IP address `172.0.0.1`. If a **Gatekeeper ID** and a **Password** are necessary, please complete these details.
- Create a suitable **alias** entry. This is done by clicking on the **Add alias** button. For further information on the **alias** entry see section 6.2 "Management of VoIP devices via RAS (Gatekeeper)" from page 81.

With that, the PBX interface configuration is complete. For more information on the PBX interface, look in the "innovaphone PBX Administrators Manual".

In the next step we will configure an interface for incoming calls, if this hasn't already been done. The interface must permit the acceptance of calls from any IP address, without previous registration:

- In the configuration applet, select the path **Config > VoIP Interfaces > GWn**, where n corresponds to the VoIP interface to be configured, e. g. **GW3**.
- In the area **VoIP Interface name and general config** in the field **Description** enter a brief description, e. g. `World`.
- In the **Mode** area, enter the correct mode **Gateway (w.o. registration)**.
- In the area **Remote gateway address** in the field **IP address**, enter the IP address `0.0.0.0`.

With the entries **Gateway (w.o. registration)** and IP-Adresse `0.0.0.0` incoming calls from persons unknown will be accepted. See also section 6.3 "Static management of VoIP devices" from page 84.

With that, the configuration of the interface for incoming calls is finished.

To establish a call via an ENUM enquiry, at least one route must lead to the newly created ENUM interface. For information on the routes, see section 7.1 "General considerations on the configuration of call routing" from page 87. To create a route in the ENUM interface, proceed as follows:

- In the configuration applet, choose the path **Config > Routing table**.
- Click on the **Add route** button to add a further entry to the routing table. Note the order of the routes here. The new route is always inserted after the current entry.
- In the **Description** enter a name for the route, e. g. `to ENUM`.
- Select the entry underneath the new route `to ENUM` (the one with the "**->**").
- Tick the checkboxes of the gateways and ISDN-interfaces in the **Enable calls from interfaces** area to validate them as sources for this route. You will only be offered the interfaces, which have been configured. In our previous example, that was **GW2**.
- From the **Default call destination** list, select the destination to which the calls are to be connected - i.e. the new ENUM interface. In our previous example, that was **GW1**.

Now, the route to the ENUM interface has been created. As ENUM requests have to be transmitted with complete E.164 numbers, it is necessary to prepare the number to be dialled accordingly, to be able to create the corresponding ENUM domain.

So, in the next step we will configure the map to the **Tone Interface**, so that when you dial a `0`, you can hear a dial-tone.

- Click on the button **Add map**, whilst the cursor is in the previously configured route `to ENUM`.
- In the **Called number in** field, enter the telephone number `0`.
- In the **Destination:** field, select the entry **Tone**.

This entry guarantees, that when you dial `0` you will hear a dial tone.

In the next step, the telephone number mapping is defined for international, national and local calls. To do this, three additional maps are required, to make sure that every user number that is sent to the ENUM interface is in the standardised, international format (without any prefixes).

Tip

Please note, that the order of the configured maps is extremely important. The longest entries must be listed first, as the entries are processed in sequence.

- Click on the **Add map** button.
- In the **Called number in** field, enter the digits `000`.

With this entry, `000` is recognised as the international prefix and is removed.

- Click on the **Add map** button.
- In the **Called number in** field, enter the digits `00`.
- In the **Called number out** field, enter the country prefix. For Germany, for example, enter `49`.

With this entry, `00` is recognised as the national prefix and will be transformed into the international format.

- Click on the **Add map** button.
- In the **Called number in** field, enter the digit `0`.
- In the **Called number out** field, enter the country prefix, followed by the area code (without the leading `0`). Taking the city of Berlin as an example (area code `030`) in Germany (country prefix `49`) the entry will be `4930`.

With this entry, `0` is recognised as the area code and will be transformed into the international format.

These three maps, just configured, mean that any dialled telephone number can

be transformed into the international syntax, which is necessary for the ENUM protocol. If someone calls reception at innovaphone® AG by dialling the telephone number +49 7031 73009-0, the associated number, sent to the ENUM interface will be 497031730090. It is irrelevant, where in the world this number was dialled.

- For the three routes just set up, for international, national and local prefixes, activate the **Final map** option, so that, if there's any rerouting, the next map for the subsequent route can be used.

To transform outgoing telephone numbers into a fully compatible E.164 number, it is sensible to the extend the three routes just created for international, national and local prefixes, with a **CGPN map** (CGPN CallinG Party Number). This means that a subscriber you have called via ENUM, can, if required, call you back. Proceed here as follows:

- Click on the **Add CGPN map** button after you have activated the option **Final map** and add a **CGPN map** entry.
- In the **Calling number out** field, enter the sequence of digits which will replace the outgoing telephone number. This means the country prefix followed by the area code (without the leading `0`) and the telephone number. Taking the city of Berlin as an example (area code `030`) in Germany (country prefix `49`) with the telephone number `1234567` the entry will be `49301234567`.

4.2.11 Rerouting outgoing calls

Rerouting is supported. If the call to an ENUM interface should fail to be established, rerouting means looking for another, subsequent route and trying again.

Tip

If rerouting is to work correctly, the **Final map** option must have been activated for the three routes just set - international, national and local prefix.

If you combine the ENUM functions with rerouting, you have set up a simple form of "least cost routing". At the first attempt, we try to establish a cost effective connection by using the ENUM interface. Should this fail, the call will be established conventionally, using an ISDN line.

5 Configuration of the ISDN interfaces

The IP 400 has two "virtual" interfaces, whose configuration is described in section 5.3 "Considerations on the configuration of the virtual interfaces" from page 66.

The IP 400 has ISDN interfaces.

To configure the ISDN interfaces you first need to decide about the following points:

- Which devices you want to connect to the gateway. That could be telephones, PBXs, network terminations from your ISDN network provider, or other ISDN terminal equipment.
- Whether the ISDN connections are to be used exclusively for voice connections or whether one of them is also to be used for an ISDN/PPP connection for data routing.

This is configured in the "ISDN Interfaces" area of the configuration applet.

... for experts

S_0

- **tel1** and **tel2** can be operated in TE and NT mode with or without power supply and termination.
- **PPP** and **S/T** can only be used in TE mode.
- **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 (also mixed).
- **NT** (**Line Emulation**) switches on the NT mode for layers 1, 2 and 3.
- **Power** switches on the power supply for terminal equipment on the bus (in NT mode only, maximum 4 W).
- 100 Ohm **Termination** switches on the bus termination.
- **Permanent activation** (in TE mode only) activates the line permanently (clock).
- **Point to Point** switches on the point to point mode.

BRI

- **Disable overlap receive** suppresses a SETUP_ACK on incoming single digit dialling on a point to multipoint connection, in TE mode.
- **Suppress sending of HLC** suppresses the transmission of **high layer compatibility** information elements on the interface.
- **Suppress sending of FTY** suppresses the transmission of **facility information elements** on the interface.
- **Provide inband progress tones** (in TE mode only) enforces the generation of tones (dial tone, ring tone, busy tone) also in TE mode (always generated in NT mode).
- **Generate connected time** adds the local gateway time to every outgoing CONNECT message.
- The **D-Channel Protocol** meanings: **EDSS1** = Euro ISDN, **QSIG** = ECMA QSIG (**CR len**=1, **channel ID** like basic rate), **QSIG-PRI-ECMA1** = ECMA QSIG (**CR len**=2, **channel ID** as primary rate, B channels 1 to 30), **QSIG-PRI-ECMA2** = ECMA QSIG (**CR len**=2, **channel ID** as primary rate, B channels 1 to 15 and 17 to 31).
- The **Dialtone types** (in NT mode or with **Provide inband progress tones**) meanings: **German PBX** = like German PBX system, **German** = like German exchange, **US** = American dial tone, **UK** = British dial tone.
- Calling Line Identifiers (CLI) can be replaced via **ADD CGPN MAP**. These replacements only apply to this interface (separately for incoming/outgoing calls).
- Called numbers can be replaced via **ADD CDPN MAP**. These replacements only apply to this interface (separately for incoming/outgoing calls).

5.1 IP 400 ISDN interfaces

The IP 400 has three ISDN BRI interfaces, which are referred to as **PPP**, **tel1** and **tel2** (see page 7).

- **tel1** and **tel2** can be used for public exchange lines, for one or two telephones, or for a PBX.

Tip

Technically, up to eight terminals can be connected to an ISDN interface. Note however, that from all these devices, only two calls can be made simultaneously. Furthermore, it must be ensured that the total power consumption of all terminals does not exceed the permitted value of 4 Watts.

- **PPP** may only be used to connect to a public exchange.

All three interfaces can be used to set up ISDN data connections (PPP), for both permanent connections as well as dial-up lines.

The **Remove** button can be used to delete all settings for the selected interface.

5.2 Considerations on the configuration of the ISDN interfaces

The TE and NT modes

The **tel1** and **tel2** interfaces can either be operated in TE or NT mode. **PPP** operates in a fixed mode.

TE (**terminal equipment**) mode means here that the interface is operating like a normal piece of ISDN terminal equipment. This means that

- layers 2 and 3 of the ISDN protocol are configured as terminal equipment,
- the connection lines are used accordingly, and
- the gateway synchronises itself to the network clock (**clock slave**).

In NT (**network termination**) mode on the other hand, the interface operates like an ISDN network termination (**NTBA** Network Termination Basic Access). This means that

- layers 2 and 3 of the ISDN protocol are configured as a network
- the connection lines are crossed accordingly, and
- The gateway provides the clock (**clock master**).

Volume adjustment

In some cases, it is desirable to adjust the basic volume level of an interface. The volume of the ISDN interfaces can be set, in the configuration applet, under **Config > ISDN, tone and HTTP Interfaces > TEL** or **PRI** under **Interface configuration** in the **Volume** field, in the range from `-31` to `+32`. The units of the volumes setting are Decibels. No entry, or the value `0` corresponds to the factory setting. A -ve entry reduces the volume and a +ve entry increases the volume of the associated interface.

The signalling protocols

Basically, the gateways support two different D channel protocols on the ISDN interfaces: Euro ISDN (EDSS1) and QSIG.

Euro-ISDN is the type of signalling that has gained worldwide acceptance for ISDN subscriber interfaces and, despite the name, is also common outside Europe. The chief exception 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 to connect PBXs. Here, **basic call** and **tunnelling** are supported by the gateways. This allows, in particular, homogenous PBX systems to be linked with QSIG, in which manufacturer-specific properties are exchanged via QSIG.

Unfortunately, there are several variants of the QSIG standard and various implementations; some conform more and some less to the standard. The gateways therefore support 3 different variants which vary with regard to

- the length of the **call reference**,
- the coding of the **channel id** and
- the numbering of the B channels

The following table specifies the differences.

Variant	**Call reference** length	**Channel ID** coding	Numbering of the B channels	Use
QSIG	1 byte	As with basic rate		S0
QSIG-PRI-ECMA1	2 bytes	As for **primary rate**	1 to 30	S0

Table 6 Differences between the QSIG variants

Single digit dialling on terminals on point-to-multipoint connections

Normally, single digit dialling (**overlapped sending**) is not used to call terminals (i.e. devices in TE mode) on point-to-multipoint connections. Under certain circumstances however, it is possible for gateways to be connected to a PBX system in precisely this mode and then also support incoming single digit dialling (**overlapped receive**). In this case, an incoming **SETUP** message is answered, as required in the standard, with a **SETUP_ACK** message. Some PBXs however do not expect this sort of message from terminal equipment and terminate the call at this point. In such a case, the **Disable overlap receive** setting prevents the gateway from answer the incoming **SETUP** message with **SETUP_ACK**.

Suppression of specific protocol elements

Not all ISDN implementations are prepared to receive certain **information elements** (so called **IE**s), which conform to the standards. Such IEs can be created, for example, when linking up different PBXs or transmitting H.323 calls to an ISDN interface and vice-versa.

If malfunctions are caused by the transmission of certain IEs, the gateways can be made to remove such IEs from the transmitted messages.

Setting	Effect
Suppress sending of HLC	No **high layer compatibility information elements** are transmitted.
Suppress sending of FTY	No **facility information elements** are transmitted.

Table 7 Suppression of the transmission of **information elements**

Dial tones

The gateways are able to generate call progress tones at the ISDN interfaces (dial tone, ring tone, busy tone).

This is done for outgoing calls from the gateway in the direction of the calling party, whenever the called party does not generate any dial tones of its own.

Tip

Dial tones can be identified by the **inband information**, which is signalled by the called party.

For incoming calls at the ISDN interface, this is usually only done in the direction of the calling party if the interface is in NT mode, not however if it is in TE mode. In a few cases though, in particular when linking up PBXs via tie lines, it can be useful to also generate these tones in TE mode. This can be done using the **Provide inband call progress tones** setting.

Generation of time stamps during the connection set-up

The ISDN network usually generates a time stamp in the **connect** message. This is used by telephones or PBXs, for example, to set their own clock at the first connection. The gateways usually pass on such time stamps, unchanged.

However, it may be desired to have the current system time of the gateway consistently used as the time stamp in all **connect** messages. This can be done using the **Generate connected time** setting. Here, the gateway should always have the correct time. Since it does not have its own real-time clock, an NTP time server should be configured for this purpose (see page 110). This setting usually only makes sense in NT mode.

5.2.1 Usage at a public exchange line (dial-up or permanent connection)

In this case, the gateway is connected to one of the ISDN-exchange lines from your network provider. This type of usage is only possible for **tel1**, **tel2** and **PPP**.

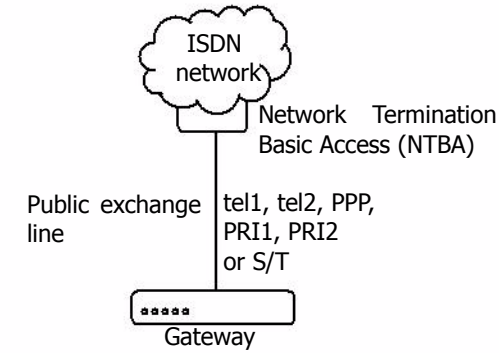

Fig. 10 Gateway on an exchange line

This type of connection makes sense for a number of scenarios:

- Use of the gateway as a gateway for H.323 calls into the public, wired network. This allows H.323 terminals to reach standard terminals in the fixed telephone network and vice versa.

- Use as an IP router to manually dial-up an ISP or the company network. In this way, the gateway and the LAN connected to its Ethernet port are connected to the Internet or Intranet. A separate IP-ISDN router is no longer required.
- Use as an IP router for operation on a permanent connection (IP 400 only). In this way, the gateway is connected to a remote PPP entity (at the ISP or in the company network) via a 64 kbit/s or 128 kbit/s permanent ISDN connection.

The specific configuration varies depending on whether the public exchange line is configured as a "**point-to-point**", "**point-to-multipoint**" or "permanent connection".

Furthermore, the type of signalling for dial-up needs to be set correctly. On public exchange lines EDSS1 signalling is always used, whilst on connections to PBXs the relevant choice may also be a variant of QSIG (see section "The signalling protocols" from page 49). Signalling is of no significance for permanent connections.

Note

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

- In the configuration applet, go to **ISDN interfaces > TEL1** or to the connection with the public exchange line.
- Remove **NT** (only **tel1** and **tel2**).
- Remove **Power** (only **tel1** and **tel2**).
- Remove **100 Ohm termination** (only **tel1** and **tel2**).
- Remove **Permanent Activation** (only **tel1**, **tel2** and **PPP**).
- If your public exchange line is the point-to-point type, check the **Point to Point** box. Remove **Point to Point** if it is a point-to-multipoint connection. This setting is irrelevant for permanent connections. If the connection is operated in mixed mode (one B channel permanently used for a fixed connection, one B channel in dial up mode), the setting depends on the operating mode of the dial-up line (**tel1**,**tel2** and **PPP** only).
- Remove **Disable overlap receive**.
- Remove **Suppress sending of HLC** and **Suppress sending of FTY** (see section "Suppression of specific protocol elements" from page 50).

- Remove **Provide inband call progress tones** (see section "Dial tones" from page 50).
- In the **D-Channel Protocol** field, set the protocol to **EDSS1** (see section "The signalling protocols" from page 49).
- The **Dialtone type** is of no importance in this configuration.
- **Called party** and **calling party number** do not usually have to be modified in any special way in this configuration. Refer here to section 5.2.7 "Dealing with the various ISDN address types" from page 62.

Caution

If the public exchange line is configured as a point-to-point connection, no other ISDN- device may be connected apart from the gateway.

If it is a point-to-multipoint connection, then other ISDN- terminals can be connected there. Take into consideration however that in this case incoming calls can be accepted by virtually all connected terminals. Refer to section 7 "Configuration of call routing" from page 87 to see how to configure the gateway, so that only calls for the desired call numbers are accepted.

If the gateway is used as an IP router, please refer to section 4.2 "Configuration of the WAN interfaces" from page 28 for the configuration of IP routing via the ISDN interface.

5.2.2 Usage as connection for a telephone or another piece of ISDN-terminal equipment

In this case, one or more ISDN-terminal devices will be connected to the interface. It thus operates as a "**point-to-multipoint**" connection from your network provider. This type of usage is only available for the **tel1** and **tel2** interfaces.

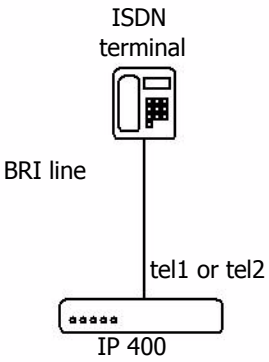

Fig. 11 ISDN terminal on the IP 400

The configuration varies depending on whether the devices to be connected have their own power supply or not. Telephones typically have no power supply of their own and are therefore supplied via the ISDN-line.

Tip

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

- In the configuration applet, call up **ISDN interfaces > TEL1** or the connection to the ISDN equipment.
- Check the **NT** box.
- Check the **Power** box, if a terminal to be connected needs power from the ISDN-line.
- Check the **100 Ohm Termination** box.
- Uncheck the **Permanent Activation** box.
- Uncheck the **Point to Point** box.
- Remove **Disable overlap receive**.
- Remove **Suppress sending of HLC** and **Suppress sending of FTY** (see section "Suppression of specific protocol elements" from page 50).
- In the **D-Channel Protocol** field, set the protocol to **EDSS1** (see section "The signalling protocols" from page 49).

- Select the desired dial tone in the **Dialtone type** field.
- **Called party** and **calling party number** do not usually have to be modified in any special way in this configuration. Refer here to section 5.2.7 "Dealing with the various ISDN address types" from page 62.

Tip

With this type of usage, two telephones or other ISDN-terminals can be connected directly to each of the ISDN -interfaces **tel1** and **tel2**, that is a maximum total of four devices on an IP 400. If an ISDN bus is connected to **tel1** or **tel2**, up to eight terminals can be connected to each bus. If the terminals concerned draw their power from the ISDN network, the total current consumption of all connected devices must not exceed 4 watts.

5.2.3 Use as a public exchange line for an ISDN-PBX

In this case, the gateway interface is connected to an ISDN-PBX as the sole exchange line or as an additional line within an exchange line bundle. In this way, it operates like a "**point-to-point**" connection from your network provider.

The interface must be operated in NT mode here. Consequently, the only interfaces suitable for this type of use are **tel1** and **tel2**.

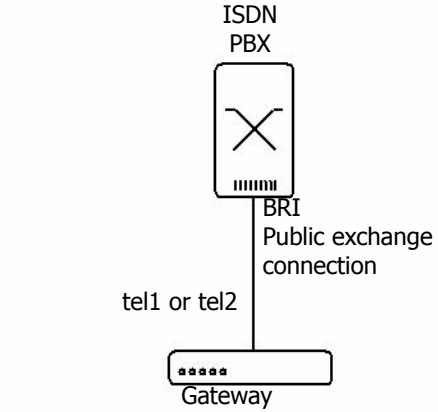

Fig. 12 Gateway as a public exchange line

Note

Some of the BRI PBXs (especially the smaller ones) are intended for connection to a "**point to multipoint**" connection. The ISDN-interface must be configured accordingly. Take a look at the operating manual, if you are not sure what type of connection your PBX expects.

- In the configuration applet, go to **ISDN interfaces > TEL1** or to the connection with the ISDN PBX.
- Check the **NT** box (only **tel1** and **tel2**).
- Remove **Power** (only **tel1** and **tel2**).

Check the **100 Ohm termination** box (only **tel1** and **tel2**).

- If your PBX is intended for operation on a point-to-point connection, check the **Point to Point** box. Remove **Point to Point** (**tel1** and **tel2** only) if operation is intended on a point-to-multipoint connection.
- Remove **Disable overlap receive**.
- Remove **Suppress sending of HLC** and **Suppress sending of FTY** (see section "Suppression of specific protocol elements" from page 50).
- Remove **Provide inband call progress tones** (see section "Dial tones" from page 50).
- In the **D-Channel Protocol** field, set the protocol to **EDSS1** (see section "The signalling protocols" from page 49).
- Select the desired dial tone in the **Dialtone type** field.
- **Called party** and **calling party number** do not usually have to be modified in any special way in this configuration. Refer here to section 5.2.7 "Dealing with the various ISDN address types" from page 62.

The PPP interface is intended solely for connecting a public exchange line to the gateway. It is therefore not possible to connect an ISDN PBX system in this manner (refer however to section 5.2.4 "Use as a subscriber to an ISDN-PBX" from page 58).

If, in addition to the gateway, the PBX is connected to another public exchange line, it must be ensured that both exchange lines are synchronous, using the same clock. This is achieved by connecting the IP 400 **PPP** interface to the direct public exchange line, in parallel to the PBX, using a normal ISDN-cable. The second socket normally available at the provider's network termination (NTBA) can be

used here. If the PBX is not connected to the ISDN fixed network via basic access (e.g. on a primary rate interface), the interface can be connected to an unused PBX BRI subscriber line instead.

Caution

In this case, under no circumstances may the interface be used for incoming or outgoing calls (see section 7 "Configuration of call routing" from page 87). The **Point to Point** checkbox of the interface must be unchecked and the **permanent activation** box checked.

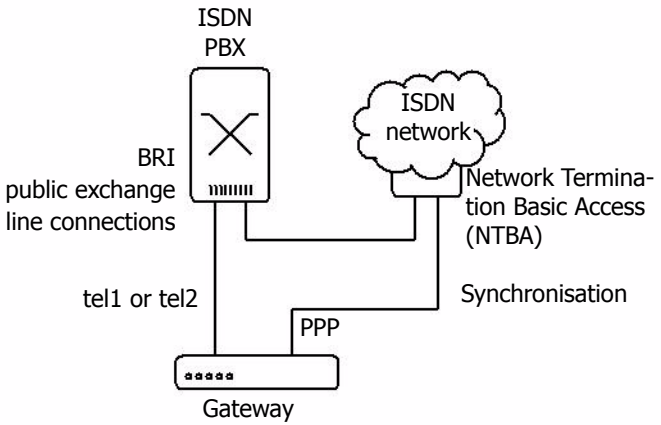

Fig. 13 Synchronisation of a gateway with an ISDN BRI connection

5.2.4 Use as a subscriber to an ISDN-PBX

In certain cases, it might be necessary to connect the gateway as a subscriber to a terminal connection (and therefore also to a point-to-multipoint connection) of the ISDN-PBX. This is necessary, for example, if the PBX does not support an additional exchange line, the existing one is to be operated unchanged, and no tie line is available either (see section 5.2.5 "Use on a PBX tie line" from page 59).

Remember, that in this case various limitations must be expected (depending on the PBX), since it expects a single terminal on this connection and not a piece of switching terminal equipment.

This type of connection only occurs in connection with BRI interfaces and is thus usually only relevant for the IP 400.

In this case, the PBX is connected to the gateway in the same way as an exchange line, as described in section 5.2.1 "Usage at a public exchange line (dial-up or permanent connection)" from page 51. The connection provided by the PBX however is usually a "point-to-multipoint" connection. The **Point to Point** box should be unchecked accordingly. Check the **Disable overlap receive** box, if the PBX does not support single digit dialling to the terminal (see section "Single digit dialling on terminals on point-to-multipoint connections" from page 50).

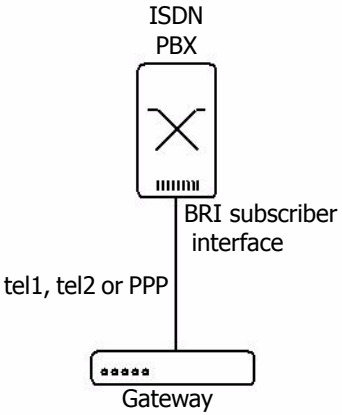

Fig. 14 Gateway on PBX subscriber interface

The limitations mentioned above generally do not apply, if the PBX 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 protocols for operating telephones on PBXs.

5.2.5 Use on a PBX tie line

Connecting the gateway to a PBX tie line is usually the most sensible way of linking two or more PBXs.

In this case, the gateway can be operated as **clock master** (NT) or **clock slave** (TE) (see section 5.2 "Considerations on the configuration of the ISDN interfaces" from page 48). If the PBX has its own clock, the gateway can be operated in TE mode without any difficulty. This is possible at both ends of the connection.

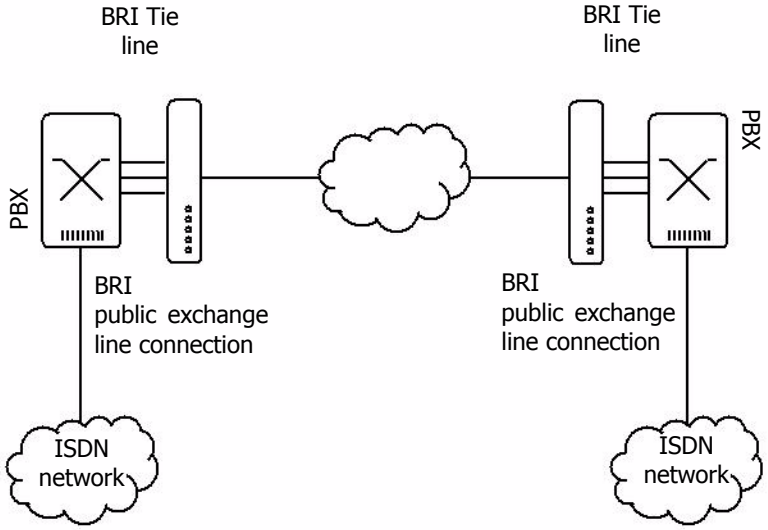

Fig. 15 Gateway on tie line

- In the configuration applet, select **ISDN interfaces > TEL1** or the connection with the tie line.
- Check the **NT** box, if the gateway is to provide the clock. Uncheck the box, if

the PBX provides the clock (**tel1**, **tel2** only).

- Remove **Power** (only **tel1** and **tel2**).
- Remove **100 Ohm termination** (only **tel1** and **tel2**).
- Remove **Permanent Activation** (only **tel1**, **tel2** and **PPP**).
- Check the **Point to Point** box.
- Remove **Disable overlap receive**.
- Remove **Suppress sending of HLC** and **Suppress sending of FTY** (see section "Suppression of specific protocol elements" from page 50).
- Check **Provide inband call progress tones** (see section "Dial tones" from page 50).

Tip

Turn this option off, if it leads to errors when switching calls via the tie line or when clearing calls.

- Set the correct signalling in the **D-Channel Protocol** field (see section "The signalling protocols" from page 49).
- Select the desired dial tone in the **Dialtone type** field (see section "Dial tones" from page 50).
- **Called party** and **calling party number** have to be modified specifically if call numbers with any **type of address** other than **unknown** are transmitted on the tie line. Refer here to section 5.2.7 "Dealing with the various ISDN address types" from page 62.

5.2.6 Looping the gateway into an existing public exchange line

In some cases no other ISDN interface can be used to connect the gateway to the PBX. In such cases it makes sense to loop the gateway into the existing public exchange line.

Per exchange line, this requires one ISDN interface to the public exchange (TE mode) and one to the PBX (NT mode) in the gateway. The IP 400 can also be looped into an exchange line, but in this mode not all of the four possible calls can actually be made in parallel, since the IP 400 has two NT interfaces (**tel1** and **tel2**), but only has one TE interface (**PPP**).

The interfaces are configured towards the public exchange as described in section 5.2.1 "Usage at a public exchange line (dial-up or permanent connection)" from page 51 and towards the PBX as described in section 5.2.3 "Use as a public exchange line for an ISDN-PBX" from page 55. However, call numbers are generally transmitted on a public exchange line with different **types of address**, making it necessary to modify **called party** and **calling party number** specifically. Make absolutely sure you refer here to section 5.2.7 "Dealing with the various ISDN address types" from page 62.

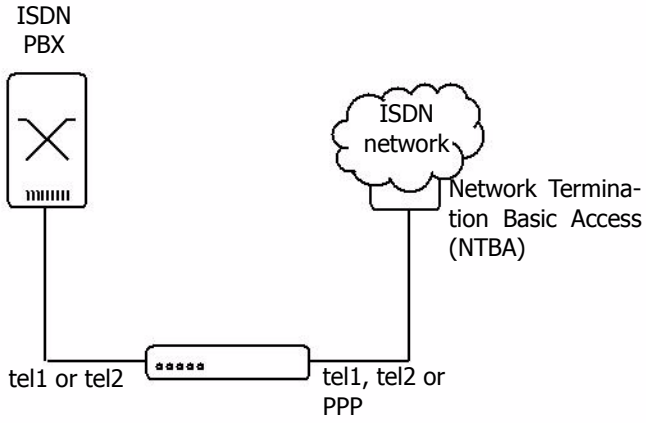

Fig. 16 Looping the gateway into an existing exchange line

5.2.7 Dealing with the various ISDN address types

Call numbers are always treated internally by the gateway as **unknown type of number**. In ISDN however, there are various types of call numbers (see Table 8) with the effect that call numbers are only ever interpreted in combination with their number types. On an exchange line in Germany for example a call number `0711654321` with the type of number **unknown** corresponds to the call number `711654321` with the type of number **national**. This is due to the fact that in Germany the code for national numbers is `0`. On the other hand the call number `41551234` with the number type **unknown** refers to a connection within one's own local network, whereas the same number `41551234` with a number type **international** refers to a connection in the local network of Pfäffikon in Switzerland.

The call number type unknown therefore has to be standardised in order to evaluate call numbers within the gateway. This can be done with the help of entries in the so-called **CGPN (calling party number) map** and **CDPN (c**alle**d p**arty **n**umber) **map** , which can be defined both on the ISDN interfaces, and in the individual gateway definitions.

Name	Description	Typical use	Abbreviation[1]	Code[2]
Unknown	Unspecified	Number called in outgoing call.	u	
Subscriber	Call number in local network.	Number called in incoming call.	s	
National	Call number with area code	Calling number from home country.	n	0
International	Call number with country code and area code.	Calling number from abroad.	i	00
Abbreviated		Unusual	a	

Name	Description	Typical use	Abbre-via-tion[3]	Code[4]
Network specific		Unusual	x	

1. In the CGPN/CDPN mappings
2. Equivalent codes for outgoing calls in Germany
3. In the CGPN/CDPN mappings
4. Equivalent codes for outgoing calls in Germany

Table 8 Number types

The following map entries for the calling number are included in the standard configuration of all ISDN interfaces and gateways (see Fig. 17 on page 64):

Type	Number type	Number prefix	Replaced number prefix	Use
Incoming calling number	National	Blank	0	Places the discriminating digit 0 in front of national CLIs
Incoming calling number	Interna-tional	Blank	00	Places the discriminating code 00 in front of international CLIs

Table 9 CGPN mappings in the standard configuration

This ensures that the calling number is displayed correctly for incoming calls of all number types.

A typical application of CDPN mappings is the manipulation of the root number on point-to-point connections, for incoming calls. Here, the root is removed from the called number, which is usually received as a number of type **subscriber**. Then only the extension number is dealt with in the routing table of the gateway. Fig. 18 on page 64 shows such a configuration.

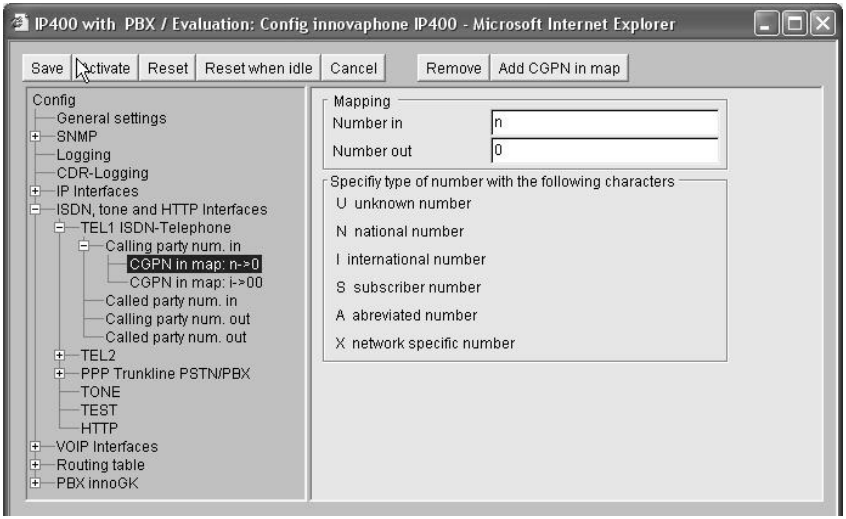

Fig. 17 Standard CGPN/CDPN maps

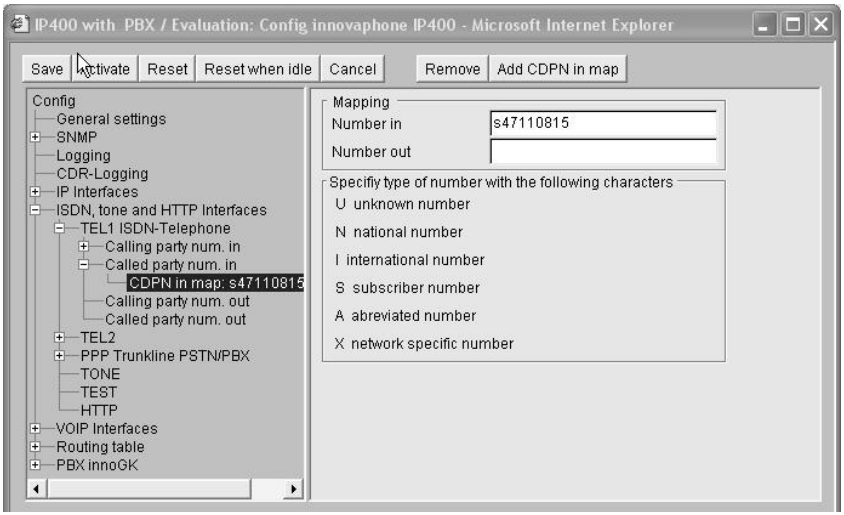

Fig. 18 Manipulation of the root number by means of CDPN maps

- 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 display by clicking on the + symbol in the white square next to the interface name.
- Select one of the following lines on the left-hand side.
  - **Calling party num. in** if you want to edit 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 edit the called number of incoming calls
  - **Called party num. out** if you want to edit the called number of outgoing calls.
- You can add maps by clicking on the **Add CGPN/CDPN in/out map** button at the top edge.
- Under **Number in** define the number type and –prefix that you wish to have replaced. The number type is denoted using the abbreviation from Table 8 on page 63.
- Define the substitution under **Number out**.

The example shown in Fig. 18 on page 64 results in the called number of incoming calls (**CDPN in**) being replaced if the call number type is **subscriber** (abbreviation `s`) and the number begins with the code `47110815`.

Note that call numbers within the gateway are always processed in **unknown** format. That is why the result of a number replacement, for incoming calls, is always of the type **unknown** and the call number type of outgoing calls to be replaced is likewise 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.

5.3 Considerations on the configuration of the virtual interfaces

The gateway has the virtual interfaces **TONE, TEST** and **HTTP**. These are not physical interfaces, but virtual interfaces, implemented within the device.

5.3.1 The public dial tone interface TONE

The gateway has an internal **TONE** interface. It only makes sense to use it as a destination for a call. If a call arrives at the TONE interface, it is not forwarded, but the dial tone configured for the interface is played (the incoming call is acknowledged with **SETUP_ACK** and a media channel is set up). The call is rejected if a further digit is dialled or if the original call contained other digits already dialled.

The Tone interface can be used to play a caller a public dial tone, even though the call has not yet been connected to a "genuine" public exchange line. This happens particularly with **least-cost-routing** scenarios, where the call can only be switched once some of the dialled digits have been analysed.

The Tone interface can process a number of calls simultaneously. The dial tone played is set in the **Analogue/ISDN Interfaces**, **Tone** under **Tone provider interface configuration** .

5.3.2 The TEST interface

The gateway has an internal **TEST** interface. It only makes sense to use it as a destination for a call. If a call arrives at the **TEST** interface, it is connected and the hold music stored in the non-volatile memory is played. Subsequently dialled digits are ignored.

Please note that the **TEST** interface can only process calls with **G.729A** or **G.723**. No music is played for incoming calls with **G.711**.

It is not possible to configure this interface.

5.3.3 The HTTP interface

The HTTP interface makes it possible to play music, make announcements or provide other information via an external data source. The configuration only makes sense in combination with the innovaphone PBX. For further information please refer to the "Administrator's Manual - innovaphone PBX".

6 Configuration of VoIP interfaces

In the same way as ISDN interfaces lead the world of classical telephony, "VoIP interfaces" are channels to the world of **Voice over IP**. If your gateway needs to communicate with other devices via VoIP, access to these devices has to be configured as a VoIP interface.

These can be different types of equipment:

- 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 to connect analogue terminals or a DECT base station,
- Third-party VoIP gateways, as a gateway to telephone switches or into the SS7 network, for example,
- Further gatekeepers for call control,
- VoIP PC programs such as innovaphone Softwarephone.

Each VoIP interface defines access to a group of devices, which are all treated similarly. This allows, for example, all IP telephones at one location to be configured via a single VoIP interface. Since your gateway allows the definition of 12 different groups, it is able to communicate in all with several hundred VoIP devices.

The configuration is performed in the **VoIP Interfaces** area of the configuration applet.

6.1 General considerations on the configuration of the VoIP interfaces

The telephony infrastructure in the VoIP environment always consists of three different modules:

- VoIP end points

  These 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 innovaphone Softwarephone. Such end points are usually assigned to just a single user.

- VoIP Gateways

  These are gateways to other telephony networks or technologies. These can be gateways to the ISDN network or to the analogue telephone network, but

also adapters to connect traditional, analogue terminals or existing PBXs. Gateways usually make it possible to reach a number of users or terminals.

- Gatekeeper

  Gatekeepers are used for call control and call switching. They can manage VoIP terminals and gateways, interpret call numbers and names and thus switch calls. They adopt the role of the PBXs or the exchange in traditional telephony. Gatekeepers are optional however, since, optionally, end points and gateways can also communicate directly with one another.

Your innovaphone gateway always includes a gatekeeper that you can use as desired. Gatekeepers and VoIP end points or VoIP gateways usually communicate via the so called **RAS** protocol. Your gateway can be used with or without **RAS** protocol, as you wish. As far as the telephony features are concerned, no disadvantages result from operating without **RAS**. Even the sophisticated routing functions of your gateway can be fully used in this operating mode.

Using the **RAS** protocol though, offers a number of advantages:

- The gatekeeper is able to convert logical device names (referred to as **aliases**) into IP addresses. This allows VoIP devices with dynamic IP addresses to be integrated. Only in this way can VoIP devices be used which have been configured via 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 have an overview of the status at any time. Furthermore, the switching of calls can be made dependent on availability, without having to make this time-consuming check at the time of the call. This results in a considerable improvement in dealing with errors.
- For many third party VoIP devices, the **RAS** protocol is mandatory.

We recommend putting your gateway's gatekeeper into operation and, if possible, using the **RAS** protocol. Individual VoIP devices with which your gateway is supposed to communicate which do not allow the **RAS** protocol can still be addressed directly without any difficulty.

Of course, you can also operate your gateways in conjunction with a gatekeeper which is already available.

Note however, that a number of features in a VoIP network also depend on the gatekeeper in use. The specific features available when operating with an external gatekeeper therefore vary depending on the individual case.

6.1.1 Understanding your gateway's gatekeeper

There are basically 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 features of your gateway, although device management is optional.

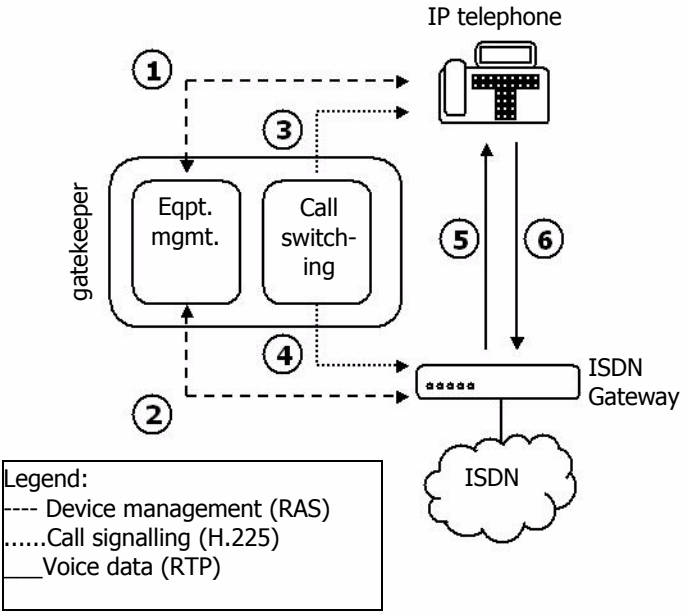

Fig. 19 Call sequence with a gatekeeper and RAS

Fig. 19 on page 69 shows a scenario with an IP telephone, an ISDN gateway and a gatekeeper. The gatekeeper can be another innovaphone gateway or, alternatively, it can be the gatekeeper incorporated in every innovaphone gateway. For a clearer understanding though, the gatekeeper and ISDN gateway are shown separately.

The individual steps of a call which are relevant in this context are displayed in the following. In reality, the procedures can be far more complex.

- Both the IP telephone (1.) and the ISDN gateway (2.) register with the gate-

keeper's device management. They submit their identity and their current IP address in the process. This step requires the RAS protocol and therefore doesn't apply when operating 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 the gateway exchange their IP addresses. Further signalling between the two of them goes via the gatekeeper.
- The IP telephone and ISDN gateway directly set up the two voice channels (5. and 6.) between one another.

The source and destination of the call do not necessarily have to use the same gatekeeper. Fig. 20 on page 71 shows the sequence of a call which is forwarded via two gatekeepers.

The sequence of the call is the same for the destination and source as illustrated by Fig. 19 on page 69. The more complex infrastructure is fully concealed by the gatekeepers. Only two gatekeepers now have to be known to one another. This again can be done via the RAS protocol, either by one gatekeeper logging on to the other or by both gatekeepers logging on to the other (step 1). The incoming call from the IP telephone is now forwarded by the first gatekeeper to the second, which in turn forwards it to the destination gateway. In this way, very complex structures can be set up involving a number of gatekeepers.

The device management is configured in the configuration applet in the **VoIP Interfaces** area.

The devices are managed dynamically by means of **Registration** in the **RAS** (**R**egistration, **A**dmission and **S**tatus) protocol. First of all the registering device finds out which gatekeeper is responsible. During this procedure, referred to as **Gatekeeper discovery**, the terminal searches the network for a gatekeeper with the desired gatekeeper ID, a logical name for the gatekeeper.

A number of gatekeepers can be operated in a network and found by "their" respective devices by means of the gatekeeper ID. However, many external gatekeepers do not support the gatekeeper ID.

Tip

Many gatekeepers and also some VoIP devices do not support the Discovery procedure. In this case the gatekeeper's IP address has to be configured in the device to be registered. Likewise, multicasts of routers are not usually transmitted. That is why the IP address of the gatekeeper also has to be registered if it is separated from the registering device by a router.

The device transmits its identity and IP address once the gatekeeper has been identified. This can be a logical name, a telephone number or both. The device is ready for operation and accessible if the ID is OK. Devices that log on to the gatekeeper using the RAS protocol are configured in **Gatekeeper client group mode**.

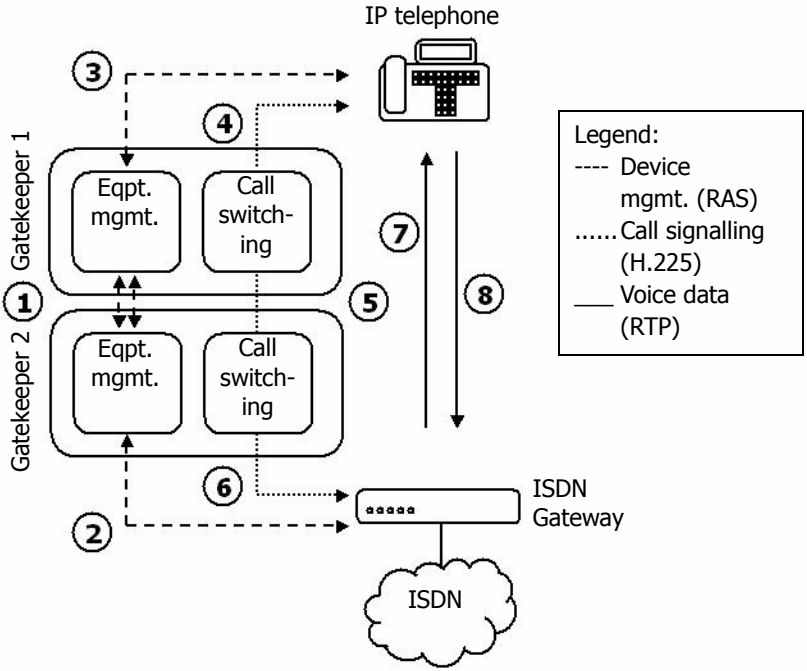

Fig. 20 Call sequence with two gatekeepers and RAS

A number of VoIP devices do not support the RAS protocol. Such devices can nevertheless still be managed by being configured statically (hence with fixed IP addresses) in the gatekeeper. Steps 1 and 2 then no longer apply in the sequence in Fig. 19 on page 69. Such devices are configured in **Gateway** or **Gateway group** mode.

Of course, your gateway itself can also log on to another gatekeeper with RAS protocol as illustrated in Fig. 20 on page 71. This operating mode is configured in **Registration at Gatekeeper as endpoint** or **Registration at Gatekeeper as Gateway** mode.

6.1.2 Gatekeeper discovery

Gatekeeper discovery works via **IP multicast** packets which a gatekeeper client transmits if it wants to find a suitable gatekeeper.

Normally, such packets are only transmitted within one's own LAN segment and, in particular, are not routed into other networks. That is why gatekeepers can only be found within one's own LAN segment. However, routers can be configured so that they transfer such packets according to certain rules. This makes it possible to also find gatekeepers which are connected via WAN links.

The difference made is based on the so called **multicast addresses**. The **multicast address** used for **gatekeeper discovery** is `224.0.1.41`.

6.1.3 The Gatekeeper ID

Each gatekeeper within a network can be identified by means of its own **Gatekeeper ID**. This ID allows the administrator to operate a number of gatekeepers in parallel within a network, with each terminal nevertheless identifying the "correct" gatekeeper by means of **gatekeeper discovery**. The ID is defined directly in the configuration applet in the **Gatekeeper ID** field within the **VoIP Interfaces** area.

If you have assigned your gateway a gatekeeper ID, it will only answer those **RAS Discovery** inquiries in which either this ID or no **Gatekeeper ID** at all is specified. Even if your terminals have configured the gatekeeper permanently and therefore do not perform **gatekeeper discovery**, the RAS registrations are again only accepted if they include the configuration of the correct gatekeeper ID or of no gatekeeper ID at all.

A configured **Gatekeeper ID** applies to the entire gateway.

In general, you can operate without **Gatekeeper ID** if only one gatekeeper is operated in your network or if **Gatekeeper discovery** is not used.

6.1.4 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 regardless of the **Gateway mode** used.

Option	Description
Disable Faststart	The basic settings allow the H245 Faststart procedure. Outgoing calls are implemented with Faststart, incoming calls with Faststart are answered with Faststart. The **Disable Faststart** option has to be activated if the H245 Faststart procedure is to be disabled. Outgoing calls are made without Faststart and incoming calls, with or without Faststart, are answered without Faststart if this option is deactivated. We only recommend activating the **Disable Faststart** option if compatibility problems occur with third party products.

Tip

Some ring tones might not be audible, if connections are established to end points with H.323 version 2. In this case, update the protocol of the remote entity.

Disable H245-tunneling	In the basic settings, the voice data connection is negotiated in the TCP signalling connection[1] already available. A TCP connection of its own is established for this negotiation if **Disable H245-tunneling** is activated. This applies to the signalling connection out of the gatekeeper. A separate connection for negotiations is not required if **Disable H245-tunnelling** is deactivated, which can be of advantage in connection with **NAT** and **firewalls**. We only recommend activating **Disable H245 tunnelling** if compatibility problems occur with third party products.

Tip

Some ring tones might not be audible, if connections are established to end points with H.323 version 2. In this case, update the protocol of the remote entity.

Option	Description
Enable T.38 fax protocol	Voice connections used for transmitting a fax are transmitted using the special **Fax over IP** protocol **T.38**. Otherwise fax transmissions are not treated specially. We always recommend this option unless compatibility problems occur with third party products.
fake connect	This is used to signal a connection to the calling party as soon as **in-band** information is received from the called party even though no connection has yet been established. This could, for example, be ring tones or network fault announcements. Some VoIP devices only activate the voice channel once the connection has been established. In such cases, announcements made previously cannot be heard by the caller. This option resolves the problem. Only use this option for VoIP devices showing this problem.
Suppress sending of HLC	Prevents the transmission of so called **high layer compatibility (HLC)** information elements. This is required if the receiving VoIP device responds erroneously to **HLCs**. Otherwise the HLCs are forwarded transparently by the gatekeeper. Only use this option if a VoIP device with this kind of fault needs to be used. Do not use this option when linking PBX systems via innovaphone gateways, since otherwise under certain circumstances important information could be lost.
Suppress sending of FTY	Prevents the transmission of so called **facility (FTY)** messages. This is required if the receiving VoIP device responds erroneously to **FTYs**. Otherwise the **FTYs** are forwarded transparently by the gatekeeper. Only use this option if a VoIP device with this kind of fault needs to be used. Do not use this option when linking PBX systems via innovaphone gateways, since otherwise under certain circumstances important information could be lost.

Option	Description
Generate connected time	Causes the gatekeeper to add a time stamp with the local gateway time to outgoing **Connect messages**. Use this option if the called VoIP devices rely on the time stamp but the call sources (e.g. the ISDN network) do not supply it.

1. From a technical viewpoint, the H.245 protocol doesn't establish its own TCP connection, but shares the H.225 TCP connection.

Table 10 H.323 protocol options

6.1.5 Setting up a gatekeeper on another gateway

If the gatekeeper is not to operate on its own gateway, a **Remote gatekeeper address** can be configured in the **VoIP Interfaces** area of the configuration applet.

The gateway tries to log onto a remote gatekeeper, if its IP address is entered in the **IP address** field. If this attempt to register is unsuccesful, the gateway tries to log onto an alternative gatekeeper, provided an alternative address has been entered in the **Alternate Gatekeeper** field.

It is important to enter an alternative gatekeeper IP address, particularly when using redundant systems.

If the gatekeeper operates with a gatekeeper ID (see section 6.1.3 "The Gatekeeper ID" from page 72), enter it into the **Gatekeeper ID** field.

The **Password** corresponds to the H.235 password required for logging on to the remote gatekeeper.

By clicking on the **Disable dynamic signalling port** button, a fixed **Signalling port** can be entered, which, for example, can be configured on firewall systems.

6.1.6 Voice transmission

Your gateway supports various methods of voice transmission using IP. For calls between one of your gateway's ISDN interfaces and a VoIP device defined by this VoIP interface, you can make the relevant definitions in the **Codec configuration** area. Note that calls between two VoIP devices, i.e. from IP to IP, do not take this setting into account, since the parameters are negotiated directly by the terminals and their configuration is thus relevant.

Voice coding

There are various ways of encoding voice transmission. Some of the available encoding options compress speech, others do not. Your gateway supports various customary voice-encoding schemes, whose properties are described in the following table:

Encoding	Bandwidth[1] per call	Minimum delay[2]	Properties
G.711A	64 kbit/s	20 ms	No compression, best voice quality (comparable to digital telephone systems). Sound digitisation using European encoding
G.711U	64 kbit/s	20 ms	As above; sound digitisation using US encoding[3]
G.726-16 G.726-24 G.726-32 G.726-40	16, 24, 32, 40 kbit/s	20 ms	Intended only in exceptional cases for fax and modem data.
G.723-53	5.3 kbit/s	30 ms	Good voice quality (comparable to analogue telephone systems)
G.723-63	6.3 kbit/s	30 ms	Slightly better voice quality than G.723-53 with slightly greater bandwidth.

Encoding	Bandwidth[1] per call	Minimum delay[2]	Properties
G.729A	8 kbit/s	20 ms	Best voice quality of all compression encoding schemes, lowest minimum delay.

1. The specified bandwidth is merely the nominal bandwidth of the encoding algorithm. Additional control information is transmitted in the network together with the compressed data, with the effect that, depending on the configuration, the total bandwidth required may turn out to be considerably higher.
2. This is the minimum delay caused by data encoding and packeting. Further delays occur in connection with the transmission of data in networks.
3. You can use both **µ-law** and **A-law** encoding, regardless of the encoding used on your ISDN connection. In both cases, the encoding is correctly adapted to the ISDN connection.

Table 11 Voice encoding schemes

The type of voice data compression can be chosen in the **Standard** field. This setting is used preferentially. If the remote VoIP device does not support the encoding selected, encoding supported by both parties will be negotiated. Check the **exclusive** box if you want to force the use of the selected encoding. This can of course result in call failure if your gateway and the remote VoIP device do not support a common **Coder**.

Tip

The best trade-off between voice quality and required bandwidth is offered by G.729. Select this scheme for remote telephony gateways accessed via the Internet, the intranet or heavily loaded local area networks. Use G.711 in powerful local networks, to ensure best voice quality. You need G.723.1 for connections to telephony gateways which do not support the G.729 standard. G.726 encoding should only be used in cases where fax data is to be transmitted on a line without T.38.

Packet size

You can set the size of the packets used for exchanging encoded voice data between telephony gateways under **Packet size** (**ms**). The value entered here defines the period of time for collecting voice data prior to transmitting it as a voice data packet. Voice transmission is delayed correspondingly. A value of 30 ms is perceived by the human ear as virtually without delay, a value of 100 ms similarly, does not irritate most users.

Larger packets cause greater **Delays** in voice data transmission, but cause less stress to the network since the **Overhead** involved in transporting packets in the network is lower.

Note that the overhead is increased considerably if the **Packet size** is reduced, since the overhead data required for transmission with the IP-protocol (on a LAN) and also in the PPP protocol (in the WAN) remains the same per packet, whilst the voice data quantity, and with it the data actually used, is reduced. The bandwidth actually required is therefore considerably higher (depending on the packet size) than the pure voice data bandwidth as specified in Table 11.

By background noise (crackling) or greatly increased delays, you can tell if voice data can no longer be transmitted quickly enough, due to insufficient bandwidth or excessive network transit times. In such a case, increase the packet size for the telephony interface concerned to reduce the effect, or select a more efficient encoding scheme (for example G.723-53 instead of G.729). Table 12 shows the required bandwidths, depending on the encoding and packet size.

Encoding scheme	Effective bandwidth used (in kbit/s) related to packet sizes of				
	20 ms	**30 ms**	**60 ms**	**90 ms**	**150 ms**
	possible connections per 64 kbit/s				
G.711	83 kbit/s	77 kbit/s	70 kbit/s	68 kbit/s	67 kbit/s
G.723-53	24 kbit/s	18 kbit/s	12 kbit/s	9 kbit/s	8 kbit/s
	2	3	5	6	8
G.723-63	25 kbit/s	19 kbit/s	13 kbit/s	10 kbit/s	9 kbit/s
	2	3	5	6	7
G.729	27 kbit/s	21 kbit/s	14 kbit/s	12 kbit/s	11 kbit/s
	2	3	4	5	6
G.726-16	19 kbit/s at 150 ms				
	3				
G.726-24	27 kbit/s at 150 ms				
	2				
G.726-32	35 kbit/s at 150 ms				
	1				
G.726-40	43 kbit/s at 150 ms				
	1				
T.38	14 kbit/s at 120 ms[1]				
	4				

1. Faxes are transmitted using the T.38 protocol at a fixed packet size of 150 ms. Strictly speaking, the fax data is not compressed. There is merely no **overhead** which would otherwise be necessary for analogue transmission.

Table 12 Required bandwidths depending on the packet size

The values specified here are approximate values, as determining the bandwidth exactly depends upon a number of factors.

Tip

The effective bandwidth required can vary according to conditions in the given environment. On the one hand, routers used in the transmission link can apply special compression techniques (RTP header compression) and thus reduce the required bandwidth. On the other hand, voice channels being switched off during pauses in speech also results in reduced bandwidth requirement. The values specified in the table represent the most unfavourable values for transmission over long-distance routes (PPP).

Please note however that the specified values only apply to one direction. The overall values for a call without **Silence compression** are thus twice as high. Bandwidths of communications media are usually specified per direction anyway. An ISDN connection uses 64 kbit/s per direction, the data in the table can thus be compared intuitively with the familiar bandwidths.

A further way of saving bandwidth is by not transmitting any data during pauses in speech. Considerable bandwidth can be saved in this way, since only one party usually speaks at a time during a conversation. This function is referred to as **Silence compression** and can usually be activated without any loss of quality.

Absolute silence at one end would cause some irritation at the active end, since users often assume that the connection is faulty, if they do not hear anything from the remote end. To avoid this situation, an artificial background noise referred to as **comfort noise** is introduced at this end. Information is exchanged at regular intervals in order to match the volume of these simulated background noises to the actual background noises at the currently silent end. These so called **comfort noise updates** still require considerably less bandwidth than the bandwidth saved by **silence compression**. **Silence compression** and **Send comfort noise updates** should therefore be activated together and only deactivated if compatibility problems arise involving third party devices.

6.1.7 Defining the VoIP Tracing Level

You can define the subject areas for which your gateway records **traces** by setting the **tracing level**. This is done on the initial page in the **VoIP Interfaces** area.

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

Table 13 VoIP **Tracing Level**

The logging of traces does not cause any performance problems since the entries are merely written to a special buffer in your device's main memory. This is a ring buffer though, with the effect that new messages overwrite older ones. It could therefore make sense to hide some uninteresting aspects to obtain a complete trace for a particularly difficult situation.

6.2 Management of VoIP devices via RAS (Gatekeeper)

The management of VoIP devices in your gateway, using the RAS protocol, is the recommended way of managing devices.

- Switch to a new **Undefined GWn** in the **VOIP Interfaces** configuration applet.
- Set the **Gatekeeper ID** as required (refer to section 6.1.3 "The Gatekeeper ID" from page 72).
- To define the VoIP devices that are to be managed by the gatekeeper, in **VoIP Interfaces** under **GW1** to **GW12** set up a definition in the mode **Gatekeeper client group**.
  If necessary, restrict the access of VoIP devices to your gateway. To do this, enter the network address of the IP network with the authorised devices under **IP address**. Set the network mask under **IP mask**.
  In this way, you can define the group of authorised VoIP devices as you wish. It is not necessary, for the configured network to actually be an existing network.

- For the VoIP devices to be managed, define the H.323 protocol options (see section 6.1.4 "H.323 protocol options" from page 73).
- Create an **alias** entry for every VoIP device. This is done by clicking on the **Add alias** button.

  For VoIP end points, you should define the assigned extension number or MSN here as **E.164 Address** and the name as **H.323 Name**. For VoIP gateways it is sufficient to define the name.

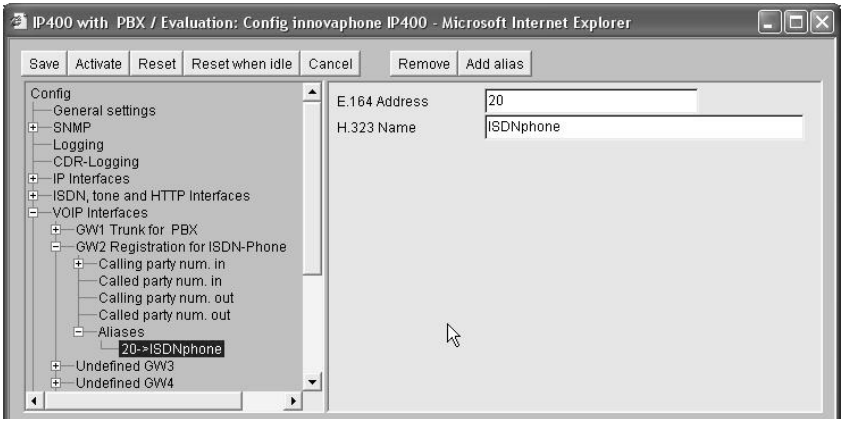

Fig. 21 Entering a VoIP device

Please note, that it always suffices for the VoIP device to register with its name. In general, the registration is checked to see if the details contained in the registration match with a configured alias entry. If details have been omitted during registration (the E.164 address for instance), then these are not checked. A terminal can thus register with just its name. Its extension number is only defined in the gatekeeper, in the alias entry associated with its name. However if the terminal registers with name and number, you can't just change the number in the gatekeeper, since the terminal would continue to log on with an incorrect **E.164 Address**, after the change.

If a VoIP device registers with several H.323 aliases simultaneously, each one is compared with those defined in your gatekeeper and the registration is only carried out once all aliases have been defined.

- If it is necessary to modify call number processing (see section 5.2.7 "Dealing with the various ISDN address types" from page 62), then make the entries, using the **Add CGPN** / **CDPN in** / **out map** button, in the area **Calling** /

Called party num. in / **out**.

- If the configured VoIP devices are also to have access to your gateway's ISDN interfaces, define the voice transmission parameters (see section 6.1.6 "Voice transmission" from page 76).

6.2.1 Special features, when configuring innovaphone devices

innovaphone devices provide the option to register using their serial number. This is always done if they are configured for operation with a gatekeeper but no alias name has been configured in the profile. In this case for example, the IP telephone tiptel innovaphone IP tries to log on with the **H.323 Name** `IP200-03-`***`xx-xx`*** where ***`xx-xx`*** is taken from the last four digits of the IP telephone's serial number. This makes it possible to operate with all IP telephones configured absolutely identically.

Tip

Please note, that terminals, managed by the optional innovaphone PBX, do not have to be configured in the **VoIP Interfaces** area.

- In the configuration applet, under **VOIP Interfaces** go to the **GWn** which you have configured for the management of VoIP devices via RAS (see section 6.2 "Management of VoIP devices via RAS (Gatekeeper)" from page 81).
- Create an appropriate Alias entry in the gatekeeper. The serial number is entered in the **H.323 Name** field and the telephone's extension number is defined in the **E.164 Address** field.
- If the IP telephone is also to be assigned a "descriptive" name, then set up a further alias, with the same extension number as text, in front of the serial number alias. Enter the desired name as **H.323 Name**.

To be able to use all of the available features, terminal devices should be managed by the optional innovaphone PBX components.

6.3 Static management of VoIP devices

If you are using VoIP devices that don't support dynamic registration using the RAS protocol, they must be configured statically. As a consequence, the accessibility of the devices no longer has to be constantly checked, and it is not possible to use changeable IP addresses (i.e. for example with DHCP). There are no other disadvantages though.

You can configure the VoIP devices separately, or in groups. This can be particularly practical when using a large number of VoIP clients that do not support RAS.

- To define a single VoIP device to be managed statically, in the area **VoIP Interfaces** under **GW1** to **GW12** set up a definition in **Gateway** mode
  Or:
  To define a group of VoIP devices that are to be managed statically, set up a definition in **Gateway group** mode in the **VoIP Interfaces** area under **GW1** to **GW12**. This way you grant access to all VoIP devices on an IP network. Proceed carefully, when setting up such gateway groups, and make sure that you prevent unwanted access (e.g. those trying to gain access to your gateway from the Internet).
- For a single VoIP device, enter its address under **IP address**.
  Or:
  For a group of VoIP devices, enter the address of the IP network, where the authorised devices are located, under **IP address**. Set the network mask for the network under **IP mask**.
  In this way, you can define the group of authorised VoIP devices as you wish. It is not necessary, for the configured network to actually be an existing network. You allow access to all VoIP devices by setting the IP address to `0.0.0.0` and the IP mask to `0.0.0.0`.
- Set the H.323 protocol options for the VoIP devices to be managed (see from page 73).
- If it is necessary to modify call number processing (see 62), then make the entries, using the **Add CGPN** / **CDPN in** / **out map** button, in the area **Calling** / **Called party num. in** / **out**.
- If the configured VoIP devices are also to have access to your gateway's ISDN interfaces, define the voice transmission parameters (see from page 76 onwards).

6.4 Registering the gateway with another gatekeeper

If your gateway (or the gatekeeper contained therein) has to log on to another gatekeeper as, for instance, in the scenario illustrated in Fig. 20 on page 71, this can be done using a gateway definition in **Register at gatekeeper as gateway** mode. As a result, your gateway will be registered as a VoIP gateway (see page 67). In most cases, this is the correct mode. Use the **Register at gatekeeper as endpoint** mode, if the gatekeeper only allows the registration of a VoIP end point. On the other hand, the behaviour is identical in both modes, if the external gatekeeper is an innovaphone gateway.

- To register with a gatekeeper, in the area **VoIP Interfaces** under **GW1** to **GW12** , set up a definition in **Register at gatekeeper as gateway**, or **Register at gatekeeper as endpoint** mode.
- You can leave the **IP address** field empty, if the gatekeeper is to be found using **Gatekeeper Discovery** (see section 6.1.2 "Gatekeeper discovery" from page 72). Otherwise, enter the IP address of the gatekeeper there.
- If the gatekeeper operates with a gatekeeper ID (see section 6.1.3 "The Gatekeeper ID" from page 72), enter it into the **Gatekeeper ID** field.
- Define the **H.323 Alias** required to identify yourself with the gatekeeper by clicking on the **Add alias** button. It usually makes the most sense if the gateway only registers with an H.323 name and not with an E.164 address (i.e. with a telephone number). This is obligatory with some gatekeepers though. Look therefore at the documentation for the gatekeeper where you want to register.
- Define the H.323 protocol options for communication with the gatekeeper (see section 6.1.4 "H.323 protocol options" from page 73).
- If it is necessary to modify call number processing (see 62), then make the entries, using the **Add CGPN** / **CDPN in** / **out map** button, in the area **Calling** / **Called party num. in** / **out**.
- If calls from external gatekeepers are also to have access to your gateway's ISDN interfaces, define the voice transmission parameters (see section 6.1.6 "Voice transmission" from page 76).

6.5 Routing via the ENUM protocol

Another option for routing calls is to use the ENUM protocol. ENUM stands for a protocol, which has to do with mapping so-called E.164 numbers to Uniform Resource Identifiers (URI). With the help of the ENUM protocol, it is possible to check whether a number can be called via a cost effective Internet connection, or rather via an ISDN connection. For more information on the subject of ENUM and how to configure ENUM on your innovaphone gateway, see section 4.2.9 "The ENUM protocol" from page 40.

7 Configuration of call routing

Call routing is the main feature of the gateway. It determines which calls are able to be accepted by the gateway and where they are to be switched to.

7.1 General considerations on the configuration of call routing

Your gateway's gatekeeper is responsible for call routing. It is controlled by so called **routes**.

Tip

These are voice routes, not to be mistaken with the data or IP routes described in section "Configuration of the IP routes" from page 32.

Each route defines a permitted path for a call, from the interface where the call arrives, to the interface from which the call departs. The interface concerned can either be an ISDN interface (whose configuration is described in section 5 "Configuration of the ISDN interfaces" from page 46) or a VoIP interface (see section 6 "Configuration of VoIP interfaces" from page 67).

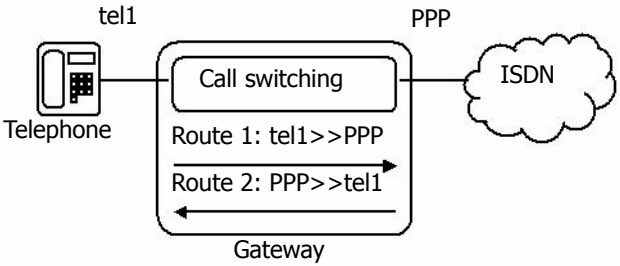

Fig. 22 Unidirectional routes

A route is always defined for one call direction only. Two routes are thus necessary for bidirectional calls. One for each direction.

Routes define call routing within a single gateway. If a call is to be switched via two gateways, a separate route is required in each gateway. Four routes are then required in total, for bidirectional calls.

Fig. 23 on page 88 shows a scenario in which calls are switched via VoIP between a telephone connected to gateway A and the ISDN network connected to gateway B.

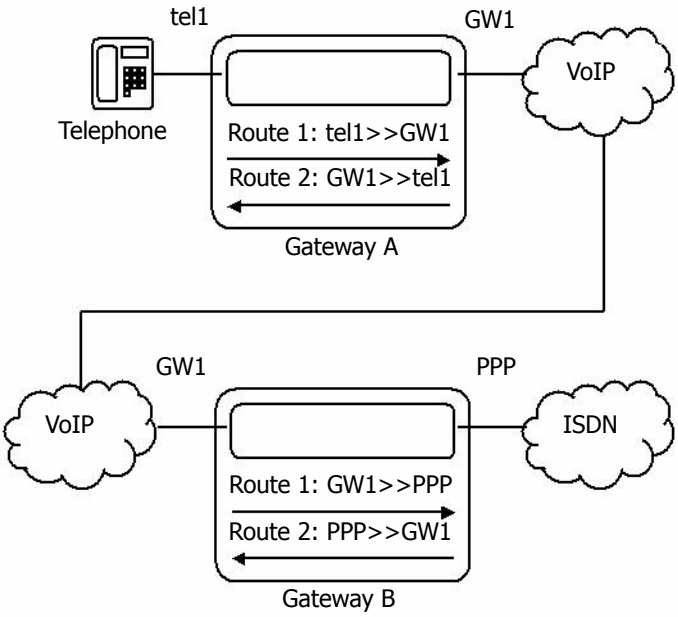

Fig. 23 Routes via 2 gateways

The type of call is of no relevance to call switching. In principle, any call can be forwarded to any given interface. For instance:

- For a call from your telephone, via your network provider's fixed network, the call is switched from the gateway's ISDN-interface, where your ISDN-telephone is connected, to the ISDN-interface to which the corresponding exchange line is connected.
- For a call from a remote 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 connected.

Calls from different interfaces are often handled in the same way. In the scenario illustrated by Fig. 22 on page 87 it may, for example, be desired to allow calls from both TEL1 and TEL2. That is why a number of interfaces can be specified as permitted sources for a route.

Of course, call switching often also depends on the call numbers dialled. That is why it is necessary to define the validity of routes for calls with certain destination numbers. This is done by attaching a so called **Map** entry to the route of each valid dial prefix. Each map entry therefore determines that calls from the source interfaces specified in the route with the combination of digits specified in the map, can be connected to the destination interface defined in the route. Fig. 24 on page 89 shows such a scenario.

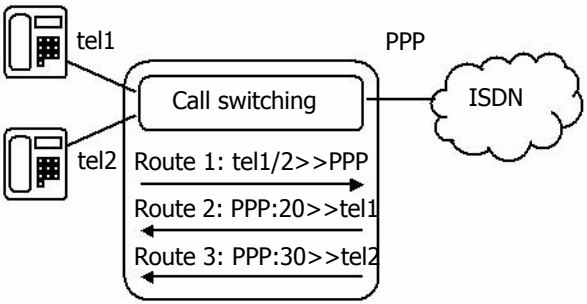

Fig. 24 Call number dependent routes

Sometimes it is useful to modify the called number in the course of call switching. Fig. 25 on page 90 shows the configuration of such a scenario in the configuration applet of your gateway. The MSNs (`529969` and `529096`) assigned to a point-to-multipoint connection are mapped onto the internal extension numbers `20` and `30`.

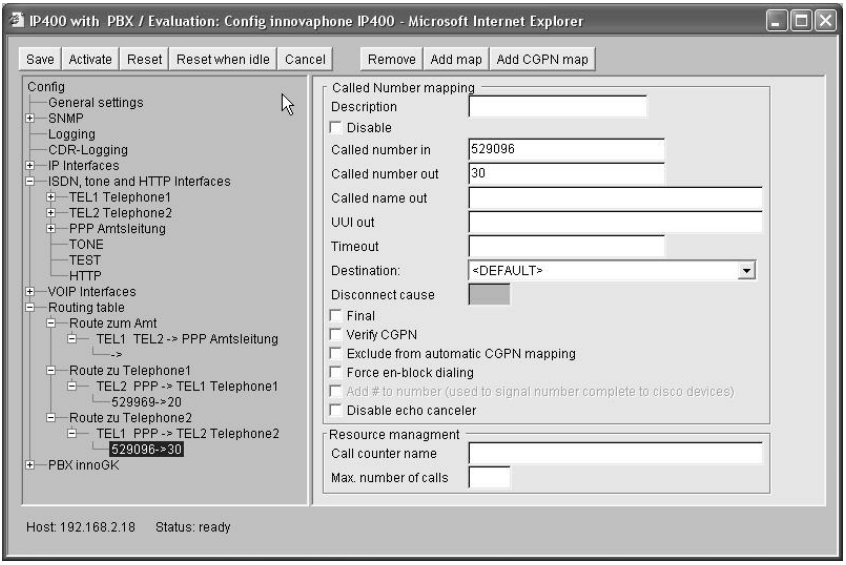

Fig. 25 Routes with call number replacement

After all, it is occasionally necessary to define routes that depend on the calling number. To do this, so called **CGPN Maps** are attached to the **Maps**, very much in the same way as the **Maps** that are attached to the routes. This not only allows the calling numbers to be modified in order, for example, to suppress the extension for outgoing calls, but also the entire **Map** to be made dependent on the calling number.

Fig. 26 on page 91 shows the configuration from Fig. 25 on page 90, altered in such a way that access to the public exchange line is available only for the telephone with number `20` and, contrary to the incoming mapping, the call number `529096` is transmitted for outgoing calls.

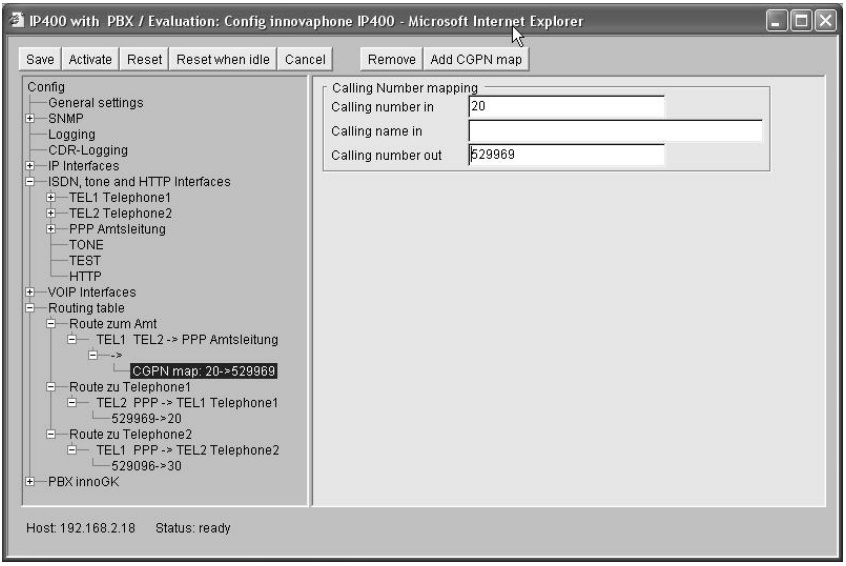

Fig. 26 Dependence on the calling number

Call switching is controlled by the gateway's **Routing Table** (in the **Routing table** area).

The routing table is searched through from top down for every single call. If a **Map** is found,

- whose route has specified the source interface of the current call as a permitted interface in the **Enable calls from interfaces** list and
- whose dial prefix specified in the **Called number in** field matches the called number of the current call, and

  whose **Verify CGPN** box is not checked
  or
  whose **Verify CGPN** box is checked and the calling number of the current call matches the **Calling number in** entry, **CGPN maps** attached to **Map**.

then, the current call will be switched to the interface specified in the **Default call destination** field in the route of the **map** or in the **Destination** field of the **Map**.

In the process, the called number is modified in such a way that the dial prefix in the **Called number in** field is replaced by the sequence of digits in the **Called number out** field. The calling number is modified accordingly using the **Calling**

number in and **Calling number out** fields if the map entry used has a CGPN map entry whose **Calling number in** field matches the dial prefix of the calling number of the current call.

If it is not possible to switch the call to the identified interface however, the routing table is searched for the next **Map** entry that meets the requirements specified above.

Tip

If no suitable **Map** entry is found in the routing table, the call is invalid and is not put through. In this way you can prevent, for example, an exchange line being accessed from certain sources, resulting in costs.

7.2 Configuration of the routes

The routing table is configured in the **Routing table** area of the configuration applet.

The following steps are used to define a new route:

- Click on the **Add route** button, to add a further entry to the routing table. Note the order of the routes here. The new route is always inserted after the current entry.
- Enter a name for the route in the **Description** field. This will help you maintain an overview later on.
- Select the entry beneath the new route (the one with "**->**")
- In the **Default call destination** list, choose the destination to which the calls are to be connected.
- Check the boxes of the gateways and ISDN- interfaces in the **Enable calls from interfaces** area, to mark them as valid sources for this route. You will only be offered the interfaces, which have been configured.
- Click on the **Add map** button.
- In the **Called number in** field, enter the dial prefix the route shall be valid for.

- Enter the replacement for the dial prefix that you specified in the **Called number in** field in the **Called number out** field. Simply copy the dial prefix into this field if the call number is to be adopted unchanged.
- Add an "!" to the number if a route is to apply to a certain number and all of the digits subsequently dialled are to be ignored.
- If manufacturer-specific data is to be transmitted in the signalling channel, e. g. the URL for an announcement, this URL (e.g. "http://www. ...") can be entered in the **UUI out** field.
- A # can be transmitted to mark the end of the call number by setting the **Add # to number** option. This is required for devices, such as from Cisco, which are unable to identify the end of a number properly.

You can actuate the **Add map** button a number of times if you want to specify a number of routes for a set of sources.

Fig. 27 on page 93 shows an example. In this example, two MSNs (529096 and 529294) are connected at an ISDN interface and mapped there onto the MSNs (30 and 31) set in the telephones. Both call numbers, with replacements, are configured as **Map** to a route.

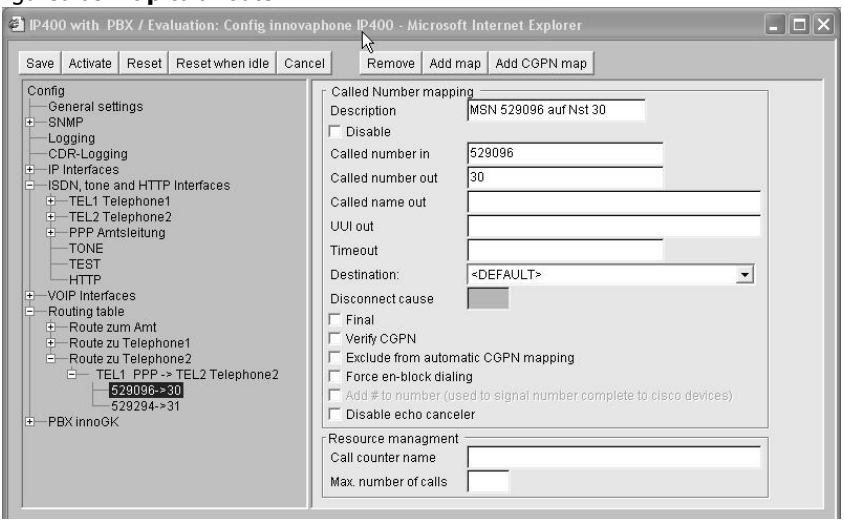

Fig. 27 Routes with multiple maps

- If, by way of exception, the route for a **Map** entry is to be configured with a different destination than that specified in the route's **Default call destination** field, you can select this from the **Destination** field of the **Map**.
- 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.

7.2.1 Manipulation of the calling number (CLI)

When switching calls, it may be necessary to manipulate the calling number, for example to ensure a correct callback.

Fig. 28 on page 94 shows the configuration of a `0` as the access digit for an exchange line.

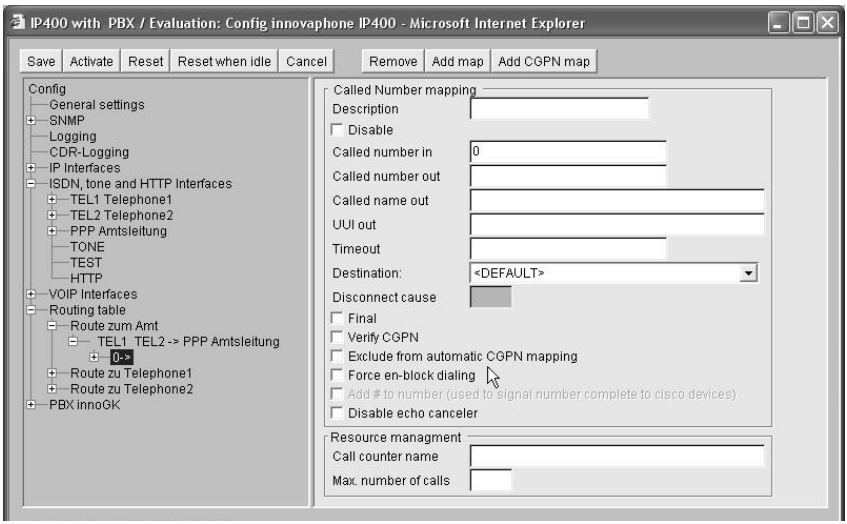

Fig. 28 Configuration of an exchange access code

To ensure here that an exchange access digit of `0` is placed in front of the calling number for all incoming calls via the exchange line, a **CGPN** (**calling party number**) map must be created for the respective interface.

The basic procedure for this is described in section 5.2.7 "Dealing with the various ISDN address types" from page 62.

Fig. 29 on page 95 shows how an additional `0` can be added as exchange access

code on the PPP interface.

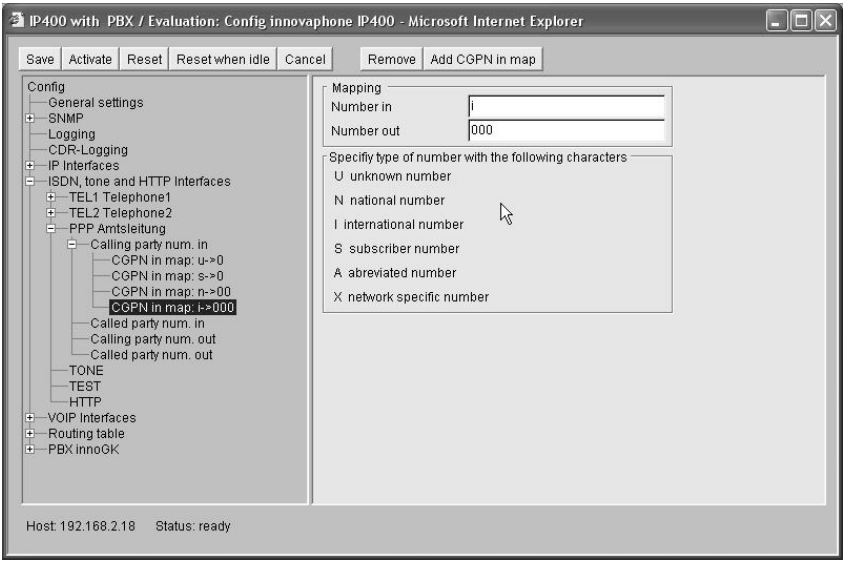

Fig. 29 Manual insertion of an exchange access code

7.2.2 Automatic correction of all calling numbers

With complex routing tables, manual correction as described above can be very laborious and error prone. It is thus possible to automatically have all calling numbers correctly set. To do this, you merely have to to check the **Automatic CGPN mapping** box in the **Routing table** area.

The modifications to the calling numbers are produced by analysing the routing table. Here a route is searched for, that would enable callback to the current call. The number replacements for this route would then be used in reverse order. This automatic correction of the calling numbers is made according to the CGPN maps specified for ISDN interfaces or gateways, if available.

Check the relevant **Exclude from automatic CGPN mapping** box if you want certain routes to be excluded from this process.

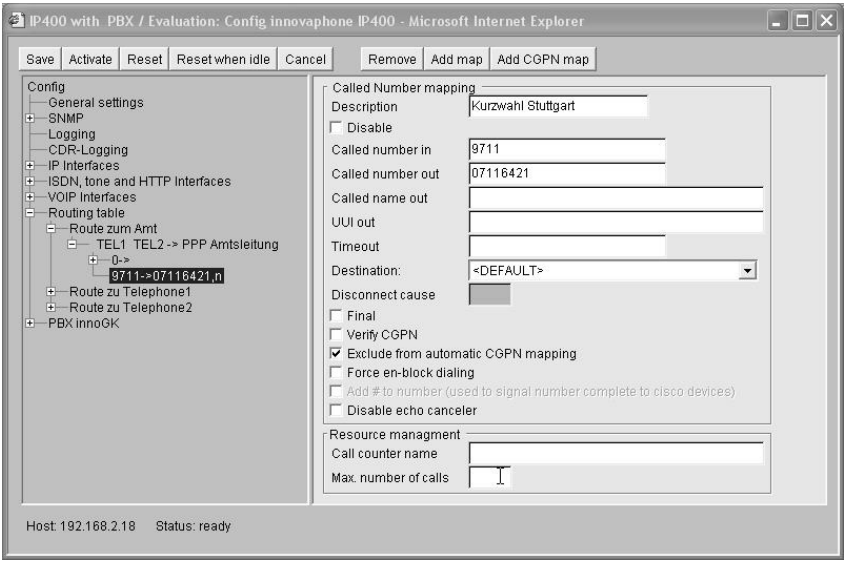

Fig. 30 Exclusion from **automatic CGPN mapping**

Fig. 30 on page 96 shows two abbreviated dialling routes which are to be excluded from any involvement in the modification of the calling number. Otherwise calls from the Berlin branch beginning with `930` instead of `0030926` would be displayed, which could be confusing to the users.

7.2.3 Selective routes depending on the calling number

In certain cases it can be useful to restrict individual routes to particular calling numbers. In this way, access to a chargeable exchange line, for example, can be restricted to certain extensions (**selective class of service**).

Proceed here as follows:

- In the routing table, mark the entry that you want to restrict.
- Check the **Verify CGPN** box.
- 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. In this case it does not make any sense to make no entries.
- Under **Calling number out** enter the sequence of digits that is to replace

the prefix entered above. It usually does not make any sense to make any replacements here. The same sequence of digits is then specified as under **Calling number in**.

- Leave the remaining fields empty.

I you have set automatic correction of all calling numbers (see section 7.2.2 "Automatic correction of all calling numbers" from page 95) the check applies to numbers already corrected.

Fig. 26 on page 91 shows such a configuration.

If you delete the **CGPN Mappings**, make absolutely certain that you deactivate the **Verify CGPN** checkbox, since otherwise no calling number at all would be allowed, making the **Map** ineffective.

7.2.4 Changing the calling party number for specific routes

In some case it can be useful to modify the calling party numbers for calls routed with the aid of specific **Maps**. Proceed here in accordance with the relevant descriptions under section 7.2.1 "Manipulation of the calling number (CLI)" from page 94.

Make certain in this case that the **Verify CGPN** checkbox is not activated. Note also that, during the execution of a route, the interpretation of calling numbers is always independent of the type of address (see section 5.2.7 "Dealing with the various ISDN address types" from page 62), with the effect that no address types can be specified here.

7.2.5 Defining call number replacements

It often makes sense to replace dial prefixes generally and independent of individual routes, for instance to implement abbreviated dialling. Here the abbreviated dialling number is replaced by the complete number and then routing is performed again for the now complete number.

This can be achieved by defining a route to the destination **MAP** in the **Default call destination** field. After the number replacement, the call is not connected in the usual way but a suitable **Map** is searched for in the routing table with the replaced call number.

Please note that, in order to avoid endless replacement operations, only those routes after the MAP route (text-wise) are searched through. MAP routes must thus always be specified before the routes that define the treatment of the replaced number.

7.2.6 Configuration of multiple routes for a dial prefix

You can specify different routes for different call sources for the same dial prefix, with the effect that the routing process is dependent on the call source and not only on the called number.

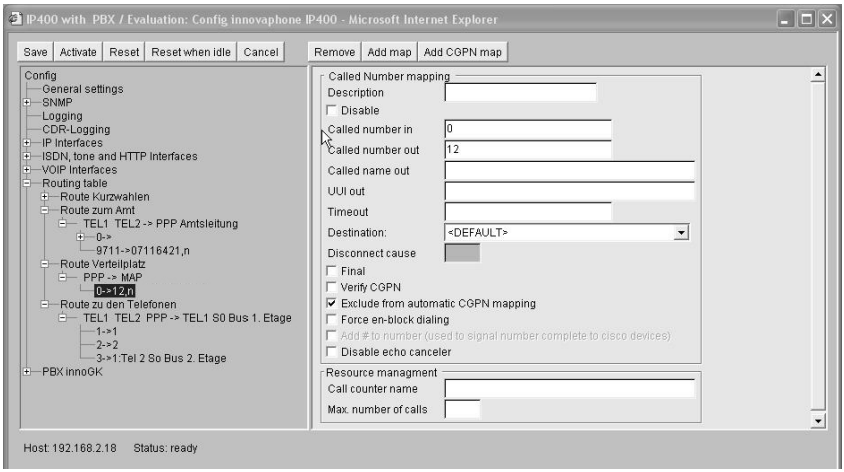

Fig. 31 Different ways of call routing depending on the calling interface

Fig. 31 on page 98 shows an example of such a configuration. Here the call number `0` is switched to number `12` (switchboard position) for calls from the exchange line, but to the exchange line for all other calls.

7.2.7 Call forwarding

It can make sense to define several routes for calls from the same call source with the same dial prefix.

The gateway's routing process always uses the first suitable route. If a connection cannot be established using this route however, a further attempt can be made using another route. Various types of call forwarding can be implemented in this way.

- If an attempt is made to switch a call using a route and this call is unable to be set up due to missing local resources (e.g. no exchange line available, see Table 14 on page 100), a search will immediately be made for a further route. If several exchange lines are connected to the gateway for example, this allows the calls to be distributed successively around the exchange lines

(Fig. 32 on page 99 shows such a configuration)

- If a route is used to make an attempt to switch a call and the call can be successfully signalled to the called terminal (terminal responds with an **Alerting** message) and if a value greater than `0` has been entered in the **Timeout** field for this route, then a search will be made for a further route, if the call is not accepted within the specified number of seconds. This corresponds to the "Call forwarding no response (**CFNR**)" function. If you enter a **Timeout** of more than 120 seconds, this timeout will have no effect since the global timeout for setting up the call will expire first. Since, if timeout is entered, available alternative routes will always be tried, after a failed call, it has the same effect as the "Call forwarding busy" (**CFB**) function.

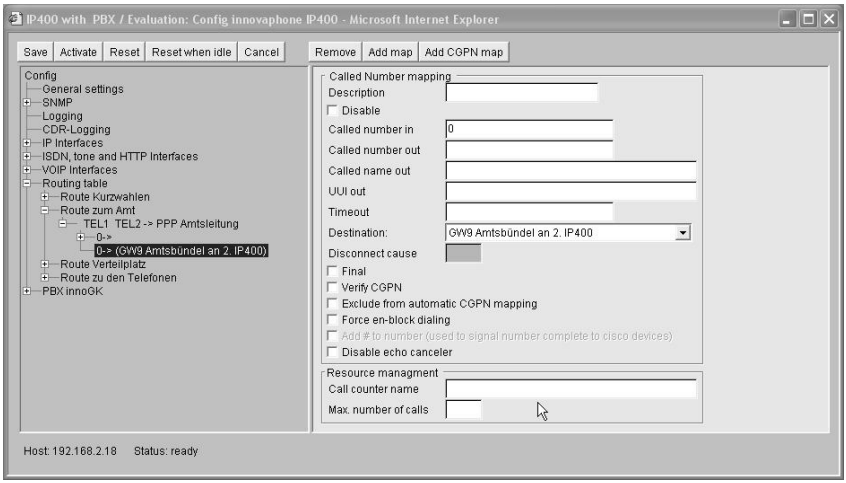

Fig. 32 Configuration of an exchange line bundle

Check the **Final** box in the **Map** entry if, after attempting to switch a call using a map entry, you want to prevent further routes from being tried out.

You can likewise check the **Final** box in the **Map** entries for a route with destination `MAP` . In this case, no further `MAP` entries will be evaluated but a search will still be made for other appropriate routes.

Error code (decimal)	Description
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable

Table 14 "Local problems" concerning call forwarding

7.2.8 Call sequences

Routes with the call destination `TRY` are a special case. If this type of route is used to switch calls, the call number is first replaced and the result is then used to search for normal routes. If the call can't be successfully switched in this way a further `TRY` route is subsequently searched for.

If a timeout is specified for the `TRY` route, it takes effect on the routes used to try to switch the call.

No further searches for `TRY` routes are made, if the **Final** box is checked in the **Map** entry.

Fig. 33 on page 101 shows the configuration of a switchboard, which can be accessed by the exchange line via the extension number `0` and is tried out internally for the extensions `12`, `13` and `22` in succession.

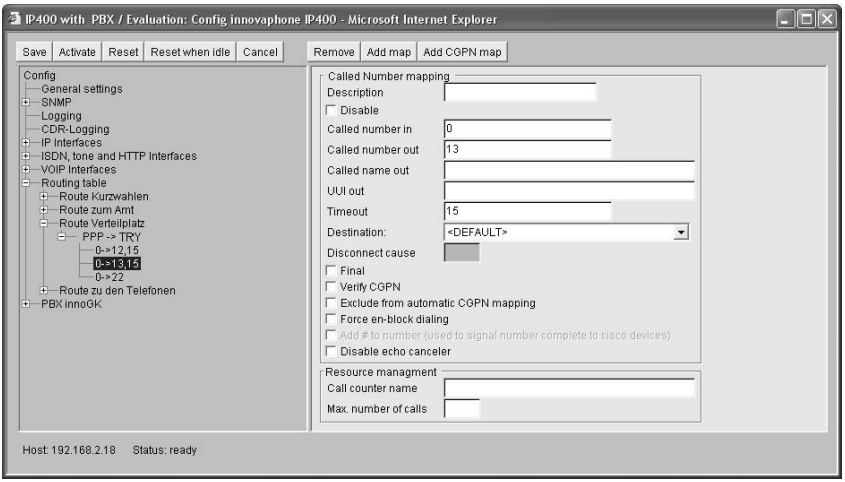

Fig. 33 Call sequences with `TRY` routes

7.2.9 Rejecting calls

Every time a call is routed, your gateway will try to find routes with suitable **Maps** and to switch the call accordingly. If no suitable **Map** entry is found in the routing table or if all call attempts fail, the call will finally be rejected.

Sometimes though, it is useful to explicitly reject certain calls by making an entry in the routing table. This can be done by setting up a route with **DISC** as the call destination. The reason for rejection can then be specified in the **Disconnect cause** field.

Fig. 34 on page 102 shows a configuration in which the exchange access code is configured in such a way to make it impossible to call certain call numbers.

A list of the defined reasons for rejecting calls can be found in Table 23 starting on page 151. The value specified in the "Error value (decimal)" column must be used.

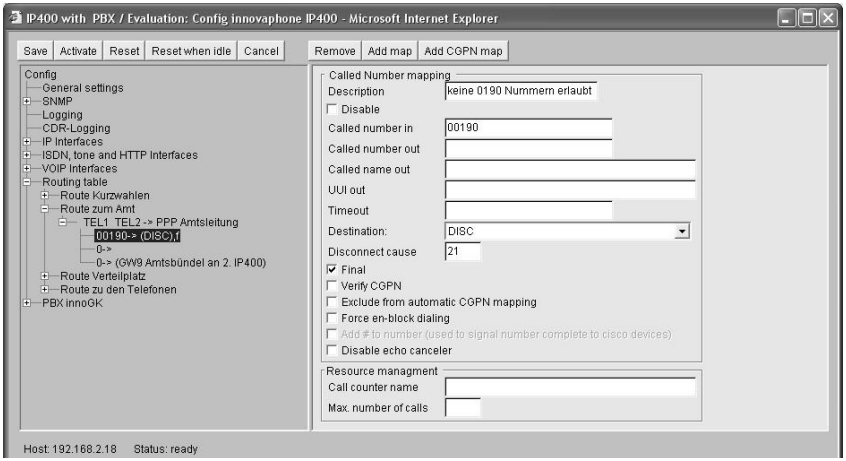

Fig. 34 Rejecting calls

7.2.10 Enforcing en-bloc dialling

Since your gateway supports continuous digit-by-digit suffix dialling, no specific dial digit is required to complete the dialled number. This behaviour resembles that of customary PBXs.

So called **Overlapped sending** is however not supported by all H.323-compatible devices. When a call is set up to such a gateway, it will not able to process the suffix dial code and the call will fail.

In such a case, a hash (#) can be added to the dial prefix for a route. In this case, the gateway waits until the user has dialled a hash before setting up the call to the remote gateway. The hash itself and any digits subsequently dialled are not transmitted to the remote gateway.

If there is always a fixed number of digits required to complete the call number for this route (e.g. always 3-digit extensions), a corresponding number of full-stops (.) can be added to the dial prefix. The gateway expects a digit to follow each full-stop and then carries out the call without a hash having to be dialled. Any digits subsequently dialled are not transmitted to the remote gateway.

The **Force en-bloc dialling** checkbox can also be ticked in the appropriate **map** entry if the number of digits required to complete the call is not constant for this route and if dialling is not to be explicitly completed with a hash. If such a map entry takes effect, the gateway collects the digits subsequently dialled until more

than 4 seconds have elapsed since the last digit was dialled. The call is then switched and any digits subsequently dialled are ignored.

7.2.11 Routes from and to fax machines

With version 2 of your gateway's firmware it was possible to assign certain map entries to fax connections. This made it possible to force the usage of the appropriate G.726 encoder for the transmission of Group 3 faxes.

This function (**Fax** (**force G726 40 Kbit/s coder**)) is no longer available from version 3 of the firmware onwards, since faxes can be reliably transmitted using the T.38 protocol (see section 6.1.4 "H.323 protocol options" from page 73).

If you update a version 2 configuration to version 3 or higher, you merely need to check the **Enable T.38 fax protocol** box in the relevant gateway definitions in the **VoIP Interfaces** area.

7.2.12 Suppressing echo compensation

Your gateway implements **echo cancellation** for all voice connections that terminate on a local ISDN interface. Echo compensation is automatically not carried out for data and fax connections. In rare cases though, in may be that no echo compensation is to be performed even though a connection is treated as a voice connection. This can be the case, for example, with modem connections.

You can suppress echo compensation by checking the **Disable echo canceler** box in the relevant **Map** entry.

7.2.13 Resources management

The maximum number of permitted calls for a route can be limited, using resource management, if there are only limited resources for a route, e.g. due to the bandwidth of the data connection being too small.

Resource management is configured via the configuration applet in the **Resource Management** field of the map of the respective route.

A **call counter name** can be entered here and the maximum number of calls permitted for this route can be defined in the **Max. number of calls** field.

The system checks the number of calls taking this route and rejects calls exceeding the specified number of calls. If another route is set up to this destination, this will then be used.

The number of current calls for the respective name of the call number counter can be displayed in the **Call counts** area on the user interface of the gateway (see section 9.2.4 "Call Counter submenu" from page 127).

7.3 Call routing depending on device management

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

7.3.1 Calls to and from gateway groups

Section section 6.3 "Static management of VoIP devices" from page 84 describes how the gateway becomes aware of groups of VoIP devices.

In principle, routes to such groups are configured in the same way as normal routes. The dial prefix defined for the route is regarded as matching the called number if the number matches the dial prefix completely ***and*** all of the missing digits required to complete the IP address of the destination device have been dialled. Superfluous digits subsequently dialled are passed on to the destination device, if appropriate.

Size of the host share in bits	Number 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)

Table 15 Digits required to complete the address

3, 6, 9 or 12 digits are required to complete the IP address. This depends on the size of the host share in accordance with the subnet mask specified in the **VoIP Interfaces** definition. The individual digits are converted to bytes of the address in groups of three digits.

Table 15 on Page 105 shows the number of digits required. Complete bytes of the address have to be dialled in groups of three, even if less than 8 bits are required, according to the subnet mask configured. Leading zeroes must also be dialled.

Assuming there is a group of VoIP devices defined by the network address `195.226.104.128` and the subnet mask is `255.255.255.128`. The addresses `195.226.104.129` to `195.226.104.254` are thus accessible. The dial prefix for the route to this group has been configured with `91`. To call the device with the address `195.226.104.135`, the number `91135` has to be dialled.

If "Automatic correction of all calling numbers" (see section 7.2.2 "Automatic correction of all calling numbers" from page 95) 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 placed in front of the calling number. As a result, callback is possible via the supplied number.

7.3.2 Calls to and from devices managed by RAS

Calls can be routed to a device registered with the gatekeeper by means of the RAS protocol (see section 6.2 "Management of VoIP devices via RAS (Gatekeeper)" from page 81) using the call number or name. Here, calls to gateways are treated somewhat differently than calls to terminals (see page 67).

In principle, calls are switched to a VoIP device managed by means of the RAS protocol in a normal manner (refer to section 7.1 "General considerations on the

configuration of call routing" from page 87).

If a **Map** entry of a route is found which matches the called number and if this entry or the route has a **VoIP Interfaces** definition as destination which is configured as **Gatekeeper client group**, all aliases are searched through in this gateway for an entry with an **E.164 Address** that matches the called number. If such an entry is found and the corresponding device is currently registered with the gatekeeper, the call is switched there. Otherwise the search for suitable aliases is resumed. If there are no suitable entries or the client is not registered at the time of the call, the call will fail and an alternative route, if available, will be used (refer to section 7.2.7 "Call forwarding" from page 98).

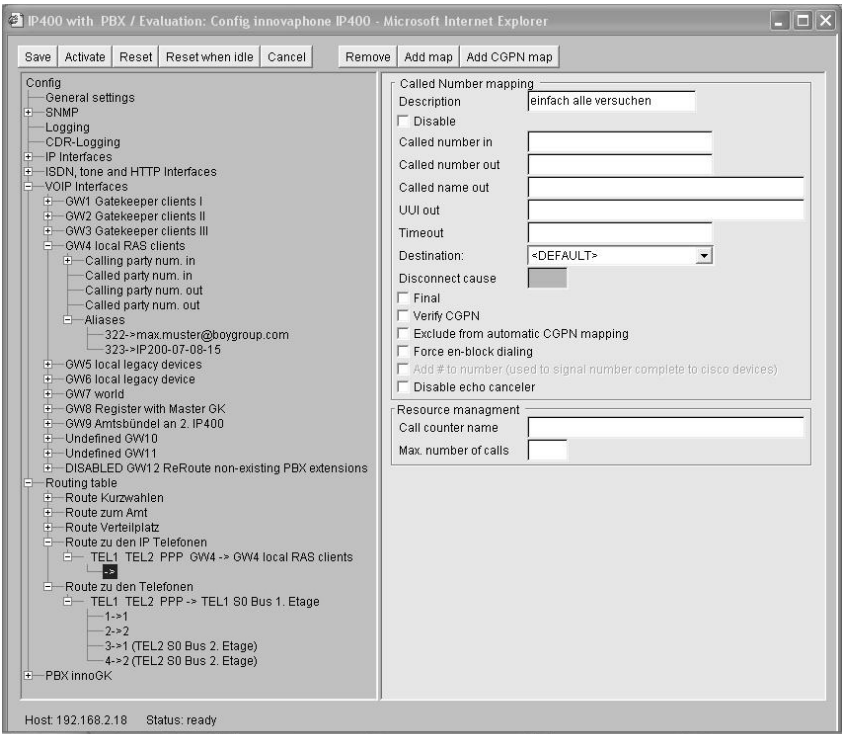

Fig. 35 Routes for terminals registered by RAS

Due to this procedure, the called number of a call being switched will be checked twice. The first time when searching for a route appropriate for the call, and the second time when searching for an appropriate alias within the **VoIP Interfaces** definition. It is therefore possible, and normal, to configure routes of this kind very simply using empty **Map** entries. This means that at first there will be an attempt to switch all calls to the devices registered by means of RAS. However this will fail, silently, if no device is registered with the correct number.

Fig. 35 on page 106 shows such a configuration. In this example, two IP telephones with extensions `22` and `36` are configured as devices registered by RAS in the **VoIP Interfaces** definition **GW2**. The remaining range of numbers from `10` to `49` is distributed between two ISDN S_0 busses.

As opposed to VoIP terminals, which are registered with the gatekeeper with name and number, no number is usually entered for VoIP gateways. This would also not make sense, since the gateways implement an entire number range and not an individual number. With that, determining the call destination using the called number, as described further above, won't work.

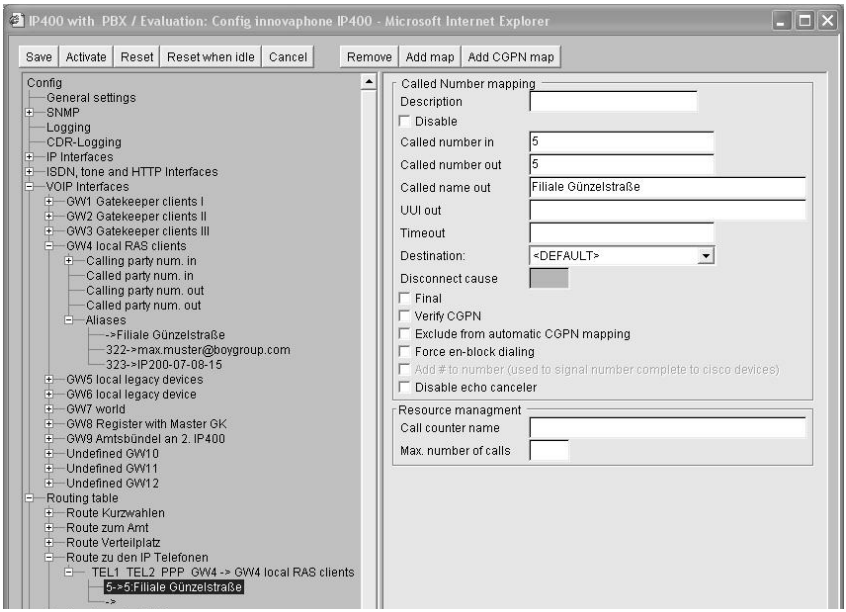

Fig. 36 Routes to gateways registered via RAS

The gateway specification **GWxx** is insufficient to identify the destination of a call, if gateways have been registered in a **VoIP Interfaces** definition and a route is supposed to switch a call there. It is thus necessary here to also enter the correct H.323 name in the **Map** as **Called name out**.

Fig. 36 on page 107 further above shows a configuration in which the call numbering plan - from 10 to 49 refers to two ISDN S_0 busses, from 50 to 59 to a branch connected by the VoIP gateway and otherwise to IP-telephones.

7.3.3 Calls to gatekeeper clients via H.323 name

Dialling call numbers is only one way of addressing destinations within the VoIP environment. Another convenient way is to specify a name as the call destination.

If a call arrives at the gatekeeper with an **H.323 name** but without an E.164 address (i.e. without a phone number), the number belonging to the ID is determined first by searching through all of the **VoIP Interfaces** definitions of the type **gatekeeper client group** for an alias entry with the corresponding **H.323 name**. The **E.164 address** of the first matching entry is then used to further switch the call in the same way as if the call had arrived right from the start with this number as the called number.

7.3.4 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 make calls based on names using terminals unable to call H.323 names (e.g. ISDN telephones).

To do this, enter the H.323 names as **Called name out** for the normal routes.

This procedure only makes sense if the VoIP terminal is not registered directly at your gateway as gatekeeper, since otherwise the normal methods would of course be adequate.

7.4 Configuration of the PBX components in the gateway

By calling up the **DISABLED PBX** menu and setting the **ENABLE PBX** option, the menu item **DISABLED PBX** will be changed to **PBX** and the submenus **LDAP server**, **LDAP replication** and **Licenses** can be configured.

The LDAP protocol is required for redundant systems in which the server and a replicating client access a joint user database.

To configure the **PBX** menu - particularly when setting up and administering licences - please note the advice given in "Administrator´s Manual - innovaphone PBX".

8 Definition of various operating parameters

8.1 General settings

General parameters can be set in the **General settings** area of the configuration applet.

8.1.1 Defining the gateway name

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

8.1.2 Defining the user administrator and -password

You can define the user's name and the corresponding password, which secures the gateway's configuration, in the **Change login parameters** area.

The validity of the newly defined password is checked when saving or activating the configuration. Like any other changes to the configuration, a change to the password must be activated and saved as described in section 3.2 "Checking and saving the configuration" from page 22.

8.1.3 Defining the source for time and date

Your gateway does not have a battery-backed real-time clock. The internal time will thus be reset to 0:00 hrs, 1.1.1970 after every restart.

The correct time is not required for normal operation. However, if this is important to you, to get, for example **call detail records** with the correct time, you can specify the IP address of a source for time and date in the **Get time from SNTP Server** area. Your gateway will then synchronise its internal clock to the time source at intervals specified under **Update interval**.

You can use a public server if your network does not have an NTP server. The TU Berlin, for example, provides a time service under the IP address `130.149.17.21`. Bear in mind that it is a voluntary service and no claims can be made with regard to its availability.

Tip

Bear in mind that every Windows 2000 server can work as an SNTP server. Equally, there are freely available SNTP software packages for Windows and Unix/Linux platforms.

Your gateway also operates at the same time as an NTP server. If you are operating additional IP 400 gateways or IP 200 telephones, you can synchronise one of them with a time server (external if required) and then in turn synchronise the other ones with it.

Tip

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

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

If you are operating other devices in your network that require a time server (for example further gateways or IP telephones), please enter the IP address of your IP 400 there. Your gateway will then operate as the time service and signal the correct time to the other devices. Avoid synchronising all devices with one external time service, since this results in unnecessary high loads on these servers.

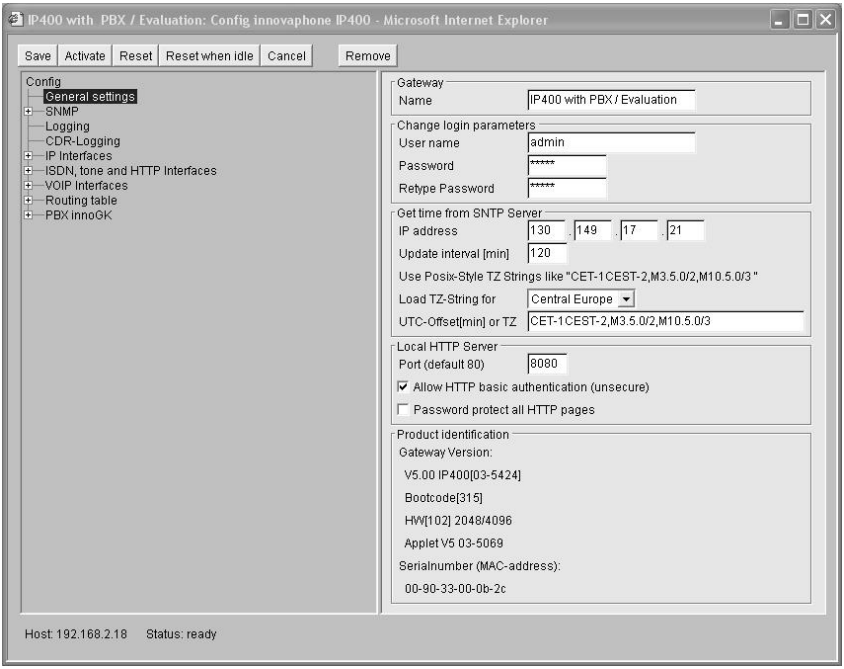

Fig. 37 The "general settings"

Time services always provide the coordinated world time (**U**niversal **T**ime **C**oordinated [UTC] which corresponds to **G**reenwich **M**ean **T**ime [GMT]), not however the correct time zones and summer time. You can therefore specify the time difference between your time zone and the universal time in the **UTC Offset**[**min**] **orTZ** field. The difference from the time zone `GMT+1` (Central European time zone) is 60 minutes. A further 60 minutes has to be added with summer time, adding up to a total difference of 120 minutes. In this case however, you must adjust the time difference manually when switching from winter to summer time and vice versa.

This setting can be automatically made by the device if you specify the **TZ string** (**T**ime **Z**one) in the **UTC Offset**[**min**] **or TZ** field. The name of the time zone, the name of the summer time zone, their respective differences in time compared to the **UTC** and the time switch points are encoded in this value.

Since the values are somewhat complicated, the configuration applet provides

help editing to make correct entries for Central Europe and Great Britain:

- If you select the value `Central Europe` in the **Load TZ-String for** field, then the **TZ string** will be entered in the **UTC Offset[min] or TZ** field for the Central European time zone.
- If you select the value UK from the Load TZ-String field, then the **TZ string** for the British time zone will be entered into the **UTC Offset**[**min**] **or TZ** field.
- If you select the value UK from the **Load TZ-String for** field then the **TZ-string** will be deleted and you will be able to enter any value of your choice. There are various formats that are defined by the IEEE POSIX standard.

innovaphone equipment can access the POSIX time zone using DHCP. For further information on the DHCP-Client and POSIX TZ see Appendix D: "The innovaphone DHCP Client" from page 152.

Tip

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

For most practical purposes however, the following description is sufficient (based on a translation from the FAQ list of the Linux Samba package):
Posix TZ strings have the following form (optional parts in square brackets):

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

- ***Std*** stands for the time zone (e.g. `CET` or `MEZ` for **Central European Time**).
- ***Offset*** specifies the time difference between the time zone and **UTC**, e.g. `-1` for Central European time. The difference is negative if the time zone is ahead of UTC, therefore `-1` for Central European time. If the time difference does not only include full hours, the number of minutes can be added, for example `-1:30`.

  The TZ string ends here, if you are not using summer time.

- *Dst* stands for the summer time zone (e.g. CEST or MES for **Central European summer time**).
- The optional, second *Offset* gives the offset of the summer time with respect to UTC. An hour before normal time is assumed if no entry is made.
- *Date*/*Time*,*Date*/*Time* define the beginning and end of summer time. The format for a point of time is M*m*.*n*.*d*, which means day *d* in week *n* in month *m*. Day 0 is Sunday. If the fifth week is entered, the last day (with respect to *d*) of the month is referred to. The format of the time entry is *hh*[:*mm*[:*ss*]], in 24-hour format.

The Central European time zone, which applies to Germany, is specified as follows:

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

Fig. 37 on page 112 shows the configuration of an SNTP server which is queried every two hours. The gateway interprets the time in the Central European time zone.

8.1.4 Defining the port for the local HTTP server

Your gateway is administered via the network via the TCP port 80 (http). If for some reason the port 80 is not supposed to be used, you can set up another port in the **Local HTTP Server Port** field of the basic settings page **General settings**. You can then access your gateway via this port.

For web administration via the browser, you must specify the link, for example for port 8080 as follows: http://192.168.0.3:8080. Note that all applications such as the **innovaphone PBX Operator** switchboard position and the **TAPI** need to be set to the port of the HTTP server.

8.2 Monitoring the gateway via SNMP

You can use the gateway to monitor the operating condition via SNMP. The standard MIB-II is supported, along with a manufacturer-specific MIB. For details about this MIB, consult your dealer or download the MIB file from the download area of the innovaphone web site (http://www.innovaphone.com).

To access the gateway using SNMP, proceed as follows:

- Open the **SNMP** field of the configuration applet.
- Make sure that the **Access** parameter is set either to read-only or to

`read-write`. If `read-write` is set, certain MIB variables can also be written.

- Enter the name in the **Community** field if you are not using the standard **Community Name** `public`.
- The entries **Name**, **Contact** and **Location** are for information only and therefore optional.

The gateway can now be monitored via SNMP.

Additional destinations for trap messages must be defined if the gateway is to trigger the traps defined in the manufacturer-specific innovaphone MIB.

- Select the **Trap Dest** area.
- Use the **Add trap dest** button to add a new destination. You can define a maximum of five destinations.

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

- Select the **Accepted Hosts** field.
- Use the **Add Host** button to add the IP address of an authorised computer. You can define a maximum of five authorised computers.

Access via SNMP is only possible if the correct **Community Name** is entered. If you have ticked **Authentication Trap** in the **SNMP** field, a trap will be generated in the event of access with an incorrect **Community Name**.

8.3 Defining the syslog parameters

Your gateway can record significant events, occurring during operation, in a system log.

The type of events which can be recorded can be configured in the **Log sources** field in the **Logging** area of the configuration applet as follows:

Setting	Description
Log TCP	All TCP connection set-ups in the H.225 / H.245 protocol are recorded.
Log PPP	All PPP connection activity is recorded.
Log calls	All call switching operations are recorded.
Log RAS messages	The gatekeeper information is recorded in terms of H.323 terminals logging on and off.

Setting	Description
Log gateway routing	The individual call switching steps for processing the routing table are recorded.
Log configuration changes	All changes to the configuration are logged.

Table 16

The current syslog entries can be checked on the web interface at any time via the **Log** link as illustrated by Fig. 38 on page 116.

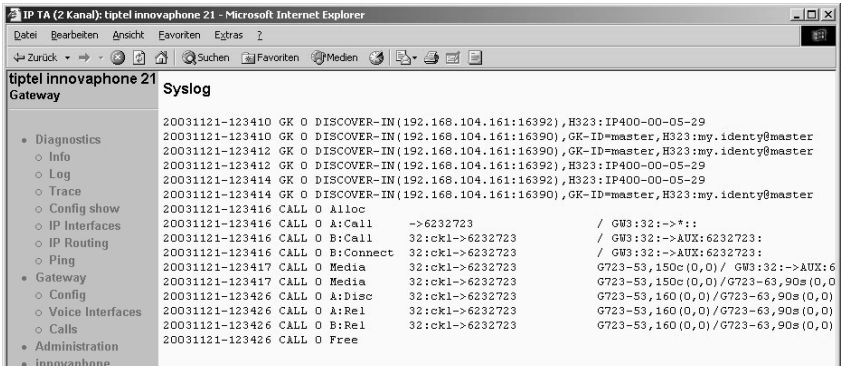

Fig. 38 The syslog entries on the web interface

Syslog entries are only displayed if a web browser displays the **Log** page. Otherwise they will be lost.

There are three ways of saving the syslog permanently.

- Storing the Syslog entries in a `syslogd`.

  In this case, the entries are reported to a `syslogd` server in the network, which is then responsible for their further evaluation or storage.

  - 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**.

- Storing of Syslog entries in a Web server.

  In this case the syslog entries are transferred to a web server where they can be further processed. Each individual 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 form programme on your web server under **URL-Path**.

Tip

Your gateway will make an HTTP GET request to the web server on the registered URL followed by the URL-encoded log entry. Enter the value `/cdr/cdrwrite.asp` in the **URL-Path** field 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. Your gateway will then make a `GET /cdr/cdrwrite.asp?event=syslog&msg=`***`logmsg`*** request to the server.

- Transferring the Syslog entries to a TCP programme.
  Here, the gateway writes the Syslog entries to a TCP connection. The other end of the TCP link is then responsible for further evaluating the entries.

  - Select `RAW-TCP` as **Syslog mode**.
  - Enter the TCP port number of the connection under **TCP port number** in the **Raw TCP parameter** area.
  - If the gateway is to establish the TCP connection automatically, enter the IP address of the destination under **Address**.
  - If the gateway is to wait, for an incoming TCP connection, enter the IP address from which the connection comes, under **Address** and check **Wait for incoming connections**.

8.4 Transmission of call detail records (CDR)

The gateway can transmit detailed information on every single call made. This

information is available in the call detail records and can be evaluated with the appropriate software.

There are 2 ways of transmitting CDR data, which can be selected in the configuration applet under **CDR0-Logging** and **CDR1-Logging**. In this way, the same data can, for instance, be sent to the administrator via **SYSLOG** and, for instance, to the book-keeping department via **HTTP**.

Log files can be transmitted using the **SYSLOG**, **RAW TCP** and **HTTP** protocols. Selecting **off** deactivates the transmission of Call Data Records.

Depending on the protocol chosen, the associated parameters such as the server's IP address, etc. must be entered.

If **Send only billing CDR´s** is active, in the **CDR Format** area, then only one Call Data Record will be transmitted, at the end of an outgoing call, over the telephone network. In this way, only outgoing, external calls, which will be billed, are recorded.

For further information please refer to the description on the download area of the innovaphone web site or get in touch with your dealer.

9 Administration via the Web Browser user interface

Administration via the web browser allows you to:

- Monitor the status of the device (**Diagnostics** area).
- Configure the gateway and the gatekeeper (**Gateway** area).
- Save the configuration and load and activate up-to-date firmware (**Administration** area).
- Configure and monitor the optional innovaphone PBX components, if installed (**PBX pbx** area).

To use the administration user interface properly, your web browser has to meet the following requirements:

- HTTP 1.1 protocol
- HTML 4.0 protocol
- Frames
- Java applets
- XML/XSL (XML/XSL is only required for advanced functions such as sorting lists. The gateways can be fully configured and administered however without these functions.)

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

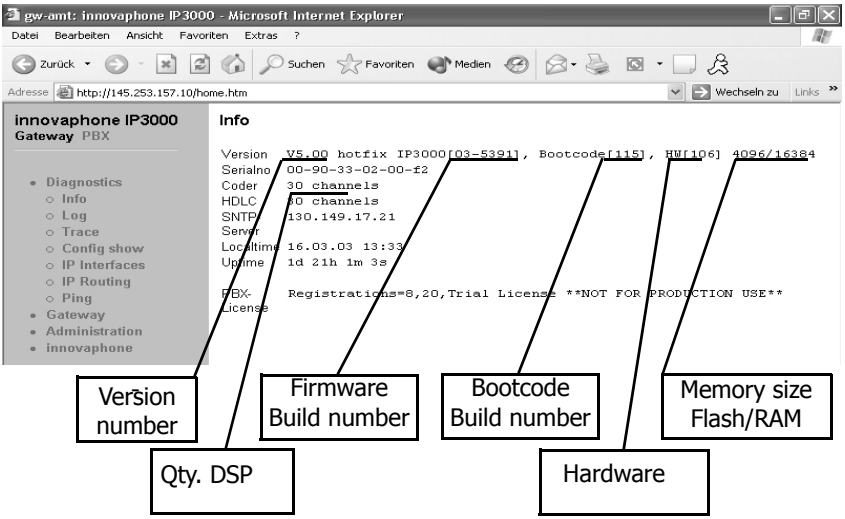

Fig. 39 The browser administration user interface

The welcome page will appear, once you have connected your web browser to the IP address of your gateway. The **URL** is

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

with ***xxx.xxx.xxx.xxx*** replaced by the IP address of the gateway.

The hyperlinks within the upper frame of the browser window can be used to navigate throughout the various functional areas.

Some areas require you to enter the administrator's user ID and password (see page 120).

9.1 Diagnostics menu

9.1.1 Info submenu

The home page of your gateway (see Fig. 39 on page 120) displays information on

- The device's hardware and software versions
- The serial number
- The number of voice channels

- The innovaphone PBX 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 or warm restart

9.1.2 Log submenu

In this area you can view your gateway's log messages directly, while it is in operation. The messages are constantly automatically updated and are scrolled upwards, out of the window.

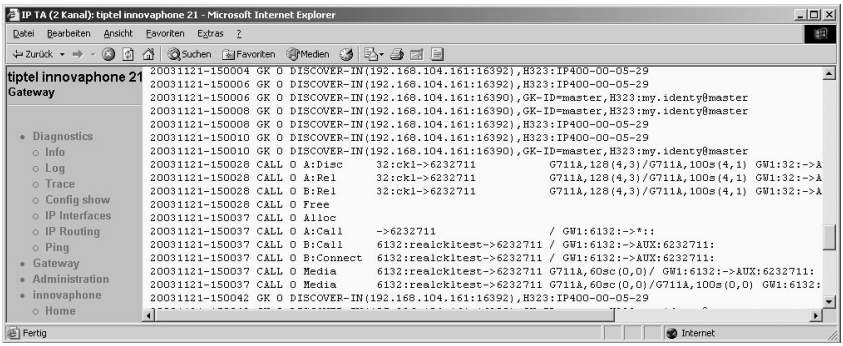

Fig. 40 Displaying the log messages with the web browser

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**.

9.1.3 Trace submenu

This area allows you to download trace files from your gateway. You can save the trace in files in the same way as described in section 9.1.4 "Config show submenu" from page 122.

Please note that the trace information grows constantly. To obtain a continuous trace, the page must be regularly updated. Depending on the browser's settings, this can be done simply by clicking on the **Trace** link again or by updating the frame in the context menu. To do this, use the right mouse button to click in the browser window and select **Update** from the context menu.

9.1.4 Config show submenu

The **Config show** menu can be used to display the current configuration of your gateway in text.

Depending on the browser in use, you can also save the current configuration in a file using the **Save target as...** function. You can also mark the entire text (Ctrl-A) and copy it into the clipboard using the right mouse button via the context menu. You can now paste the configuration into any text editor and save it there.

A configuration saved in this way can be reloaded either partly or fully using the **Config update** link (refer to section 9.3.3 "Config update submenu" from page 132). In this way, you can save and restore configurations or also create reference configurations and load them onto a number of devices.

9.1.5 IP Interfaces submenu

This area itemises all of the IP- interfaces configured for your gateway with their respective current status. The entries are explained in Table 17.

Column	Description	Values
interface	The type of interface • **ETH0**: Ethernet interface • **PPP**x: configured logical PPP interface	**ETH0, PPP0, PPP1, PPP2, PPP3**

state	Status
	• **Up**:
	  • **ETH0**: the Ethernet link is OK.
	  • **PPP**x: the connection has been established and the **IPCP** protocol has run successfully.
	• **Down**: Ethernet link error or PPP connection not established
		Up, Down
		
		Down

Column	Description	Values
action	Changes the connection status • **connect**: initiates the establishment of a connection • **clear**: closes the connection • **disconnect**: currently has no meaning; please use **clear**	**connect, disconnect clear**
description	Shows the description specified in the **IP Interfaces** configuration applet	`Text`

Table 17 The IP Interfaces table entries

9.1.6 IP Routing submenu

The current IP routing table is displayed in this area.

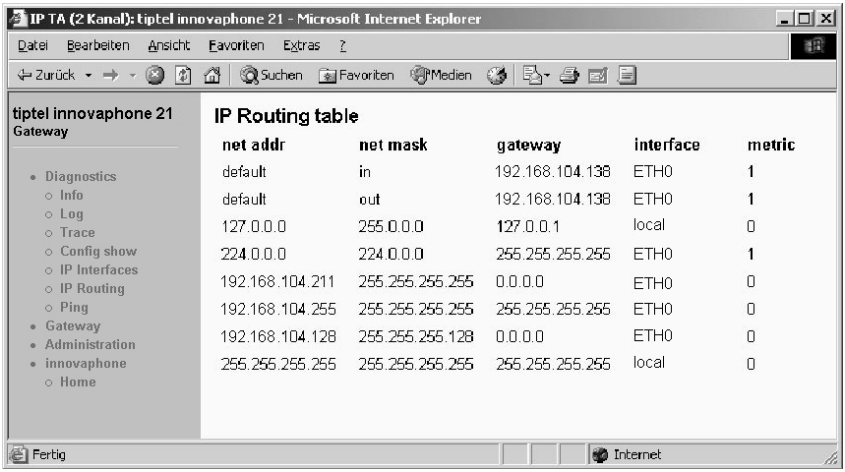

Fig. 41 The IP routing table

9.1.7 Ping submenu

It is often necessary to have a ping command issued for test purposes by the VoIP gateways. Any IP address can be entered in the field. The commands are com-

pleted with the Enter key. The ping command is executed on the connected gateway. The results are in turn displayed in the same window.

9.2 Gateway menu

9.2.1 Config submenu

You can access the configuration applet introduced in section 3 "General information on configuration" from page 20 here.

9.2.2 Voice Interfaces submenu

This area itemises all of the voice interfaces configured for your gateway together with their current status.

The entries are explained in the following table.

Column	Description	Values
Type	The type of interface • **IF**: ISDN interface • **GW**: gateway registered via RAS • **EP**: end point registered via RAS • **GK**: own registration with a gatekeeper	**IF, GW, EP, GK**
Addr	IP address • IP address of the RAS client for **EP** and **GW** • IP address of the gatekeeper for **GK**	xxx.xxx.xxx.xxx

State	Status of the interface
	• **Up**:
	  • **IF** point to multipoint: layer 1 is set up
	  • **IF** point to point: layer 2 is set up
	  • **GW**/**EP**: the device is registered
	  • **GK**: registered successfully at the gatekeeper
	• **Down**: other
		Up, Down

Column	Description	Values
Number	The E.164 address (extension) of the registration • **GW/EP:** the device's configured extension • **GK**: the E.164 address supplied together with the registration • **IF**: no meaning	`nnn`
Name	The name of the interface **IF**: the interface labelling **GW**/**EP**/**GK**: the H.323 alias of the registration	**TEL1, TEL2, TEL, PPP, TEST, TONE,** `Text`
Product	Manufacturer's label • **GW**/**EP**: manufacturer's label for the registered device supplied together with the registration • Otherwise no meaning	

Table 18 The entries in the **Voice Interfaces** table

9.2.3 Calls submenu

In this area you can see the currently active calls to and from your gateway. Please note however that internal calls between innovaphone PBX subscribers are not displayed, if you have installed the optional PBX components.

The individual columns are explained in the following table.

Column	Format	Values	Description
State		`Dial-ling`	Dialling is in progress.
		`Alert-ing`	The dialled distant terminal is being called.
		`Con-nected`	The call is connected.
		`Clear-ing`	The call has been terminated by one of the two parties.
Numbers	`Caller->Called`	`Caller`	The number of the caller as transmitted to the call destination.
		`Called`	The number dialled.
Coders	`ACoders/BCoders`		Encoder used from A to>B or B to>
	`Coder,ms(round, jitter)`		Coder: voice compression used. ms: packeting used. round Transmission duration in ms. jitter: Variance of transmission delay in ms.

Column	Format	Values	Description
Inter-faces	`sif:cgpn:cgnm ->dif:cdpn:cdnm/ ccn`		Sif: Interface for incoming call. Cgpn: calling number, before routing. Cgnm: calling name before routing. Dif: Interface for the outgoing call. Cdpn: called number after routing. Cdnm: called name after routing. ccn: Name of the call counter used for this route (call counter name).

Table 19 Entries in the **Calls** list

9.2.4 Call Counter submenu

The name of the call counters (**name**) and the number of current calls (**calls**) are displayed in this area, provided a call counter with call limiting function has been set up in the resource management for the respective route (see section 7.2.13 "Resources management" from page 104).

9.3 Administration menu

You can save and load the configuration and activate updated firmware in this area.

9.3.1 Licences submenu

In this area, the installed licences will be displayed. Licences can also be installed via this menu.

Two groups are defined for the licences. The hardware based licence (Relay) and the software based licence (PBX).

Type of licence	Licence name
Relay - Registrations	Licence(s) for registration with the gatekeeper
Relay - PRIs	Licences for the S_2M hardware interface
Relay - BRIs	Licences for the S_0 hardware interface

Table 20 hardware based types of licences

The hardware based type of licence (see table 20) is mandatory, to be able to use the hardware. A licence is required both for the connection of the gateway to the public exchange (PRI or BRI) and for each registration with the gatekeeper.

Type of licence	Licence name
PBX - Registrations	Licence(s) for registration with the PBX
PBX - Operators	Licence(s) for the registration of the PBX switch-board operator's location
PBX - SoftwarePhones	Licence(s) to register the SoftwarePhones

Table 21 PBX-related types of licence

The licences are loaded into the gateway using a text file.

The hardware based licences have to be generated via the Web, using the serial number of your innovaphone gateway, and downloaded.

The software based licences are necessary to be able to use the innovaphone PBX and associated applications. A licence is necessary for each registration with the PBX. The software based licences are activated using a **Licencekey** or

Activationkey.

Transmit the licences to the gateway

In the upper area of the licences menu, in the administration user interface, you will find an overview of the licences which have already been installed. Tables 20 and 21 show the various types of licence.

To transmit further licences to the gateway, a text file is required, which you can create using the **License Manager**. The procedure for a hardware based licence is described in section "Create a hardware based licence" from page 130. The procedure for a software based licence is described in section "Create a software based licenceusing the licence manager" from page 131.

To transfer a licence text file to the gateway, proceed as follows:

- In **File:** enter the location of the licence text file, written above, or select the location of the **licence files** using the **Browse...** button.
- Press the **Upload licence file** button to load the licence file into the gateway.

During this upload procedure, the licences are saved in the gateway's configuration, where they are then available. The installed licence is displayed. The type of licence is in the **type** column and the name of the licence followed by the serial number in the **name** column.

You can download the additionally installed licences from the gateway again, to transfer them to another innovaphone device or to save them before deleting the configuration.

Proceed as follows, to download an additionally installed licence from the gateway:

- Press the **download** button next to the licence entry to be saved in the **action** column to save the additionally installed licence as a text file. Follow the further instructions.

Proceed as follows to delete the additionally installed licence from the gateway:

Caution

You should back up the additionally installed licences as previously described before deleting them. Or make sure you still have the original text file you used to install the additional licences.

- Press the **delete** button next to the licence entry to be deleted in the **action** column to delete the additionally installed licence. Follow the further instructions.

The **download all** and **delete all** buttons are used the same way as the **download** and **delete** buttons, but apply to all licences displayed.

Create a hardware based licence

- Connect your web browser to the following web site: `http://www.innovaphone.com/license/license.php`
- After accepting the licence agreement, confirm with "yes".
- You will be asked to log in with your account details. Enter these and click on **Login**.

Tip

Should you not have an account, click on **register** and create an account by entering your email address and a password.

- In the **Serialnumber** field, enter the serial number (`00-90-33-xx-xx-xx`) of your gateway and click on the **Download Licence** button.
- Confirm the serial number with **confirm**. Following the successful confirmation, you will be offered a licence, ready to download.
- Click on **download** to download the licence to your computer.
- Click on **Logout** to leave the area.

The hardware based licences are also managed in the licence manager and can also be downloaded from there, at any time. innovaphone creates these licences using the MAC address, so that they cannot be used on any other hardware.

Create a software based licenceusing the licence manager

If more registrations are attempted than the number of licences available, you must buy and install additional licences. You can obtain licences from your authorised dealer or directly at innovaphone. Licences are activated with a **Licencekey** which in turn is created with an **Activationkey**.

- Connect your web browser to the following web site:
  `http://www.innovaphone.com/license/license.php`
- After accepting the licence agreement, confirm with "yes".
- You will be asked to log in with your account details. Enter these and click on **Login**.

> **Tip**
>
> Should you not have an account, click on **register** and create an account by entering your email address and a password.

- On the welcome page, click on the **Licence manager** button.
- Select the **Activationkeys** menu.
- In the **Activationkey** field, enter the activation key that you received, and click on the the **Add** button.

After you have added the activation key, the **Balance** menu will be displayed, where you can see, at any time, how many licences you have bought, have used or still have available. This pool is available for free use.

- To create licence files from this pool, which can then simply be loaded to the equipment, select the **Licencekeys** menu.
- Here, you can use a drop down menu to enter the corresponding licences and the necessary quantity. To maintain an overview, it's a good idea to enter the serial number and the final customer, the first time.
- For each, individual licence you will be shown what you just asked to be produced as a licence. If you have made a mistake, there is an opportunity here, to undo the step.
- Once the process is completed, you will be returned to the overview page. This will show all of the licences allocated to you and is where you can easily download the licence text file.

9.3.2 Config submenu save

The **Config save (all)** menu enables you to open and save the entire configuration of your gateways as a txt file.

The **Config save (config)** menu enables you to open and save the configuration of your gateways without the user data as a txt file.

The **Config save (LDAP)** menu enables you to open and save the user data from the configuration of your gateways as a txt file.

9.3.3 Config update submenu

In the **Config update** menu, a configuration saved with **Config show submenu** (see section 9.1.4 "Config show submenu" from page 122) is loaded onto your gateway.

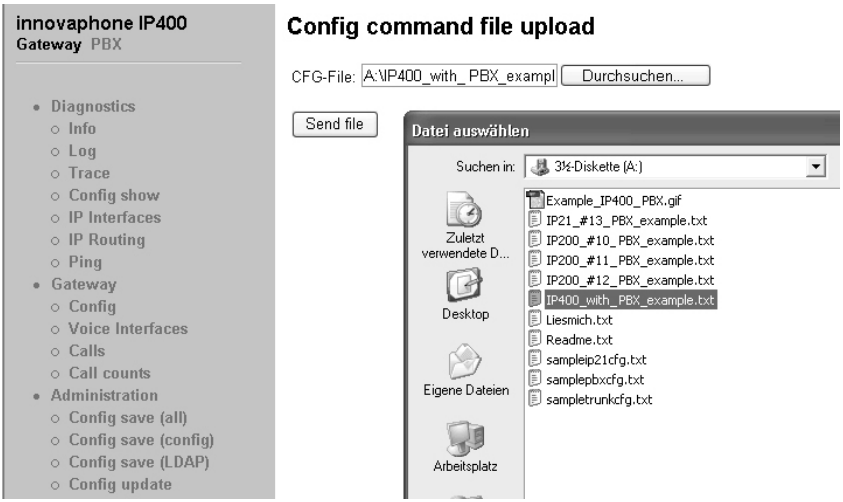

Fig. 42 Loading a configuration in the web browser

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.

Fig. 43 Activating the loaded configuration

Please observe that the configuration file is loaded into your gateway's volatile memory. This means it is neither permanently backed up nor immediately operative. That is why the menu shown in Fig. 43 on page 133 appears after successfully uploading the configuration.

Refer to section 3.2 "Checking and saving the configuration" from page 22 to find out how to check and back up the new configuration.

9.3.4 Firmware update submenu

This function allows you to upload a new firmware version onto your gateway. You can obtain new firmware versions from your dealer.

Fig. 44 Updating the firmware in the web browser

Enter the path and file name of the firmware file to be loaded in the **Protocol-File** field and click on the **Send file** button.

You will be told not to interrupt the loading process under any circumstances, whilst loading the new firmware.

Caution

If the **Ready** LED flashes, when downloading, this process may not be interrupted. Otherwise, the equipment may be damaged.

If the loading process is nevertheless interrupted, do not on any account switch your gateway off. Repeat the procedure again, once you have eliminated the problem.

Look at the documents supplied with the new versions, to find out whether new boot firmware also has to be loaded. If this is the case, note the sequence required (if specified) of the boot code and firmware update.

The new firmware is not immediately activated. You have to perform a reset, to activate the new version. The **immediate reset** and **reset when idle** links are provided for this purpose.

After successfully updating the firmware, you must then close all browsers and applet windows and restart the browser. This is necessary, as the new firmware may also include new user interface elements, which can only be activated this way.

9.3.5 Update Server

There is a special function, to automatically update the firmware of your innovaphone gateway, under **Config > General settings > Update Server**. With the **URL** field, you can enter a URL pointing to a script file within your network. This script file must follow a particular syntax, which you will find in the document "How to use the Update Server"; one of the innovaphone support files. In the **Poll interval [min]** field, you can enter an interval, to regularly check this script file for any changes. If the script file contains a link to a new version of firmware, the update will proceed automatically. You must simply ensure that the new version of firmware has first been copied to a suitable directory on an internal web server.

A web server is necessary, which can be reached by all of the equipment to be updated. Furthermore HTTP-PUT write access (to save the equipment configuration) and HTTP-GET read access (for all innovaphone equipment requiring access) must be set up, on this internal web server. The web server must also permit

simultaneous access from all equipment.

innovaphone equipment use DHCP for access. For further information on the DHCP-Client and the update server see Appendix D: "The innovaphone DHCP Client" from page 152.

9.3.6 Boot update submenu

This function allows you to upload a new version of boot code onto your gateway. New versions of boot code can be obtained from your dealer.

Enter the path and file name of the boot code file to be loaded in the **Boot-File** field and click on the **Send file** button.

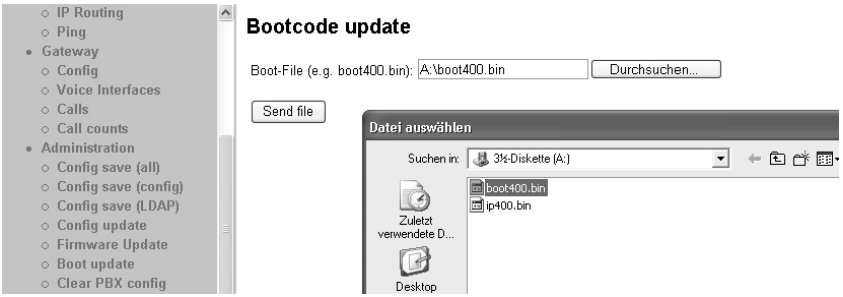

Fig. 45 Updating the boot code in the web browser

You will be told not to interrupt the loading process under any circumstances whilst loading the new boot code.

Caution

If the **Ready** LED flashes, when downloading, this process may not be interrupted. Otherwise, your gateway may be damaged.

If the loading process is nevertheless interrupted, do not on any account switch your gateway off. Repeat the procedure again, once you have eliminated the problem.

The new boot code is not immediately activated. You have to switch your gateway off and then back on again to activate the new version.

Look in the documents supplied with the new versions to find out whether new protocol firmware also needs to be loaded.

9.3.7 Clear PBX config submenu

This function enables you to delete the entire configuration of any installed innovaphone PBX component. This is useful, for example, after restoring the standard configuration, since it means that the configuration of the innovaphone PBX components is not reset.

We recommend that you make a backup of the configuration before deleting the data (see section 9.1.4 "Config show submenu" from page 122).

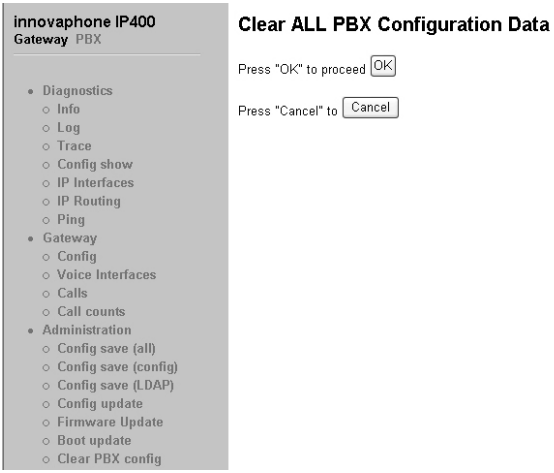

Fig. 46 Deleting the innovaphone PBX data

You are first asked whether you really want to delete the entire configuration after actuating **Clear PBX config**. If this is confirmed, the innovaphone PBX configuration will be completely deleted. You then have to perform a reset. You can decide whether this should happen immediately or only when the gateway is in idle status.

Fig. 47 Reset after deleting the innovaphone PBX configuration

9.4 innovaphone menu

9.4.1 Home submenu

The innovaphone web site is called up by selecting this area.

Appendix A: Safety instructions

The manufacturer assumes no responsibility for any personal injury, damage to property or subsequent damage that can be attributed to improper use of the device.

This devices complying with the essential requirements of the regulation 1999/5/EC and the other relevant provisions related to it (Article 3 of the R&TTE directive), if used for its intended purpose.

The declaration of conformity for this device is available in the CD as part of this package.

To configure VoIP terminal equipment see the "VoIP terminal - users manual" and "Administrator's manual - innovaphone PBX". All instructions specified there should be followed carefully and the devices should only be used in accordance with these instructions.

Safety instructions for the IP 400

Caution

Please note the following instructions for your own safety:

Power supply

Only use the delivered external power supply to operate the equipment.

The external power supply is designed for operation with a 100-240 V, 50-Hz AC mains network. Never try to connect the mains adapter to other mains systems.

- External power supply, primary: 110-240 V AC +10 % - 15 %, 50/60 Hz, 250 mA; secondary: 12 V DC, 800 mA

The equipment cannot be operated during a mains failure. The equipment settings however are retained.

The power socket must be near to the equipment and easy to access. The only way of interrupting the power supply to the equipment is by removing the mains lead from the mains socket.

Installation and connection

Only qualified personnel may install and mount (if required) the equipment.

Make sure the equipment has adequate ventilation, particularly in closed cabinets.

Lay the connection cables in such a way that no-one can trip over them. None of the cables may be bent excessively, pulled or subjected to mechanical strain.

The equipment is intended for use in dry rooms only.

- Operating temperature: 0 °C to 40 °C, 10 % to 90 % relative humidity, non-condensing
- Storage temperature: -10 °C to 70 °C

The equipment may not be installed and operated under the following conditions:

- In damp, dusty rooms or in rooms where an explosion may occur
- At temperatures over 40 °C or under 0 °C
- Where it is subject to impact stress or vibrations

Cleaning

Use a soft, slightly damp cloth to clean the surface of the equipment housing. Do not use any chemicals or abrasives. The equipment does not require any maintenance.

Malfunctions

There is no need to open the device, if it is used as intended and serviced as specified. Should you nevertheless decide to open the device, make sure that all connection cables are removed beforehand. Before opening the device, interrupt the power supply by removing the mains plug.

Do not open or reconnect faulty equipment. In this case, return the equipment to your dealer or service centre. Keep the original packaging in case you need to return the equipment, since it provides ideal protection. Back up all entries (e.g. on a PC) to avoid losing data.

Appendix B: Troubleshooting

Typical problems

In our experience, some problems occur more frequently than others. These problems are listed in Table 22 below, which also gives advice on how to solve them.

Symptom	Description	Action
The gateway does not respond. The **ready**, **link** and **act**. LEDs (with the IP 400) are permanently on.	The gateway is waiting for a firmware download.	• Perform a quick reset by pressing the **Reset** button.
The gateway does not respond. **ready** LED is on, **link** LED is off.	The Ethernet connection is not working.	• Check the position of the "**connect to** ..." switch. • Check the Ethernet cabling.
The gateway does not respond. The **ready** and **link** LEDs are on; the **act**. LED flashes during attempted access.	The gateway's configured IP address is incorrect.	• Configure the IP parameters correctly.
As delivered from the factory, the gateway does not assign the PC an IP address.	The DHCP client is active, once the equipment is turned on.	• Press the Reset button briefly. • Have the PC assigned an IP address again.
A telephone connected to **tel1** or **tel2** is not working (IP 400 only). The display is not displaying anything.	There is no power to the telephone.	• Check the **Power** box in the interface configuration.

Symptom	Description	Action
A terminal connected to **tel1** or **tel2** is not working 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, activate the **100 Ohm Termination** checkbox in the interface configuration (see page 53). • If the termination is ok, deactivate the **100 Ohm Termination** checkbox in the interface configuration (see page 53).
Incoming calls are received properly, but callback is not possible from the call list of the telephones in use.	The **Calling Line** ID is incomplete, because the exchange line access code is missing.	• Configure the trunk line access code for the interface where the call arrives (see page 94) or activate the automatic CLI correction (see page 95).
Calls can be established 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 78).
Calls can be set up to a remote VoIP device, but no voice connections can be established.	The media channel can't be set up as the two VoIP devices do not have a common voice codec.	• Make sure that the **exclusive** checkbox is deactivated (see from page 76 onwards).

Symptom	Description	Action
Calls can be set up to a remote VoIP device, but no voice connections are established.	The media channel can't be set up as the two VoIP devices do not have a common voice codec.	• Only the media channel is set up directly between the two VoIP devices; all signalling connections are operated via the gatekeeper. • Make sure both VoIP devices have been correctly configured for IP routing, particularly the subnet mask and standard gateway.
Calls to a remote telephony gateway are constantly rejected.	The gateway does not support overlapped sending (single digit dialling).	• Add a hash (#) to the dial prefix of the route leading to this gateway in order to force en-bloc dialling (see page 100).
The gateway loses its configuration after it has been disconnected from the power supply.	The configuration has not been saved in the non-volatile memory.	• Save the configuration to non-volatile memory after any successful change (see page 22).
A telephone connected to **tel1** or **tel2** is working, but does not have a dial tone (IP 400 only)	No route has been defined for this interface.	• Define at least one valid route entry for the interface concerned.
The gateway is connected to the network behind a "firewall" and the configuration is not working.	The firewall does not allow any access to the gateway.	• In the firewall, enable the service tcp/80 (http) for the gateway.

Symptom	Description	Action
The gateway is connected to the network behind a "firewall" and no connections can be established to other VoIP devices.	The firewall does not support the H.323 protocol.	• Activate "H.323 Firewalling" in your firewall software and if necessary "H.323 NAT" too. Refer to your firewall documentation for this purpose. • Refer to the Section "NAT and firewalls" from page 143.
You are using the `gwload.exe` utility. Uploading of new firmware fails, although the gateway is found.	Your computer's arp-cache contains incorrect information.	• Clear the computer's arp-cache. To do this with a Windows PC, use the command `arp -d` *`ip-addr`*.
Fax transmissions are interrupted.	T.38 is not authorised in the gateway definition.	• Activate the T.38 protocol (see from page 73 onwards).
Fax transmissions are interrupted, in particular with lengthy faxes.	The gateway and PBX to which the fax machine are not connected to a synchronous ISDN clock.	• Provide correct clock synchronisation (see page 53).

Table 22 Troubleshooting

NAT and firewalls

If there is a firewall protecting your network from the Internet and you want to establish connections between your gateway and remote terminals via the Internet, you need to ensure that the firewall is configured appropriately.

Firewalls usually have two jobs. They control access to equipment and areas within your network and they implement IP address translation in networks that do not have their own regular network address (so called "NAT", network address translation). "NAT" can also be implemented by routers.

In connection with voice over IP, both functions require a detailed analysis of the data stream in order to be implemented. This must be performed by your firewall or router firmware. Please refer to the documentation of the product you are using.

There are four ways of proceeding, if the product you are using does not have "H.323 firewalling":

- You configure the firewall so that it allows ***all*** required data to and from the gateway.

  Although this solution is usually not well received by system administrators, it does not present a security problem, since the gateway, as a dedicated device, does not perform any services other than "voice over IP". No security gaps are caused in your network by opening the path to and from the gateway.
- The number of ports to be released can be restricted if the H.323 devices whose data is to cross the firewall are all innovaphone devices. For this, however, the **Disable H.245 Tunnelling** box must not be checked, in the gateway definitions for any equipment (see Section 6.1.4 "H.323 protocol options" from page 73).

  The following ports have to be released in both directions:

  - Tcp: destination port `80` (http), any source port (for configuration)
  - Tcp: Destination port `1720` (h.225), any source port (for VoIP calls). We recommend releasing ports `1721`, `1722`, `1723`, etc.. The number of ports to be released results from the number of connections and the administrator should do this, as required.
  - Udp: destination port >= `2050`, source port `5004` and `5005` (RTP) (for VoIP calls)

Tip

If the RAS protocol is not used, QSIG tunnelling is no longer possible. In a scenario for example, where two locations with PBXs are linked, this can lead to performance limitations, as no additional features can be transmitted.

The number of ports to be released cannot be restricted if the gateway has to communicate with third party products. It is thus necessary to release all ports to and from the gateway.

- If the RAS protocol is to be used (we recommend this) and, if the H.323 equipment whose data is to cross the firewall is exclusively from innovaphone, then the number of ports to be released can be restricted as shown in the following section. For this, however, the **Disable H.245 Tunnelling** box must not be checked, in the gateway definitions for any equipment (see Section 6.1.4 "H.323 protocol options" from page 73).

  - Tcp: destination port `80` (http), any source port (for configuration)
  - In the configuration applet, all RAS-Gateways (**VOIP-Interfaces > GWnn** area) must be set to **> Registration at gatekeeper as gateway mode**, the **Remote gatekeeper address > IP-address** must be entered and the **Disable dynamic signaling port** must be activated. In the **Signaling Port** field, the port (`1720`, `1721`, `1722`, `1723`, etc.) for the GWnn interface must be entered.
  - Tcp: Destination port `1720` (h.225), any source port (for VoIP calls). We recommend releasing ports `1721`, `1722`, `1723`, etc.. The number of ports to be released results from the number of connections and the administrator should do this, as required.
  - Udp: destination port >= `2050`, source port `5004` and `5005` (RTP) (for VoIP calls)
  - Udp: Destination port `1718` and `1719`
  - Udp: Source port `1719` (for RAS and h.225)
  - Udp: Source port `5004` and `5005` (for RTP)
  - If the fax service is used, Udp: source port `5006` must also be released, as after establishing a connection, it switches to T.38.

  The number of ports to be released cannot be restricted if the gateway has to communicate with third party products. It is thus necessary to release all ports to and from the gateway.
- The gateway is located ***in front of*** the firewall, which means that the data stream doe not need to pass the firewall. Bear in mind however, that in this case it is not possible to establish voice connections from within your network to the gateway (e.g. with innovaphone Softwarephone PCs).

It will not be not possible to operate across the firewall if your network is operated in NAT mode and the product you are using does not support "H.323 NAT".

VoIP and heavily loaded WAN links

If voice data is transmitted over heavily loaded, narrowband WAN links, the voice quality can suffer, if the links can no longer ensure adequate transmission quality (see Table 11 on page page 77 and Table 12 on page page 79).

Prioritisation of voice data on the WAN links can help here. This can usually be achieved by the routers used.

Direct use can be made of the "Prioritisation of H.323 voice data" function, if it is supported by your router.

If your router is able to use the IP **type of service** (TOS) field for prioritisation, you can make use of this function. Your gateway sets the TOS field to `0x10` for all IP packets that it transmits. You can change this value as required in the configuration applet in the **TOS Value** field in the **IP Interfaces** area.

Tip

You can enter hexadecimal, octal or decimal values; the entries `0x10`, `020` and `16` are all equivalent. Bear in mind that the same value should be set in the TOS field for all devices.

If this is not the case, you can use the function "Prioritisation according to source/ destination address", if available. In this way, data packets from and to the gateway are prioritised. This in effect corresponds to the prioritisation of voice data as above.

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

Some routers are able to prioritise but are unable to interrupt the transmission of larger packets once it has started. This can result in poor quality in spite of prioritisation. In such a case, check whether this interruption can be separately enabled. Some routers refer to this function, somewhat confusingly, as **interleaving**.

If you require technical support

Please have the following information on hand whenever you need to contact your dealer for support:

- The entire configuration as displayed by **Config show** (see Section 9.1.4 "Config show submenu" from page 122)
- A trace which shows the error situation (see Section 9.1.3 "Trace submenu" from page 121),
- The complete version identifier of your gateway. You can find it on the gateway's welcome page (see Fig. 39 on page 120)
- The serial number. You can find it on the serial number label which is on the bottom of the device or on the gateway's welcome page (see Fig. 39 on page 120).

Appendix C: ISDN error codes

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

Error code (hex)	Error code, bit 8 set to 1 (hex)	Error code (decimal)	Description
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
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

Error code (hex)	Error code, bit 8 set to 1 (hex)	Error code (deci-mal)	Description
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

Error code (hex).	Error code, bit 8 set to 1 (hex).	Error code (decimal).	Description.
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

Error code (hex)	Error code, bit 8 set to 1 (hex)	Error code (decimal)	Description
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

Table 23 ISDN error codes

Appendix D: The innovaphone DHCP Client

innovaphone equipment supports automatic configuration using standard DHCP options. In addition, they support several innovaphone specific options, for some configuration options which are particular to VoIP.

This configuration includes:

- **POSIX Time Zone** (to define the time zone for the equipment location),
- **VLAN ID** (the VLAN identity for voice traffic),
- **VLAN priority** (the VLAN priority for voice traffic),
- **TOS Bits** (the value of the IP TOS field for VoIP traffic),
- **Enbloc dialling** (forced en-bloc dialling) and
- Configuration parameters for the **Update Server**.

For information on the options for the DHCP standard, see section 4.1.1 "DHCP configuration options" from page 26.

System requirements

To be able to use these specific DHCP options, a DHCP server is required, which actually supports these options. The most common DHCP servers are, for example, Microsoft Windows DHCP service and Linux dhcpd.

Installation

To make these specific DHCP options useable for the DHCP server, the server has to be informed about them. Look at the documentation for your DHCP server, to see how to do this.

In the following section we will illustrate the installation of the innovaphone specific DHCP options using the Windows 2000 DHCP server as an example.

- Launch the Windows 2000 DHCP server (Start >Programme> DHCP).
- First, you have to define a new vendor class. Select **Define vendor class...** (**Define Vendor Class...**) in the DHCP server context menu.
- The **New class** window will appear. In the **Display name** field, enter `innovaphone`.
- In the **Description** field enter `innovaphone VoIP Options`.
- In the **ASCII:** field enter `1.3.6.1.4.1.6666`. When entering, and in the area, it will be displayed as **Binär:**
- Confirm your input, by clicking on the **ok** button.

- Close the **DHCP vendor class** by clicking on the **close** button.
- Choose **Configure predefined options** from the DHCP server context menu.
- Choose the **option class innovaphone**, add the innovaphone specific options (see table 24) and confirm the values by clicking on the **ok** button.

Name	Data type	Array	Code
POSIX TZ	String	No	202
VLAN ID	Word (16 bit)	No	206
VLAN Priority	Byte (8 bit)	No	207
TOS Bits	String	No	208
Enbloc dialling	Byte (8 bit)	No	209
Update URL	String	No	215
Update Poll Interval	Word (16 bit)	No	216

Table 24 innovaphone specific options

Configuration

To configure the supplier specific DHCP options for a particular area, proceed as follows:

- Select the entry **Configure options** in the context menu of the **Scope options** area.
- Select the **Advanced** tab and select the **DHCP vendor class** `innova-phone`.
- Activate the option, that you want to support, complete the associated values and accept them.

Table 25 shows the available options and their meaning.

Option	Description	How to code
POSIX TZ	Defines the time zone and the date of the change for daylight saving (Summer time).	Enter the correct TZ string into the field, as you would enter it in the equipment's configuration applet. See section 8.1.3 "Defining the source for time and date" from page 110.
VLAN ID	The 802.1q VLAN ID for the data to be sent and received from your equipment.	Enter the numerical ID into the 16 bit field.
VLAN Priority	The 802.1p VLAP priority for data sent from your equipment.	Enter the numerical priority into the 8 bit field.
TOS Bits	The value of the IP TOS field in the IP header of voice data sent from the equipment.	Enter the numerical priority into the field. Add the prefix `0x` when entering hexadecimal numbers, or start with the prefix `0`, to specify octal numbers.
Enbloc dialling	The number of seconds, that the dialled digits will be kept in the IP 200, before they are sent "en bloc" to the gatekeeper.	Enter the number of seconds into the 8 bit field. The value `0` means that en bloc dialling is deactivated and the dialled digits will be immediately transmitted to the gatekeeper.

Option	Description	How to code
Update URL	Location of the URL, from which update commands can be issued. This is identical to the `/url` option parameters for the UP1 module.	The complete URL as for example `http://192.168.0.10/file.txt`. Symbolic host names are not supported.
Update Poll Interval	Standard poll interval in minutes. This is identical to the `/poll` option parameters for the UP1 module.	Interval in minutes.

Table 25 Available options and their meaning

Index

F

G

H

I

J

L

T

U

V

W

X

innovaphone® AG
Böblinger Strasse 76
D-71065 Sindelfingen
Tel: +49 (70 31) 730 09-0
Fax: +49 (70 31) 730 09-99
www.innovaphone.com
info@innovaphone.com

CE