IP gateway

IP1200

Administrator Manual

innovaphone

Pure IP Telephony

Texts and illustrations have been compiled and software created with the utmost care, However errors cannot be completely ruled out. This documentation is therefore supplied under exclusion of any liability or warranty of suitability for specific purposes. innovaphone reserves the right to improve or modify this documentation without prior notice.

IP gateway

IP1200

Manual

Version 6.0

Release 6.0, 3rd edition, April 2007

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

Böblinger Str. 76 71065 Sindelfingen, Germany
Phone +49 (7031) 73009-0 Fax +49 (7031) 73009-99
http://www.innovaphone.com

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.

Power supply

The mains adapter of the device is designed for operation with a 100-240V, 50Hz AC network. Some devices can also be operated using **PoE** (**P**ower **o**ver **E**thernet) in accordance with IEEE 802.3af. No attempt should ever be made to connect the equipment to other mains systems! In the event of power failure, the equipment settings are retained.

Installation and connection

The connection cables should be laid safely so that no one can trip over them. Connected cables must not be bent excessively 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 must not be installed and operated under the following conditions:

- In damp, dusty, vibrating rooms or in rooms where an explosion may occur.
- At temperatures over 40°C or under 0°C

Malfunctions

There is no need to open the device, if it is used as intended and serviced as specified. But if the device is opened for some reason, it must be ensured that all connection cables have been first removed. Before opening the device, interrupt the power supply by removing the power/Ethernet cable.

Do not open or reconnect faulty equipment. The original packing should be kept safely in case the device needs to be returned, since it provides ideal protection. All entries (for example, on a PC) should be backed up beforehand to avoid losing data.

Disposal

When due for disposal, the device must be returned directly to the manufacturer innovaphone AG in accordance with the WEEE guidelines (**W**aste **E**lectrical and **E**lectronic **E**quipment). The costs for returning the device shall be borne by innovaphone AG.

Table of contents

1 Introduction

This manual describes the innovaphone IP DECT device IP1200. The IP1200 gateway enables DECT-compatible terminals to be used with the innovaphone PBX. It is a combined system with the gateway and the DECT base station in one housing.

The IP1200 is an IP DECT gateway that integrates DECT-compatible subscribers in the innovaphone PBX. It enables very complex DECT systems to be set up. With the multicell capability of the IP1200 base station, several devices can be installed, between which roaming and automatic handover operate. A base station supports up to 12 channels in parallel. The number of base stations in one system is theoretically limited to 254. An extension with a repeater increases the reception range and thus achieves better coverage, but does not increase the number of channels.

1.1 Standards

The system, on the IP side, is fully H.323-compatible. It supports echo cancellation and several codecs for voice compression. On the DECT side, the system is GAP-compatible. The IP50, IP52 and IP54 handsets from innovaphone are especially suited, however.

For the professional installation of an IP1200 DECT system, innovaphone in future will provide all technicians with a kit that should ensure ideal coverage already at the start of the project and before installation.

1.2 Features

- GAP compatible VoIP gateway
- 12 channels base station
- Multicell installation in master-slave configuration
- Increased reception range by using repeater
- roamin and seamless handover between base stations and repeater
- Two Ethernet interfaces
- SIP and H.323 simultanously

- Mains adapter, 110-240V, 45mA, or "Power over LAN"

Caution

All instructions in this manual should be followed carefully and the device should only be used as intended. 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.

2 Initial start-up

The device is switched on by connecting the external power supply or through a PoE (Power **o**ver **E**thernet) power supply in accordance with IEEE 802.3af. The device is on and ready if the Ready LED on the housing is lit in green. The device isn't ready if the Ready LED is lit in red. If the Ready LED is lit in orange the device is in tftp mode.

To be able to access the device, the RJ45 Ethernet connector (**ETH0**) on the device must be connected with the RJ45 Ethernet connector on the Ethernet hub or switch using twisted pair cable. The device can also be connected directly with a PC if desired. For this, no additional crossover cable is required, since *'Auto-MDX'* support is provided.

2.1 Establish administrator access

There are two ways of putting the device into service. When shipped from the factory, the device is in so-called *DHCP Automatic mode*. In this mode, the device (once switched on) tries to obtain an IP address from a DHCP server. To determine which IP address was assigned to the device, it is possible under Windows to execute the **nbtstat** command with a command line interpreter (e.g. DOS-Box):

```
c:/ nbtstat -R (reloads remote cache table)

c:/ nbtstat -a ipxxx-xx-xx-xx (displays the IP address
of the specified remote computer using the entered MAC
address, where ipxxx is to be replaced with the device
name (e.g. ip800 or ip1200) and xx-xx-xx is to be
replaced with the last 6 hexadecimal digits of the
serial number)

NetBIOS remote machine name table
   Name                Type         Status
---------------------------------------------
ipxxx-XX-XX-XX<00>  UNIQUE      Registered
195-226-104-217<00>  UNIQUE      Registered
```

```
    MAC address = 00-90-33-XX-XX-XX
```

Caution

The IP address cannot be displayed with **nbtstat** if the NetBIOS environment is configured exclusively for the name resolution via WINS. If the **nbtstat** command does not find the device, then the NetBIOS name resolution must be configured accordingly.

Under Linux, the **nmblookup** command can be used for this purpose, providing the SAMBA package has been installed:

```
[dvl@cobalt ~ 2]$.nmblookup ipxxx-xx-xx-xx

got a positiv name query response from 195.226.104.217
(195.226.104.217)
```

The device was assigned the IP address **195.226.104.217** . The device can now be accessed from any PC in the same network 195.226.104.**x** and can be configured as required.

If no DHCP server is available, the **ETH0** interface can be switched to the configured IP address by briefly pressing the Reset key. If an IP address was not explicitly configured, the IP address **192.168.0.1** is specified as standard.

Caution

Once the device has been put into service, *DHCP Automatic mode* should be switched immediately, since a reset changes the operating mode (see also the chapter entitled "*Configuration/ETH0-1/DHCP*").

Note

The initial start-up of the device concerns only the **ETH0** interface. The **ETH1** interface has the fixed IP address **192.168.1.1** during initial start-up.

Note

The state when shipped can be restored through a long reset.

3 User interface

The user interface has been tested with Internet Explorer (5.x, 6.x) and with the Firefox browser. It can, however, also be used with Netscape.

The user interface of the VoIP device can be accessed with a Web browser by calling up the IP address determined beforehand.

3.1 Structure of the user interface

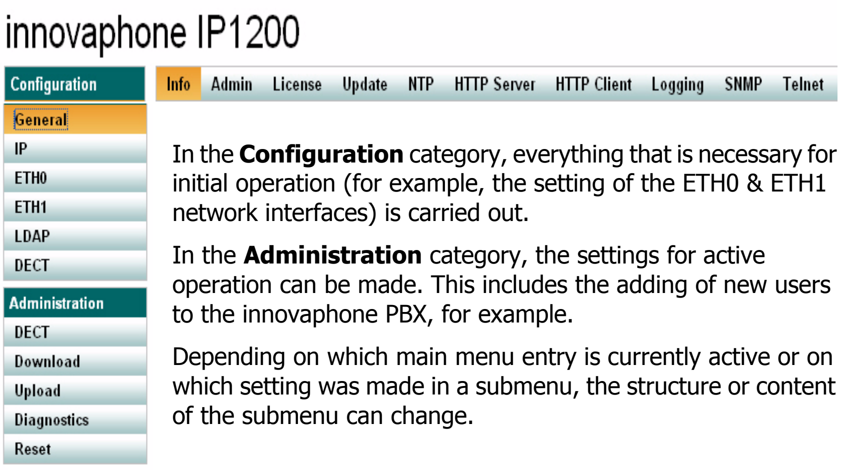
The user interface of the VoIP deviceis divided into two areas:

- The navigation area (along the left and top edge of the screen), which consists of menu and submenu commands.
- The entry area, in which the device settings are made.

The main menus in the left area of the browser are divided into two categories:

- **Configuration**
- **Administration**

A main menu, in turn, can be split into several submenus.



In the **Configuration** category, everything that is necessary for initial operation (for example, the setting of the ETH0 & ETH1 network interfaces) is carried out.

In the **Administration** category, the settings for active operation can be made. This includes the adding of new users to the innovaphone PBX, for example.

Depending on which main menu entry is currently active or on which setting was made in a submenu, the structure or content of the submenu can change.

3.2 Protected areas

Apart from the start page, all areas of the device are password-protected. When shipped from the factory, the innovaphone VoIP device has:

- The standard user name **admin** and
- The standard user password **ipxxx** (ipxxx stands for the device type, for example, ip800, ip1200, etc.).

Caution

To raise the security of the VoIP device, the standard user and the standard password should always be changed (see chapter entitled "*Configuration/ General/Admin*")!

3.3 Saving the settings

The setting are saved in the respective submenu always using the ***OK*** button.

- Some changes to settings require a device restart to become effective. In this case, *reset required* is shown in the respective menu. More detailed information on restarting the device is contained in the chapter entitled "*Administration/Reset*".

4 Configuration and administration

The structure of chapter 4 “*Configuration and administration*” corresponds to that of the user interface (*category / main menu / submenu*).

4.1 Configuration

In the **Configuration** category, everything that is necessary for initial operation of the device is carried out.

4.1.1 Configuration/General

Using the **General** menu, the basic settings for the VoIP device can be made.

4.1.1.1 Configuration/General/Info

General information about the VoIP device is displayed here:

Version
- The software version (6.00) <Gateway>[firmware].
- Die bootcode version <Boot code>[firmware].
- The hardware version <HW>[no].
- The memory size <Flash/Ram>.

Serialno The serial number or MAC address (**M**edia **A**ccess **C**ontrol) of the device (6-digit hexadecimal number).

Coder The number and type of voice channels.

HDLC The number of HDLC channels (**H**igh-level-**D**ata-**L**ink **C**hannels).

Sync The physical interface (TEL, PPP, BRI, PRI) used for synchronisation.

SNTP Server The IP address of the SNTP server (**S**imple **N**etwork **T**ime-**P**rotocol) used, if configured.

Time The time of the device in accordance with the specifications of the NTP server (**N**etwork **T**ime **P**rotocol) and the time zone.

Uptime The operating time since the last cold or warm start.

The **DECT** section provides you with information about the DECT system:

Firmware	The firmware version of the DECT system.
System ARI	The system ID of the DECT system.
Frequency	The used frequency of the DECT subsystem (EUR = 1.8 GHz; USA = 2.4 GHz).

4.1.1.2 Configuration/General/Admin

Administrator access is configured here.

Device Name	The name of the device. This name is displayed in the browser as a title.
User Name	The administrator name.
Password	The administrator password, which is used for all protected areas. See chapter 3.2 "*Protected areas*".

4.1.1.3 Configuration/General/Licence

The installed licences of the device are displayed here. This menu can also be used to load additional licences.

The types of licence are as follows:

- **BRI LIC** - Enables the activation of a BRI ISDN channel.
- **PRI LIC** - Enables the activation of a PRI ISDN channel.
- **DSP LIC** - Enables the activation of a voice channel in the digital signal processor (DSP). This is always necessary if a transition is to be created from the traditional telecommunications world (analogue or digital) to IP.
- **a/b LIC** - Enables the activation of an analogue channel.
- Gatekeeper LIC – Enables the activation of a gatekeeper function. This is always necessary if you wish to use a central gatekeeper for trunking with several media gateways. It is not required if you only connect an innovaphone PBX with home users who use the IP110/IP200/IP230 telephones; but it is advisable if you wish to manage external users, who are registered with an IP302, for example, centrally.
- **Basic LIC** - Enables installation of the PBX and Voicemail LIC. It is a basic

prerequisite for operating the innovaphone Media Gateway as a PBX. The licence size is selected in accordance with the number of necessary registrations on the PBX. An approximate value can be calculated from the number of connected user devices (including fax machines / DECT handsets, etc.) plus 10-15%.

- **PBX LIC** - Enables the connection/registration of a terminal with the innovaphone PBX. The order unit is always 10 LIC.
- **Voicemail LIC** - Enables activation of the innovaphone Voicemail. The order unit must be identical to the number of basic licences installed on the device.

All licences are linked to the MAC address of the device on which they are installed.
In the upper section, the licences already installed are displayed:

Type The installed licence type (PBX, Relay or DECT for IP DECT subsystem).

Name A precise description of the licence with number of registrations followed by the MAC address.

Action By clicking the **download** button, the displayed licences can be loaded from the device and saved as a text file.
By clicking the **delete** button, the displayed licence can be deleted from the device.
The **download all** and **delete all** buttons are used in the same way as the **download** and **delete** buttons, but apply to all licences displayed.

In the lower section, additional licences can be loaded:

By entering the location of the licence text file described above in the **File** field or by selecting the location using the **Browse...** button and then clicking **Upload**, additional licences can be loaded onto the device.

With this upload procedure, the licences are saved in the configuration of the device and are available after a short restart. The installed licence is displayed.

4.1.1.4 Configuration/General/Update

The update server is used for efficient administration of various VoIP devices. The update server reads a file at intervals from a configurable URL (**U**niform **R**esource **L**ocator).

Command File URL

An URL, for example `http://192.168.0.1/update/script-ip800.txt`, pointing to a file whose commands are executed.

If the URL ends with a slash (/), for example `http://192.168.0.1/update/`, the device is adding the file name `update-ipxxx.htm` automatically, deduced from the device short name (for example `update-ip800.htm`).

Furthermore the placeholder #h and #m can be used in the URL-String:

- #h - will be replaced by the device short name (for example IP800).
- #m - will be replaced by the device mac-adress (for example 00-90-33-01-02-03).

These placeholders may be used e.g. to address a device-specific directory (`http://192.168.1.2/update/#h/script.txt`) or to generate HTTP-GET parameters (`http://192.168.0.1/update/script.php?mac=#m`).

If the directory of the file is password-protected, the access credentials must be specified in the chapter "*Configuration/General/HTTP Client*".

Interval [min]

An interval (in minutes) at which the file is re-read and executed.

Detailed information on the update server and the update script is contained in Appendix E "*Configuration of the update server*".

4.1.1.5 Configuration/General/NTP

Through specification of an NTP (**N**etwork **T**ime **P**rotocol) server, the VoIP device is able to synchronise its internal clock with an external time source. This is required, as without specification of a time server the internal time is reset to 0:00

hrs, 01.01.1970 after every reset.

Server	The IP address of the time server.
Interval [min]	The time interval (in minutes) at which the device is to synchronise with the time server.
Timezone	Facility to select the time zone in which the device is located.
String	Additional time zones can be added in accordance with the IEEE (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) POSIX (**P**ortable **O**perating System **I**nterface for Uni**X**) standard.
Last sync	Displays the data and time of the last synchronisation.

Detailed information on the NTP server is contained in Appendix F "*Configuration of an NTP server/client*".

4.1.1.6 Configuration/General/HTTP Server

Advanced, security-related settings of the VoIP device can be made.

Disable HTTP basic authentication	The logon data is transmitted in plain text as standard, and is thus susceptible to recording and eavesdropping. To avoid this weak point, it is recommended that you disable standard authentication (with user name and password) and use digest hash authentication instead.
Password protect all HTTP pages	Apart from the start page *Configuration/General/Info*, all areas of the user interface require the entry of the administrator user ID. If you enable this check box, a password is compulsory for all pages of the device.
Port	The standard entry here is HTTP Port 80. It can be changed (for example, 8080). The device is then accessible via this port only *(for example, <IP of the device>**:**8080*).
Allowed stations	Access to the device can be restricted to a particular network area (for example, *192.168.0.0 / 255.255.0.0*) or to a particular network address (for example, *192.168.0.23 / 255.255.255.255*).

In addition, all active HTTP sessions are displayed under the **Active HTTP sessions** section.

For example: **From** `172.16.1.49` **To** /HTTP0/info.xml **No** 22.

4.1.1.7 Configuration/General/HTTP Client

Some files that the device must access via HTTP (MoH, announcement, voicemail, etc.) may be located in a password-protected area. The different URLs (**U**niform **R**esource **L**ocator) with the respective user names and passwords can be stored here.

URL An URL, for example `http://192.168.0.1/update/script-ip800.txt`, pointing to a file in a password-protected directory whose commands are executed.

If the URL ends with a slash (/), for example `http://192.168.0.1/update/`, the device is adding the file name `update-ipxxx.htm` automatically, deduced from the device short name (for example `update-ip800.htm`).

The placeholder #h and #m can be used in the URL-String for HTTP-Clients too:

- #h - will be replaced by the device short name (for example IP800).
- #m - will be replaced by the device mac-adress (for example 00-90-33-01-02-03).

These placeholders may be used e.g. to address a device-specific directory (`http://192.168.0.1/update/#h/script.txt`) or to generate HTTP-GET parameters (`http://192.168.0.1/update/script.php?mac=#m`).

User The authorised user who has access to the directory.

Password The relevant password of the user.

4.1.1.8 Configuration/General/Logging

External logging is disabled as standard (**Off**). After selection of a log type, logging is enabled, as are the relevant entry fields.

Off Logging is disabled.

TCP The device transmits the syslog entries using a TCP (**T**ransmission **C**ontrol **P**rotocol) connection.

- In the **Address** field, the IP address at which the TCP connection is to be set up is entered.
- In the **Port** field, the port to which the connection is set up is specified.

SYSLOG The syslog entries are transmitted to a syslog recipient (also referred to as `syslogd`, `syslog server` or `syslog daemon`), which is then responsible for their further evaluation or storage.

- In the **Address** field, the IP address of the `syslogd` server is entered.
- In the **Class** field, the desired message class that will be responsible for further processing of the syslog entries is entered. The syslog class is a numeric value between 0 and 7.

HTTP The syslog entries are transferred to a Web server, where they can be further processed. Each individual syslog entry is transferred as form data to the Web server in HTTP GET format.

- In the **Address** field, the IP address of the Web server that carries out further processing of the transmitted data is entered.
- In the **Path** field, the relative URL of the form program on the Web server is entered.

  The device will make a HTTP GET request to the Web server on the entered URL, followed by the URL-encoded syslog entry. If, for example, a page named `/cdr/cdrwrite.asp` with a form that expects the log message in parameter `msg` exists on a Web server, then the value `/cdr/cdrwrite.asp` is entered. The device will then make a `GET /cdr/cdr-write.asp?event=syslog&msg=`**`logmsg`** request to the Web server.

4.1.1.9 Configuration/General/SNMP

The VoIP device allows the operating state to be monitored using SNMP (**S**imple **N**etwork **M**anagement **P**rotocol with version 1.0). Standard MIB II and a manufacturer-specific MIB (**M**anagement **I**nformation **B**ase) are supported. Detailed information about this MIB can be obtained from a certified innovaphone dealer or downloaded directly in the download area of the innovaphone homepage (`http://www.innovaphone.com`).

Community If the standard community name *public* is not being used, a different community name can be entered in this field.

Device Name For more detailed information, a device name can be specified here for the SNMP agent.

Contact As can a contact person (**Contact**).

Location As can a location (**Location**).

Authentication Trap Access via SNMP is only possible if the correct community name is entered. If this check box is checked, a trap is generated in the case of access with an incorrect community name.

Trap Destination Destinations for trap messages also have to be defined if the device is to trigger the traps defined in the manufacturer-specific innovaphone MIB.

Allowed Networks To increase security, access to the device can be restricted by restricting SNMP access to a defined list of computers or IP address ranges.

4.1.1.10 Configuration/General/Telnet

Access via the Telnet protocol can be enabled here.

Enable Telnet A checked check box enables access to the device using telnet. The device can be configured with commands such as *reset, config change UP1 /url <http url> /poll <secs>*, for example.

4.1.2 Configuration/IP

General IP protocol settings are made here, as well as the configuration of the

VPN protocol PPTP, the DSL protocol PPPOE and the address translation with NAT.

4.1.2.1 Configuration/IP/Settings

The basic IP settings are made here.

ToS Priority Configuration of the ToS (**T**ype **o**f **S**ervice) field for voice pakkets. The value `0x10` is used as standard. Consequently, voice data receives priority forwarding.

First UDP RTP port / numbers of port This entry restricts the range of ports in which UDP RTP voice data (**U**ser **D**atagram **P**rotocol **R**eal-time **T**ransport **P**rotocol) is received for H.323 or SIP calls. The port range 16384 to 32767 is used as standard. 128 ports are the smallest range. For a voice connection, an RTP port and an RTCP port are used.

See also the notes contained in Appendix B “*Troubleshooting*”, section “*Port settings in respect of NAT and firewalls*”.

First UDP NAT port / numbers of port This entry restricts the range of ports that may use UDP NAT data (**N**etwork **A**ddress **T**ranslation).

Private Networks Through specification of a private network, the device can control the media relay function. The media relay function is needed, for example, to solve NAT problems.
In the case of a call, the PBX and the RELAY then automatically use the media relay function, if they determine that a VoIP call is running between the private and the public network. Here, the private network configuration is always referred to, to find out whether the Calling Party Number and the Called Party Number are located in the same IP network.
If nothing is entered here, it is assumed that both parties are located in the public network. The media relay function is not used and RTP packets are exchanged directly between the end points. If a private network is specified, RTP packets are not passed directly between the terminals, but are routed between the internal and external network via the device.

4.1.2.2 Configuration/IP/NAT

The telephone is able to connect IP terminals from the network with a non-public address to the public Internet. For this, **NAT** (**N**etwork **A**ddress **T**ranslation) is necessary. NAT serves as the router and requires a configuration of the PPPoE protocol.

The necessary parameters for this configuration can be set here:

Enable NAT A checked check box enables NAT in general. This function is only required if the IP telephone is also a DSL router.

Default forward destination If all incoming data packets are to be forwarded to a particular IP address as standard, the destination IP address must be entered here.

Port-specific forwarding To be able to address several internal destinations, different port number numbers are assigned to IP addresses of the internal network here.

4.1.2.3 Configuration/IP/H.323 NAT

H.323 NAT is an add-on for the general NAT function. This function is only needed if the telephone connects the private network with the public network. The telephone must therefore represent a connecting point between the two networks. This function enables H.323 calls between private and public networks.

Enable H.323 NAT Enables NAT for H.323 VoIP calls.

Require authentication H.323 authentication is obligatory if the check box is checked. This setting protects against externals attacks on the private network. H.323 messages without authentication are not routed to the private network.

H.225/RAS destination IP address of the server in the private network, to which incoming H.225/RAS messages are routed.

H.225/ Signalling destination IP address of the server in the private network, to which incoming H.225/signalling messages are routed.

The **Status** section provides you with a brief overview of the registered users (**Registered Clients**) and the calls currently active (**Active Calls**).

4.1.2.4 Configuration/IP/PPP Config

The parameters for the DSL and VPN connections are set here.

Clicking the interface ID (**PPPn**) opens the respective configuration page, on which the PPP interface configuration can be performed.

PPP Interface PPP*n* section:

Enable Enables/disables the interface. The PPP interface is only displayed in the PPP State overview page if it is enabled.

Connection Port For PPP connections using ISDN channels, you select one of the ISDN interfaces (PPP, TEL, BRI, PRI) here. This concerns only devices with an ISDN interface. However, PPTP (VPN) and PPPoE (DSL) connections using the Ethernet interface (ETH) are also possible.

Descriptive Name A descriptive name for the interface can be entered here. This name is used for the overview in the PPP State submenu (see chapter entitled "*Configuration/IP/PPP State*").

Bandwidth By specifying a particular bandwidth, the transfer rate for a connect can be restricted and the available network bandwidth is optimally allocated. This is necessary, since for an upstream, the available bandwidth may be lower than required. Packets that exceed the maximum available bandwidth would be discarded. If a bandwidth is specified, packets that exceed the maximum available bandwidth are not sent at all.

Maximum transfer unit (Bytes) Restricts the packet size for a data exchange. This is necessary for some devices, since they can only transfer a restricted number of bytes. Here are a few typical MTU sizes in octets:

- X.25 - 576
- PPoE (for example, DSL) - 1492
- ISDN, Ethernet - 1500
- ATM - 4500

IP Address for Remote Party Assigns a local IP address to the remote party in order to integrate it in the local network.

Auto dial after boot Results in the relevant PPP connection of the device being set up and kept open immediately after start-up.

Allow inbound connections If the server is configured as a PPP server, a checked check box allows PPP dial-up connections to the device (inbound).

No DNS on this interface When a PPP connection to the remote party is set up, an attempt is always made as standard to resolve the name of the remote party to an IP address via DNS. Here, there is always the risk, however, that there may be several PPP connections that use the same IP address (for example, `192.168.1.2`). As a result, a name resolution would take place once only, and the data packets sent to a different name with the same IP address are lost.

Exclude interface from NAT With this setting, a particular interface can be excluded from NAT (**N**etwork **A**ddress **T**ranslation), should NAT be enabled (see chapter entitled “*Configuration/IP/NAT*”).

No IP Header Compression	The VoIP devices support the compression of voice data along the PPP link using the **RTP header compression** method (RFC 2508, 2509). This drastically reduces the required bandwidth for VoIP calls. To suppress this, the **No IP Header compression** check box must be enabled.
Adapt to Cisco PPP peers	Try the **Adapt to Cisco PPP peers** option if a Cisco router is used at the remote location and problems arise in the transmission of voice data.

Authentication section:

The PPP protocol allows reciprocal authentication (inbound/outbound). Generally speaking, for inbound connections, only the **inbound** authentication is required, for **outbound** connections, only the outbound authentication. But it can also happen that an authentication is required both from the client and from the server.

Outbound User / Password	Required for outbound connections. For example, the name of the DSL provider or the DSL user ID of the remote party (1564863maxmuster.1und1.de, 1564863maxmuster@t-online.de), or the Inbound User / Password of the remote party.
Inbound User / Password	Required for inbound connections. For example, the Outbound User / Password of a different gateway.

PPPOE section:

Here, the interface can be configured as a PPPoE client (for example, for DSL).

DSL Provider (Access Concentrator)	The DSL modem name. Since several modems can occur in a network, a broadcast is sent for identification.

PPTP section:

This operating mode applies for inbound and outbound calls. The PPTP (Point-to-**P**oint **T**unneling **P**rotocol) implements private VPN connections via the Internet or other networks operated with the IP protocol.

PPTP connections are always dial-up connections. An IP address is dialled. Authentication is performed by means of user name and password. In addition, the transferred voice data can be encrypted with MPPE (**M**icrosoft **P**oint-to-**P**oint **E**ncryption). The prerequisite, however, is that the remote party also supports this method. If MPPE was enabled, this may result in a delay in voice transmission. If quality losses of this kind occur, a decision has to be made between security or voice quality.

The innovaphone devices can dial into a remote PPTP server as a PPTP client, as well as provide a dial-in point themselves.

Server Address The IP address of the PPTP server. If the device itself is to play the role of a PPTP server, then no IP address has to be entered here.

Route to Interface Here, connection setup inquiries can be forwarded directly to a particular interface. For example: ETH0-1, PPP0-31.

Enable MPPE Encryption Enables the Microsoft Point-To-Point Encryption Protocol. MPPE (RFC 3078) uses the RSA RC4 algorithm.

Stateless Operation Here, the key is modified after every transferred packet.

40-Bit Encryption Enables the encryption with a 40-bit session key.

128-Bit Encryption Enables the encryption with a 128-bit session key.

ISDN section:

Link Configuration The ISDN interface configuration can be performed here. The PPP interface can be configured here for inbound and for outbound calls.

Link type Four different link types can be selected.
Singlelink (64k) - A connection via a B channel.
Multilink (128k) - A connection via two bundled B channels. Provides double the transmission speed.
Permanent B1 - Uses the B1 channel exclusively.
Permanent B2 - Uses the B2 channel exclusively.

Local Subscriber Number The **Local Subscriber Number**, in the case of inbound dial-up connections, is the call number (MSN) under which incoming calls are to be accepted.
The **Local Subscriber Number**, in the case of outbound dial-up connections, is the outgoing call number (MSN) to be used for the call.

2nd Local Subscriber Number If **Multilink** is used, a different call number can be used for the second channel of the PPP remote terminal being called. The entry field can be left empty if the same call number as for the first channel is to be used.

Outbound Connections Here, the ISDN interface can be configured for outbound PPP dial-up connections.

Called Party Number The call number (MSN) to be used for the outgoing call.

2nd Called Party Number The call number (MSN) to be used for the outgoing call on the second B channel.

Inbound Connections Here, the ISDN interface can be configured for inbound PPP dial-up connections.

Calling Party Number By specifying the **Calling Party Number**, the acceptance of incoming calls can be restricted to this one call number. If the entry field is left empty, all data calls are accepted on the selected ISDN interface(s).

IP Routes section:

Static routes for the PPP interface can be configured here. This is required, since no routing protocol is used.

Network Address The network address of the new route being added.

Network Mask The network mask of the new route being added.

Gateway The network address of the default gateway.

4.1.2.5 Configuration/IP/PPP State

The state for all defined and enabled PPP interfaces is displayed here. In addition, it is possible to manually close the connection and set it up again.

Interface ID of the PPP interfaces.

Address The local IP address of the PPP interface.

Type The interface type: PPTP, PPPoE or, in the case of PPP using an ISDN channel, one of the ISDN interfaces.

State Displays the current state of the interface. Possible states: *Connecting, Up* or *Down*.

Since The time as of when the connection exists is specified here.

Action

- ***connect*** establishes a connection to the selected interface.
- ***clear*** deletes the current connection to the selected interface.
- ***info*** displays relevant connection data for the selected interface.

Name The name of the interface or connection.

4.1.2.6 Configuration/IP/Routing

The routing table of the current **IP configuration** of the gateway is displayed here. The table is used for fault analysis by the network administrator. The table is structured as follows:

Destination Network The destination network address.

Network Mask The associated network mask.

Gateway The IP address of the default router.

Interface Displays the interface on which the route was created. Possible interfaces are: *ETH0*, *ETH1*, *PPP0-31, Local* and *ISDN.*

State Possible states are: *Up* or *Down.*

4.1.3 Configuration/ETH0-1

The Ethernet interfaces of the device can be configured here.

The structure of both menus is identical. The special features of, and differences between, the two Ethernet interfaces (**ETH0 & ETH1**) are explained in the text at the relevant place within this chapter. For both Ethernet interfaces, *CAT5-STP* cables are recommended.

4.1.3.1 Configuration/ETH0-1/Link

The transmission mode of the Ethernet interface is defined here.

The **auto** transmission mode is pre-selected:

auto	Automatic selection of the transmission speed.
10m-hdx	Corresponds to 10 MBit Half Duplex.
10m-fdx	Corresponds to 10 MBit Full Duplex.
100m-hdx	Corresponds to 100 MBit Half Duplex.
100m-fdx	Corresponds to 100 MBit Full Duplex.

In addition, the status of the interface (*Up* or *Down*) and the Autonegation used (for example, *100m-fdx*) are displayed.

4.1.3.2 Configuration/ETH0-1/DHCP

The DHCP function can either be disabled in *DHCP Disabled* mode or operated in *DHCP Client* or in *DHCP Server mode*. The DHCP function of the Ethernet interface has four operating modes in total:

Disabled The IP address and other parameters are configured manually.

Server The IP parameters are configured manually in *DHCP Server mode* (standard IP address `192.168.0.1`). The DHCP server is on and should be configured accordingly as described in chapter "*Configuration/ETH0-1/DHCP Server*".

Client In *DHCP Client mode*, the device receives its IP configuration from a DHCP server to whose network the device is connected.

Automatic The first time the device is switched on (powered up), **ETH0** works as a DHCP client. After a restart through briefly pressing the Reset button, the **ETH0** interface is allocated the configured IP address. If an IP address was not explicitly configured (see chapter "*Configuration/ETH0-1/IP*"), the IP address `192.168.0.1` is specified as standard.

In the as-shipped state, **ETH0** is configured in *DHCP Automatic mode* with the IP address `192.168.0.1` and **ETH1** is configured in *DHCP Disabled mode* with the IP address `192.168.1.1`.

> **Caution**
>
> *DHCP Automatic mode* should **not** be used for 'normal' operation, since an accidental restart switches the operating mode.

4.1.3.3 Configuration/ETH0-1/IP

The manual configuration settings are effective if the DHCP mode *Disabled* or *Server* is configured. To the right of the entry fields, the settings currently stored are always displayed.

IP Address The IP address of the network adapter.

Network Mask The subnet mask of the network adapter.

Default Gateway The standard router of the LAN.

DNS Server The DNS server of the LAN.

Proxy ARP Where IP packets are routed from Ethernet to PPP interfaces via the device, the device can appear to the local network as if it were the addressed terminal itself. This also allows IP terminals on the same Ethernet segment, which do not have a correct routing entry, to communicate over the device and use the WAN connection. To allow dial-in access to the entire network, the *Proxy ARP* function must be enabled.

Multicast With the Multicast setting, all data packets for sending can be sent to all devices in a network. Data packets are sent to all devices in a network as standard. The Multicast check box is therefore checked.

In the **Static IP Routes** section, additional network routes can be defined, if other network areas apart from the local network are required.

Network Destination The network address of the destination route.

Network Mask The relevant subnet mask of the destination route.

Gateway The standard gateway of the network being routed.

4.1.3.4 Configuration/ETH0-1/NAT

Use of NAT (**N**etwork **A**ddress **T**ranslation) for the relevant interface can be enabled here. It is also possible to exclude particular network addresses and masks from the translation.

Include Interface in NAT A checked check box enables NAT for the interface, providing NAT was enabled in general under chapter "*Configuration/IP/NAT*". In other words, the network connected to ETH*n* is regarded as external unless it was excluded under **Exclude Address** or **Exclude Mask**.

Exclude Address IP network that should not be included in the Network Address Translation.

Exclude Mask IP network area that should not be included in the Network Address Translation.

4.1.3.5 Configuration/ETH0-1/VLAN

If a network uses several VLANs (**V**irtual **L**ocal **A**rea **N**etwork), a VLAN can be specified for every Ethernet interface . This ensures that the data packets are transmitted to the specified VLAN only.

ID The ID of the VLAN. The value 0 is applied if the **ID** entry field is empty. The VLAN ID with the value 0 switches the QoS (**Q**uality **o**f **S**ervice) off according to 802.1q.

Priority If the switch at the port to the innovaphone gateway happens to be configured to a different ID, the same value must be entered here to allow the Ethernet packets to be prioritised. A priority value between 0 and 7 is entered here (configuration on the Ethernet switch).

4.1.3.6 Configuration/ETH0-1/DHCP Server

If the DHCP server was enabled (see chapter entitled "*Configuration/ETH0-1/DHCP*"), it can be configured here.

All settings marked with a "*****" are innovaphone-specific settings that may only be found with innovaphone devices.

Lease Time [min] The validity period of the DHCP lease in minutes.

Check Interval [min] The interval (in minutes), at which a check is made whether the DHCP lease is still valid.

Address Ranges:

First Address The IP address that represents the start of the address range (for example, `192.168.1.100`).

Last Address The IP address that represents the end of the address range (for example, `192.168.1.110`).

Offer Parameters:

Network Mask The network mask in respect of the IP address (for example, `192.168.1.100` corresponds to the network mask `255.255.255.0`).

Default Gateway The standard router (for example, `192.168.1.1`).

TOS Priority The ToS (**T**ype **o**f **S**ervice**)** value for voice packets (`0x10`).

IP Routing It is possible to add static IP routes. They must be entered in the format *Address:Mask:Gateway*. The elements must be separated by a colon. By completing a route with "**;**", several routes can also be added.

DNS Server 1 The primary DNS server address.

DNS Server 2 The secondary DNS server address.

Syslog Server The Syslog server address.

Time Server The Time server address.

Timezone String * Here, new time zones can be added to the devices in accordance with the IEEE POSIX standard using a particular character string (for example, CET-1CEST-2,M3.5.0/2,M10.5.0/3).

TFTP Server The TFTP server address.

WINS Server The WINS server address.

Primary Gatekeeper * The primary gatekeeper IP address.

Secondary Gatekeeper * The alternative Gatekeeper IP address.

Coder * Coder preference for VoIP telephones.

Gatekeeper Identifier * The VoIP gatekeeper or the gatekeeper ID for VoIP telephones.

Dial Tones * The dial tone that is transmitted as the standard dial tone to the VoIP telephones (for example, *German PBX* = as German PBX, *US* = US dial tone, *UK* = British dial tone).

Enblock Dialling Timeout [s] *
Switches on enbloc dialling for VoIP telephones.

Faststart [0|1] *
With the **Faststart[0|1]** setting, you can turn on/off the H.323 Faststart procedure.

Tunneling [0|1] *
With the **Tunneling[0|1]** setting, you can turn on/off the H.245 Tunneling procedure.

Language *
All VoIP telephones that receive their IP address via DHCP have the language defined here set up as the standard language.

Dialling Location *
Defines the various PBX access numbers on VoIP telephoness for directory access. This character string must contain /cc, /ac, /ntp, /itp, /col and /pbx options. Such a character string may look like this: "*/cc 49 /ac 7031 /ntp 0 /itp 00 /col 0 /pbx 7*".

AM/PM Clock [0|1]
Enables/disables the English time format for VoIP telephones. The German time format is displayed as standard: "*dd.mm.yy hh:mm, 24-hour clock."*
If a 1 is entered in this field, the English time format "*mm/dd hh:mm xm, 12-hour am/pm clock"* is displayed.

LDAP Directory
To allocate a functioning LDAP configuration to all VoIP devices integrated via DHCP, a configuration character string can be entered in the **LDAP Directory** field. You obtain this configuration character string by executing the following command in the browser of a configured device: "*<IP address of the VoIP device>/!mod cmd PHONEDIR0 ldap-config"*. When this command has been executed, a configuration character string is output in the browser, which you copy and paste into the **LDAP Directory** field of the DHCP server. In this way, all further devices are given a correct LDAP configuration.

Update Interval [min]
All devices integrated via DHCP are assigned the interval specified here in the **Interval [min]** field of the update server (see chapter entitled "Configuration/General/Update").

Update Server URL All devices integrated via DHCP are assigned the URL specified here (for example, `http://192.168.1.2/update/script.htm`) in the **Command File URL** field of the update server (see chapter entitled "*Configuration/General/Update*"). An automated update of the devices is thereby ensured.

802.1q VLAN ID The configuration at the switch must be observed for setting the VLAN ID. An empty **802.1q VLAN ID** field (16 bit) assumes the value 0. The VLAN ID with the value 0 switches QoS (**Q**uality **o**f **S**ervice) off according to 802.1q ab. If the switch at the port to the innovaphone device happens to be configured to a different VLAN ID, the same value must be specified here to allow a prioritisation from the Ethernet. To be able to distinguish between the VLANs, the Ethernet packet is extended by 4 bytes, of which 12 bits are intended for the inclusion of the VLAN ID, making 4094 VLANs possible (VLAN ID 0 and 4095 are reserved or invalid).

802.1p VLAN Priority In the **802.1p VLAN Priority** field (3 bit), the associated VLAN priority level (a value between 0 and 7) can be specified, in order that voice data is given priority forwarding, for example.

4.1.3.7 Configuration/ETH0-1/DHCP Leases

VoIP devices that have obtained an IP address from the installed DHCP server via this interface are displayed here.

In the **Reserve IP Address** section, it is also possible to allocate a particular IP address to a particular MAC address.

IP Address The allocated IP address of the DHCP lease.

MAC Address The MAC address of the integrated VoIP device.

Acknowledged The date on which the DHCP lease was allocated.

Expires The date on which the DHCP lease will expire.

Type The type of DHCP lease: *Dynamic* or *Reserved*.

Hostname The hostname of the integrated VoIP device.

Under the **Cleanup** section, allocated DHCP leases can be deleted again.

- By clicking **Clear dynamic leases**, all dynamically allocated leases are deleted.
- By clicking **Clear reserved leases**, all reserved leases are deleted.
- By clicking **Clear all leases**, all allocated leases are deleted.

4.1.3.8 Configuration/ETH0-1/Statistics

The **Statistics** submenu provides you with an overview of all sent (tx) and received (rx) data packets:

tx-good	The number of successfully sent packets.
tx-unicast	The number of successfully sent unicast packets.
tx-broadcast	The number of successfully sent broadcast packets.
tx-multicast	The number of successfully sent multicast packets.
tx-lostcarrier	The number of lost carrier signals. Indicates a defective medium (for example, cable).
tx-deferred	The number of deferred packets.
tx-collision	The number of colliding packets (max. 16).
tx-excesscol	The number of colliding packets (if tx-collision > 16).
tx-latecol	The number of colliding packets that require too much time to be transmitted. If a collision was detected after the 512th bit of the frame being transmitted was reached, a *late collision* is output.

rx-good	The number of successfully received packets.
rx-unicast	The number of successfully received unicast packets.
rx-broadcast	The number of successfully received broadcast packets.

rx-multicast The number of successfully received multicast packets.

rx-crc-err The number of received CRC checksum errors.

rx-align-err The number of alignment errors (incorrect driver, cable defective) when receiving data packets.

rx-too-short The number of data packets that are too short during the transmission.

rx-too-long The number of data packets that are too long during the transmission.

rx-collision The number of colliding packets (max. 16).

rx-overrun-err The number of buffer overrun errors when receiving data pakkets.

rx-queue-overrun The number of queue overrun errors when receiving data pakkets.

rx-no-buffer The number of no buffers when receiving data packets.

rx-tx-64 The total number of sent and received packets of 64 Bytes.

rx-tx-64-127 The total number of sent and received packets of between 64 and 127 Bytes.

rx-tx-128-255 The total number of sent and received packets of between 128 and 255 Bytes.

rx-tx-256-511 The total number of sent and received packets of between 256 and 511 Bytes.

rx-tx-512-1023 The total number of sent and received packets of between 512 and 1023 Bytes.

rx-tx-1024 The total number of sent and received packets of 1024 Bytes.

4.1.4 Configuration/LDAP

The LDAP server and replicator configuration can be performed here. The LDAP server makes the local LDAP database available to external clients.

4.1.4.1 Configuration/LDAP/Server

Here, access data can be configured that allows external LDAP clients read or read and write access to the LDAP database.

VoIP telephones require read access to the LDAP database. Replication connections require write access.

Username	The LDAP user name.
Password	The relevant LDAP user password.
Write Access	Write authorisation is granted if the check box is checked.

4.1.4.2 Configuration/LDAP/Server-Status

The displayed server status data is automatically updated at intervals.

connections	Total number of all connections to the LDAP server.
write connections	Number of connections with write authorisation.
rx-search	Number of received search inquiries.
rx-modify	Number of received change requests.
rx-add	Number of received add requests.
rx-del	Number of received delete requests.
rx-abandon	Number of received termination requests.
tx-notify	Number of sent notifications.
tx-error	Number of sent error notifications.
tx-error-49	Number of sent error notifications due to incorrect access data.
tx-error-50	Number of sent error notifications due to insufficient rights.

4.1.4.3 Configuration/LDAP/Replicator

LDAP replication can be configured here. The task of LDAP replication is to copy and keep up to date the entire content or parts of the user database of a remote innovaphone PBX.

Replication is required in three application cases:

1. Replication of the user data from the master PBX to a standby PBX. The replicator configuration takes place on the standby PBX.
2. Replication of the user data from the master PBX to a slave. The replicator configuration takes place on the slave.
3. Replication of the user data from a DECT master to a DECT radio. The replicator configuration takes place on the DECT radio.

Server	The LDAP server IP address.
Location	To replicate only the objects of a particular location in the sense of a partial replication, the name of the location (PBX name) can be specified here.
User & Password	The LDAP user and password. Is stored on the LDAP server under the chapter "*Configuration/LDAP/Server*".
Enable	A replication only takes place if the Enable check box is chekked.

4.1.4.4 Configuration/LDAP/Replicator-Status

The displayed replicator status data is automatically updated at intervals. In addition, the last ten activity messages of the replication are displayed:

Server	IP address and port of the remote LDAP server.
Full Replication	Current state of the replication. There are four states: *Stop*, *Starting*, *Up*, *Down*.
remote	Displays the state of the replication in poll direction.
notify	Number of received notifications.
modify	Number of modified objects.
local	Displays the state of the replication in push direction.
add	Number of locally added objects.
del	Number of locally deleted objects.
modify	Number of locally modified objects.
notify	Number of notifications that have arisen locally.
pending	Number of locally waiting objects.

4.1.5 Configuration/DECT

DECT-specific settings of the IP1200 are made in this chapter.

4.1.5.1 Configuration/DECT/System

The general configuration of the DECT system, as well as the allocation of the DECT system name and password are performed in this submenu.

Name The name of the DECT system. This name determines the name of the LDAP object in which the system parameters are stored. For a replication from an innovaphone PBX, a corresponding object must be created in the PBX.

Pwd The password for the encryption of all passwords in the LDAP database. If the user data from an innovaphone PBX is replicated, the PBX password must be configured.

Sys-Mask Without configuration of a Sys-Mask, the so-called *connection handover* is always used. With configuration of a Sys-Mask, the faster *bearer handover* between the DECT base station and the associated DECT repeater can be used.

AC The access code that must be specified when logging on the DECT handset. This specification is only required if the value *With user AC only* is selected in the *Subscriptions* list box.

Subscriptions The type of handset registrations (subscriptions).

- **With User AC only**: Subscriptions are allowed that have been configured in the user input screen with specification of an IPEI number and with specification of an authentification code (**AC**). The specification of the AC is optional and can therefore be blank.
- **Allow Anonymous**: Anonymous subscriptions are allowed. The handset logon always takes place with the **AC** system. The **AC** entry field can be empty here too.
- **Disable**: Subscriptions are not possible.

Tones Various tone schemas can be used here.

Enbloc Dialling A checked check box enables enbloc dialling. This is only required if the gatekeeper or SIP provider does not support single digit dialling.

Local R Key/Display Handling The features of the R key are implemented in DECT systems on relevant VoIP protocols and should always be enabled in the innovaphone PBX.

DTMF through RTP Channel DTMF data is transmitted via the RTP media channel rather than via the signalling connection (TCP), if this check box is checked.

No Transfer on Hangup A call is being made on a telephone. A second call is received on this telephone (call waiting); the first call is put on hold and the second call is answered. If the second call is ended by replacing the handset, then the first call on hold is signalled specially on this telephone.
If this check box is checked, then a call on hold is ended.

Coder The coder is the type of voice data compression. This coder is used for all external calls. If the remote VoIP device does not support the configured encoding, an encoding supported by both parties is negotiated.

Frame The frame size of the voice data in *ms*.

Exclusive A checked check box enables the selected coder as exclusive. In this way, use of the configured encoding (coder) is forced. This can result in call failure in the event that this device and the remote VoIP device do not support a common coder.

SC A checked check box enables **S**ilence **C**ompres-sion (**SC**). In other words, no voice data is transmitted during pauses in the conversation.

4.1.5.2 Configuration/DECT/Master

It is necessary to configure the operating mode of the DECT system. A gatekeeper must also be specified here, on which the innovaphone PBX component is operated.

Mode **Active** switches on the DECT master function. In every DECT system, there must be a DECT master.
Standby switches on the standby function for the DECT master.
Off switches off the DECT master function.

GK The IP address of the primary gatekeeper. The device on which the innovaphone PBX component is operated.

Alt GK The IP address of the secondary, alternative gatekeeper.

GK ID The gatekeeper ID of the gatekeeper to be used.

Prot The protocol to be used for the communication. There is a choice between:

- **H.323** (*RFC 1889*), which is the recommended protocol for innovaphone VoIP devices, since it contains most features.
- **SIP** (*RFC 3261*).

4.1.5.3 Configuration/DECT/Features

The **Feature Codes** section is enabled as soon as the *Supplementary Services (with Feature Codes)* check box is explicitly checked for an interface (see chapter entitled "*Administration/Gateway/Interfaces*") or the *Enable* check box is chekked for an IP DECT device (see chapter entitled "*Configuration/DECT/Features*").

Using **Feature Codes**, further features are made available to the VoIP telephones. The codes for these features can be configured. Here, it is to be noted:

- that the "**$**" character stands for a variable number of characters (for example, a telephone number) and
- the "**$**(**x**)" character for a fixed number of characters of length (x).
- Principally actions will be initialized with the „*****"-character and
- with the „**#**"-character actions will be cancelled.

Forwarding options

The IP devices supports three different types of call forwardings:

Activity	Code	Description
CFU **Activate** **Deactivate**	 *21*$# #21#	Activates/deactivates continuous call forwarding. The $ character stands for the destination number.
CFB **Activate** **Deactivate**	 *67*$# #67#	Activates/deactivates call forwarding if the line is busy. The $ character stands for the destination number.

CFNR **Activate** **Deactivate**	 *61*$# #61#	Activates/deactivates call forwarding if there is no answer. The $ character stands for the destination number.

Lock

VOIP-Phones can be locked from default status with following hotkey:

Activity	**Code**	**Description**
Lock Phone **Unlock**	*33*$# #33*$#	Activates/deactivates the phone’s keylock. The „**$**“-character stands for the PIN.

PIN

Restrict access for unauthorised users. With this function the protection can be activated and the PIN can be setted.:

Activity	**Code**	**Description**
Set PIN	*99*$*$*$#	Stores a PIN for the telephone. The first $ character is the old PIN (the first time the PIN is set, no character is replaced here); the next two 2 $ characters are the new PIN.

Call protection

With this function the reaction to incoming calls can be handled specially.

In silence mode the telephone will getting muted. The caller still can hear the free-tone.

Aktivität	**Code**	**Beschreibung**

Do not Disturb		No calls are put through if the check box is checked.
On	*42#	
Off	#42#	
Do not Disturb Int.		No internal calls are put through if the check box is checked.
On	*421#	
Off	#421#	
Do not Disturb Ext.		No external calls are put through if the check box is checked.
On	*422#	
Off	#422#	

Call waiting functions

Aktivität	**Code**	**Beschreibung**
Call Waiting **On** **Off**	 *43# #43#	Activates/deactivates the call waiting function of the telephone.

Delete local settings

Aktivität	**Code**	**Beschreibung**
Clear Local Settings	*00#	Deletes all Feature Code settings made.

Pickup

Incoming calls can be overtaken inside a group.

Aktivität	**Code**	**Beschreibung**
Pickup Group **Directed**	*0# *0*$#	*Pickup Group* picks up a call of a pickup group. With *Directed*, a particular call can be picked up through specification of the call number.

Park

Aktivität	**Code**	**Beschreibung**
Park	R*16$(1)	With *Park*, a call can be parked by pressing the R key and then entering the Feature Code (1 = position on own extension).
Unpark	#16$(1)	With *Unpark*, it can be retrieved again.

Park To **Unpark From**	*17(1)# #17(1)#	Same as *Park*, only that the call is parked on a different extension, for example, the exchange (0).

Join Group

Aktivität	Code	Beschreibung
Group Join **Leave**	*31# #31#	With *Group Join*, you join a group. With *Leave*, you leave it again. Not implemented for IP DECT.

Call back

With following code it is possible to initiate a call back at the caller side, if it is busy.

Aktivität	Code	Beschreibung
Call Completion **Cancel**	*37# #37#	With *Call Completion*, a callback can be initiated if the called subscriber happens to be busy. Not implemented for IP DECT.

4.1.5.4 Configuration/DECT/Radio

In this menu, the DECT system can be configured as a DECT radio, provided that a DECT master was already configured.

Disable A checked check box disables the DECT radio (cell).

Master The IP address of the DECT master. If the device itself was defined as the DECT master, then no IP address has to be entered here. The local IP address `127.0.0.1` is automatically entered.

Alt Master The IP address of the standby master.

Radio ID In **Singlecell** operation, the radio ID 0 must be specified. In **Multicell** operation, every radio must have a unique ID. The ID must lie in the range 0 - Sys-Mask (with Sys-Mask specification) or 0 - 254 (without Sys-Mask specification).

Sync source The radio ID with which the radio is to synchronise.

Alt Sync Source The radio ID with which the radio is to synchronise in the event that the sync master is not accessible. Here, it is to be noted that no loops must be created. In other words, if a sync master exists with the radio ID 1 and an alt sync master exists with the radio ID 3, then the alt sync master must on no account synchronise with any radio, since the radio synchronises with the alt sync master in the event of failure of the sync master.

4.2 Administration

Everything that is necessary in active operation is carried out here.

This includes, for example, the registration of VoIP telephones with a gateway or, if available, an innovaphone PBX.

The registration (subscription) of DECT handsets is also possible without a PBX component directly at the IP1200. Each handset is identified via its unique IPEI number. The effect of subscription to the telephone is that, as in LDAP, the subscription is stored in the telephone. There are two ways to register a telephone:

1. Entry of the IPEI number in the relevant user object; subscription at the telephone can then be performed (known subscription).
2. Subscription at the telephone is performed first (unknown subscription); the call number of the desired free user object is then dialled. The IPEI number is automatically entered in this user object.

4.2.1 Administration/DECT

DECT-related administrative settings of the IP1200 are made here.

4.2.1.1 Administration/DECT/Statistics

Detailed information about the DECT master and the DECT radios is displayed here. The Master section is hidden, however, if the Statistics submenu is viewed from a configured DECT radio.

Master section:

Calls in	All incoming calls on the DECT master.
Calls in Delivered	All incoming calls that were put through on the DECT master.
Calls Out	All outgoing calls on the DECT master.
Handover	All handovers that took place on the DECT master. If a mobile phone is located in the transmitting range of the DECT master and switches to a different transmitting range (DECT radio), a handover to the next transmitting range must take place, so that the DECT master knows how the voice data is to be routed.
Handover Failed	All failed handovers in the DECT master range.
Abnormal Call Release	All other failed calls. An example of such an **Abnormal Call Release** is a mobile phone battery that has become empty.

Radio section:

Calls in	All incoming calls on the DECT radio.
Calls Out	All outgoing calls on the DECT radio.
Handover	All handovers initiated on the DECT radios that took place. If a mobile phone is located in the transmitting range of a DECT radio and leaves it, a handover to the next transmitting range (radio or master) must take place, so that the DECT master knows where the voice data is to be transmitted to.
Handover Failed	All handovers initiated on the DECT radios that failed.

Finally, the total operating time of the DECT subsystem is displayed.

4.2.1.2 Administration/DECT/Users

All users configured on the IP1200 are listed here. If LDAP replication with the innovaphone PBX was established, the DECT users configured in the PBX are also diplayed here. It is possible to display individual, several or all users. To display a particular user, you must enter the user’s name (**Long Name**) in the field and then click *show*. You can also display several users by entering only the first letter of a user’s name in the field and then clicking *show*. Clicking *show* without entering a character string or letter displays all created users.

The display of the user data is organised in columns:

Long Name “Long Name” registered in the PBX

No Call number registered in the PBX

Name “Name” registered in the PBX

Display Assigned display

IPEI 12-digit IPEI number

AC It is possible to assign an access code (**AC**) to a user when setting up the user in the innovaphone PBX. It this was done, the access code is displayed here. See also the chapter titled „*Configuration/DECT/System*“.

Registration The current registration state. Possible states: *subscribing*, *pending* or *IP address* of the VoIP device, with which the user has registered.

To add a new user, you must click the *new* link next to the tabular display of the existing users.

4.2.1.3 Administration/DECT/Unknown

All subscriptions (unknown subscription) that are not yet assigned to a (PBX) user are displayed here.

- Clicking **Delete** deletes the unknown subscription from the list.
- Unknown subscriptions can dial the call number of a free user to register with this object.

4.2.1.4 Administration/DECT/Radios

All registered/unregistered DECT base stations are displayed row by row here. A row contains the following information: *Name ID Address Sync Lost Busy Product*

Version Uptime:

Name <*Device type*> + <*NetBIOS name*> for example, *IP1200-a1-a2-a3* (*the last three digits of the MAC address of the* DECT device).

ID The allocated radio ID of the DECT radio.

Address The IP address of the DECT radio. If a configured DECT radio is not accessible, the *del* link is displayed instead of the IP address and can be used to delete the DECT radio from the list.

Sync If the DECT device in question is the DECT master, the character string Master is output. If the DECT device in question is a DECT radio, the number of the radio ID by which the DECT radio has synchronised is output. It is output in green if the DECT device has already successfully synchronised. In the case of failure, this number is output in red.

Lost The first value in the **Lost** column relates to the **sync master** and specifies how often synchronisation to the DECT master was lost. The second value relates to the **alt sync master** and specifies how often synchronisation to the alternative DECT master was lost and therefore was entirely lost.

LDAP Displays the status of the respective DECT device. Possible states: *Up*, *Down*, *Starting* and *Stopped*, *Server* and *Replicator*.

Busy Displays how often all channels of a DECT radio were busy. This shows whether further DECT base stations are required.

Product Displays the name of the respective DECT device, in so far as it was configured in the **Device Name** entry field as described in chapter „*Configuration/General/Admin*". If no product name (**Device Name**) was configured, the standard name of the device is used (for example, innovaphone IP1200).

Version Displays the current firmware version of the respective DECT device.

Uptime Displays the operating time of the respective DECT device in the format *days hours minutes seconds*.

4.2.1.5 Administration/DECT/Mastercalls

The currently active calls carried out via the DECT master can be monitored. Here, it is to be noted that internal calls between innovaphone PBX subscribers are not displayed if the optional innovaphone PBX component is installed.

A	`<Sender>`	Calling subscriber
B	`<Receiver>`	Called subscriber

State	`Calling`
	`Alerting`
	`Connected`
	`Incomplete`
	`Disconnecting`
		Call is being set up
		Call is being signalled
		Call connected
		Call incomplete
		Call is being disconnected

Radio	`IP1200-xx-xx-xx`	The DECT system used.
Local Media	`xxx.xxx.xxx.xxx:xxxx`	The IP address and port of the DECT system used.
Remote Media	`xxx.xxx.xxx.xxx:xxxx`	The IP address and port of the VoIP device on which the innovaphone PBX component is enabled.

4.2.1.6 Administration/DECT/Radiocalls

The currently active calls carried out via the DECT radios can be monitored.

If no values or entries are transferred, the respective value is displayed with a dash (-).

DECT	`<Sender>`	Calling subscriber
Master	`<Receiver>`	Called subscriber

Handover	`Calling`
	`Alerting`
	`Connected`
	`Incomplete`
	`Disconnecting`
		Call is being set up
		Call is being signalled
		Call connected
		Call incomplete
		Call is being disconnected

4.2.1.7 Administration/DECT/Handover

The currently active calls that go via several DECT base stations can be monitored.

If no values or entries are transferred, the respective value is displayed with a dash (-).

4.2.1.8 Administration/DECT/Radio

In this menu, all DECT radios registered with the DECT master are displayed line by line.

Each line represents a DECT radio with specification of the RPN (**R**adio **P**art **N**umber) and the RSSI (**R**adio **S**ignal **S**trength **I**ndication):

RPN (Radio Part Number)	The Radio Part Number is the radio ID of the DECT radio.
RSSI (Radio Signal Strength Indication)	The Radio Signal Strength Indication is the field strength of the individual DECT radio.

4.2.2 Administration/Download

The configuration of the VoIP device can be backed up using this menu.

4.2.2.1 Administration/Download/Config

This function allows to save the current configuration of the VoIP device. When clicking the **Download** link, a popup page opens, in which it can be specified whether to save the configuration file as a txt file or immediately open it with an editor.

4.2.3 Administration/Upload

There are several ways to update the VoIP device.

> **Note**
>
> Detailed informations respectively the status display by the Ready LED while uploading files to the device can be found in the innovaphone knowledge-base article „*How to Reset IPXXX , factory default, led behaviour, tftp mode,clear config,gwload*" (`http://www.innovaphone.com/inno-kb`).

4.2.3.1 Administration/Upload/Config

This function allows you to load a saved configuration (see chapter entitled "*Administration/Diagnostics/Config Show*") onto the device.

By specifying path and file name of the configuration file to be loaded in the **File** field and then clicking the **Upload** button, the configuration file is loaded into the device.

Here, it is to be noted that the configuration file is loaded into the device's volatile memory. This means it is neither permanently backed up nor immediately operative. The device therefore must be briefly reset. More detailed information on resetting the device may be found in the chapter „*Administration/Reset*".

4.2.3.2 Administration/Upload/Firmware

This function allows you to manually upload a new firmware version onto the VoIP device. This can be automated by configuring an update server as described in the chapter "*Configuration/General/Update*". New firmware versions can be obtained from a certified innovaphone dealer or directly via the innovaphone homepage (`http://www.innovaphone.com`).

By specifying path and file name of the configuration file to be loaded in the **Firmware File** field and then clicking the **Upload** button, the configuration file is loaded into the device.

Whilst loading the new firmware, you are advised not to interrupt the loading procedure under any circumstances.

If the loading procedure is nevertheless interrupted, the device should under no circumstances be switched off afterwards. Rather the procedure should be repeated once the problem has been eliminated.

Take a 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, it must be ensured (if specified) that the required sequence of boot code and firmware update is observed.

The new firmware is not activated directly. A reset must be performed to activate the new version. The **immediate reset** and **reset when idle** links are provided for this purpose. More detailed information on resetting the gateway is contained in the chapter entitled "*Administration/Reset*".

4.2.3.3 Administration/Upload/Radio

This function can be used to load a new radio firmware version onto the VoIP device. New radio firmware versions can be obtained from a certified innovaphone dealer or directly from Kirk.

By specifying path and file name of the radio firmware to be loaded in the **Radio File** field and then clicking the **Upload** button, the radio firmware is loaded into the device.

It is necessary to ensure that all active calls are terminated as soon as the radio firmware is loaded onto the device.

Whilst loading the new radio firmware, you are advised not to interrupt the loading procedure under any circumstances.

If the loading procedure is nevertheless interrupted, the device should under no circumstances be switched off afterwards. Rather the procedure should be repeated once the problem has been eliminated.

The new radio firmware is not activated directly. A reset must be performed to activate the new version. The **immediate reset** and **reset when idle** links are provided for this purpose. More detailed information on resetting the device is contained in the chapter entitled "*Administration/Reset*".

4.2.3.4 Administration/Upload/Boot

This function can be used to load a new boot code version onto the VoIP device. New boot code versions can be obtained from a certified innovaphone dealer.

By specifying path and file name of the boot code firmware to be loaded in the **Boot File** field and then clicking the **Upload** button, the boot code firmware is loaded into the device.

Whilst loading the new boot code firmware, you are advised not to interrupt the loading procedure under any circumstances.

If the loading procedure is nevertheless interrupted, the device should under no circumstances be switched off afterwards. Rather the procedure should be repeated once the problem has been eliminated.

The new boot code is not activated automatically. A reset must be performed to activate the new version. The **immediate reset** and **reset when idle** links are provided for this purpose. More detailed information on resetting the device is contained in the chapter entitled "*Administration/Reset*".

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

4.2.4 Administration/Diagnostics

The **Diagnostics** menu can be used to monitor the operating state of the device.

4.2.4.1 Administration/Diagnostics/Logging

Using the **Syslog** link, the log messages of the device can be viewed directly in active operation. The messages are continuously automatically updated and are scrolled upwards, out of the window.

Only messages that were enabled in the **Logging** submenu are displayed. The following settings can be enabled:

TCP	All TCP connections.
PPP	All PPP connections.
Relay Calls	All calls that go via the Relay – only visible for devices with S_0 or S_2m interface.
Relay Routing	All calls that must be routed via the Relay – only visible for devices with S_0 and S_2m interface.
DECT master	All DECT master connections – only visible for IP DECT systems.
DECT radio	All DECT radio connections – only visible for IP DECT systems.
H.323 Registrations	All H.323 registrations.
SIP Registrations	All SIP registrations.
Config Changes	All configuration changes.
TEL1-n	All TEL1-n connections – only visible for devices with TEL interface.
PPP	All PPP connections – only visible for devices with PPP interface.

BRI1-n	All BRI1-n connections – only visible for devices with BRI interface.
PRI1-n	All PRI1-n connections – only visible for devices with PRI interface.

Clicking *OK* saves the settings made.

4.2.4.2 Administration/Diagnostics/Tracing

Using the **trace (buffer)** link, the trace information of the VoIP device can be viewed and saved. In the process, a text file *log.txt* is generated, which displays the current trace in a new browser window.

Using the **trace (continuous)** link, the continuous trace information of the device can be viewed and saved. In the process, a text file c*log.txt* is generated, which displays the current trace in a new browser window. As already mentioned, the messages are continuously automatically updated and are scrolled upwards, out of the window.

For both trace variants, only messages that were enabled in this menu are displayed. Not every section and not every setting is visible; this will depend on which device is being used.

DECT section:

System	Information on the DECT system.
Master	Information on the DECT master.
Radio	Information on the DECT radio.

Interfaces section:

PPP	Information on the PPP interface.
TEL1-n	Information on the TEL1-n interface.
BRI1-n	Information on the BRI1-n interface.
PRI1-n	Information on the PRI1-n interface.
prot	The **prot** check boxes after the individual interface settings give information on the protocol used.

VOIP section:

H.323/ RAS	Information on H.323 RAS.

H.323/ H.225	Information on H.323/H.225.
H.323/ H.245	Information on H.323/H.245.
H.323/ T.38	Information on H.323/T.38
H.323/ T.30	Information on H.323/T.30
SIP/Messages	Information on SIP/messages.
SIP/ Events	Information on SIP/events.
SIP/T.38	Information on SIP/T.38.
DSP	Information on DSP.
DSP con--trol mes--sages	Information on DSP control messages.
DSP data messages	Information on DSP data messages.

IP section:

PPP	Information on the PPP protocol.
PPTP	Information on the PPTP protocol.
PPoE0-1	Information on the PPoE0/1 protocol.
DHCP0-1	Information on the DHCP0/1 server.
HTTPCLI--ENT	Information on the HTTP client.
HTTPCLI--ENT ver--bose	Detailed information on the HTTP client.

Clicking *OK* saves the settings made.

4.2.4.3 Administration/Diagnostics/Config Show

Config Show enables the output of the current configuration of the VoIP device in text format.

The current configuration can also be saved in a file using the **Save Frame As** function (depending on the browser used). It is also possible to select (highlight) the entire text (Ctrl-A) and copy it to the Clipboard using the right mouse button and the context menu (or Ctrl+C). The configuration can now be copied into any text editor (Ctrl+V) and saved.

A configuration backed up this way can be fully or partially loaded again. In this way, the configuration can be backed up and restored, or reference configurations can be created and loaded onto a number of devices.

4.2.4.4 Administration/Diagnostics/Ping

It is possible to execute a **ping** on a particular destination host (**IP address**), since for test purposes it is often necessary to execute a ping command directly from the VoIP device. This makes it possible to check whether a network address (PC, printer, telephone, etc.) is accessible. If an address is accessible, `Reply from <host>` is displayed to the sender. If the address is not accessible, `No Reply from <host>` is displayed.

4.2.5 Administration/Reset

In addition to reset the device by the hardware reset button, there are three more ways given by the webbrowser, to reset the VoIP device.

> **Note**
>
> Informations to the reset function respectively the hardware reset button on device are contained in Appendix A „*Connectors and control elements*" inside Table 1 „*Indicators and Connectors*" („*Reset*").
> More detailed informations can be found in the innovaphone knowledgebase article „*How to Reset IPXXX , factory default, led behaviour, tftp mode,clear config,gwload*" (`http://www.innovaphone.com/inno-kb/`).

4.2.5.1 Administration/Idle Reset

With an **Idle Reset**, the VoIP device is reset as soon as no more active calls are being carried out.

4.2.5.2 Administration/Reset/Reset

With a normal **Reset**, the device is immediately reset. All active calls are lost.

4.2.5.3 Administration/Reset/TFTP

With a **TFTP Reset**, the VoIP device is transferred to TFTP mode. In this mode, the device can only be accessed with the GWLoad tool and thus allocated an IP address. Further information on the innovaphone GWLoad tool may be found in the innovaphone Knowledgebase.

Appendix A: Connectors and control elements

Indicators and connectors

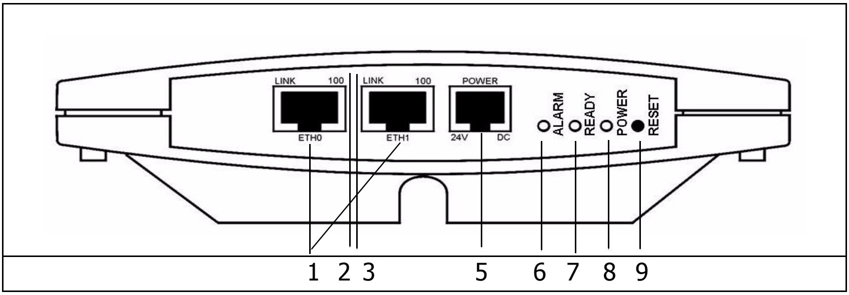


Fig. 1 - Indicators and connectors of the IP1200

Pos.	Symbol	Description and function
1	**ETH0-1**	RJ45-socket for connecting a 100 Mbps Ethernet (10/ $100_{\text{Base-T}}$ auto sense).
2	**100**	LED to indicate that the 100 Mbps network for the **ETH0/1** interface is active.
3	**LINK**	LED to indicate that data is being sent or received on the **ETH0/1** interface.
4	**POWER**	Socket for connecting an external plug-in mains adapter.
5	**ALARM LED**	LED to indicate that the IP1200 is carrying out a restart or that a malfunction error exists.
6	**READY LED**	LED to indicate that the IP1200 is ready for operation.

7	**POWER LED**	LED to indicate that the IP1200 has a power supply.
8	**RESET**	In addition to reset the device by the webbrowser, there are three (four) more ways given by the reset button, to reset the device. **Short Reset:** A short reset is restarting the device. Doing this will disrupt all active calls. **Middle Reset (TFTP-Reset):** The device is moving into TFTP-Mode, if holding the reset button until the Ready LED is blinking one-two times and then loose holding of the reset button. All ISDN-LEDs will be deleted and the Ready LED will be displayed in orange. **Long Reset (Factory-Reset):** Holding the reset button a longer time the Ready LED will blink 4-6 times and change to red. If loosing the hold on the reset button now, the deletion of the configuration is beginning. The Ready LED will be displayed 5 seconds in red and after that it will start to blink very fast in red-green and delete the display of all ISDN-LEDs. The device will go into TFTP-Mode and the Ready-LED will be displayed in orange. **Power-Cycle:** Means to disrupt the device from the power supply. Works technically and visually like the short reset.

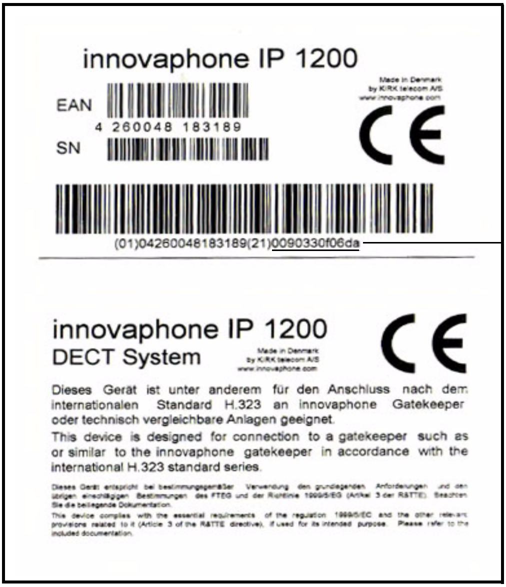
Table 1 Indicators and connectors of the IP1200

Note

Informations respectively the software reset function by the webbrowser are contained in capter „*Administration/Reset*“.
More detailed informations can be found in the innovaphone knowledgebase article „*How to Reset IPXXX , factory default, led behaviour, tftp mode,clear config,gwload*“ (`http://www.innovaphone.com/inno-kb/`).

The serial number label

The serial number label may be found on the device packaging and on the underside of the housing.



innovaphone IP 1200

EAN

4 260048 183189

SN

Made in Denmark
by KIRK telecom A/S
www.innovaphone.com

(01)04260048183189(21)0090330f06da

(**MAC address**)

innovaphone IP 1200
DECT System

Made in Denmark
by KIRK telecom A/S
www.innovaphone.com

Dieses Gerät ist unter anderem für den Anschluss nach dem internationalen Standard H.323 an innovaphone Gatekeeper oder technisch vergleichbare Anlagen geeignet.

This device is designed for connection to a gatekeeper such as or similar to the innovaphone gatekeeper in accordance with the international H.323 standard series.

Dieses Gerät entspricht bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen des FTEG und der Richtlinie 1999/5/EG (Artikel 3 der R&TTE). Beachten Sie die beiliegende Dokumentation.

This device complies 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. Please refer to the included documentation.

Fig. 2 - Serial number label of the IP1200

The MAC address is also the serial number of your IP1200.

The first three constant hexadecimal digits separated by a hyphen (`-´) are innovaphone's manufacturer identification code (009033 or 00-90-33), whilst the last three hexadecimal digits (0F06DA or 0F-06-DA) are the consecutive serial number of your IP1200.

Appendix B: Troubleshooting

In our experience, some problems occur more frequently than others. These problems are listed in Table 2 below, which also gives advice on how to solve them.

Typical problems

Symptom	Description	Action
The VoIP device does not respond. **Ready**, **Link** and **100M**. LEDs are permanently on.	The VoIP device is waiting for a firmware download.	• Perform a quick reset by pressing the **Reset** button.
The VoIP device does not respond. **Ready** LED is on, **Link** LED flashes irregularly.	The Ethernet connection is not working.	• Check the Ethernet cabling.
The VoIP device does not respond. **Ready** and **Link** LEDs are on, **100M**. LED flashes during attempted access.	The VoIP device has an incorrect IP address configured.	• Set the IP parameters correctly.
In the as-shipped state, the VoIP device does not assign an IP address to the PC.	When the device is turned on, the DHCP client is active.	• Press the Reset button briefly. • Have an IP address assigned to the PC again.
Calls can be established to a remote VoIP device, but no communication is possible.	The required bandwidth for the transfer of the voice data is not available.	• Configure a more efficient voice coding for the remote VoIP device.
Calls can be set up to a remote VoIP device, but no voice connections can be established.	The media channel cannot be set up, since the two VoIP devices do not have a common voice encoder.	• Make sure that the „*exclusive*" check box is disabled.

Calls can be set up to a remote VoIP device, but no voice connections can be established.	The media channel cannot be set up, since the two VoIP devices do not have a common voice encoder.	Only the media channel is set up directly between the two VoIP devices; all signalling connections are operated via the gatekeeper. • Make sure that both VoIP devices have a correct IP routing configuration, in particular subnet mask and standard gateway.
Calls to a remote telephony gateway are constantly rejected.	The device does not support overlapped sending.	• Add a hash (#) to the dial prefix of the route leading to this gateway to force en-bloc dialling.
The VoIP device 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 the non-volatile memory each time you make any changes.
The VoIP device is connected to the network behind a firewall and the configuration is not working.	The firewall does not allow access to the VoIP device.	• Enable VoIP device access for the service tcp/80 (http) in the firewall.
The VoIP device is connected to the network behind a firewall and no connections to other VoIP devices can be established.	The firewall does not support the H.323 protocol.	• Enable "*H.323 Firewalling*" in your firewall software and, if necessary, "*H.323 NAT*". Refer to your firewall documentation for this purpose. • See chapter "*NAT and firewalls*" for more information.

Table 2 Troubleshooting

NAT and firewalls

If there is a firewall protecting your network from the Internet and connections are to be set up to remote terminals via the Internet, then appropriate configuration of the firewall must be ensured.

Firewalls normally have two jobs. They control access to devices and network areas within your network and they implement the IP address translation in networks that do not have their own regular network address (NAT). 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 the firewall or router firmware.

If the product you are using does not have H.323 firewalling, there are two ways of proceeding:

- Release the path in the firewall for all required data to and from the VoIP device.

  Although this solution is usually not well received by network administrators, it does not present a security problem, since the VoIP device, as a dedicated device, does not perform any services other than Voice over IP. No security gaps are caused in a network by opening the path to and from the device.

  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.

  The following ports must 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
  - Udp: destination port >= `2050`, source port `5004` and `5005` (RTP), for VoIP calls

  The following ports should also be released if the RAS protocol is used:

  - Udp: destination port 1718
  - Udp: destination port 1719
  - Udp: source port 1719

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

- The device is placed in front of the firewall, so that the data stream does not have to pass the firewall. In this case, you will not be able to set up any voice connections from within the network to the device (for example, with innovaphone Softphone PCs).

If the network is operated in NAT mode and the product you are using does not support H.323 NAT, then it is not possible to operate beyond the firewall.

VoIP and heavily loaded WAN links

If voice data is transmitted over heavily loaded, narrowband WAN links, the voice quality can be affected if the respective links can no longer ensure adequate transmission quality.

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 you router is able to prioritise on the basis of the ToS field (**T**ype **o**f **S**ervice), you can use this function. The VoIP device sets the ToS Priority field to the value `0x10` for all IP packets that it sends. This value can be changed, if necessary, under the chapter "*Configuration/IP/Settings*" .

> **Tip**
>
> You can specify hexadecimal, octal or decimal values: the entries `0x10`, `020` and `16` are all equivalent. The value set for the ToS Priority field should be the same on all used devices.

If this is not the case, the function "*Prioritisation according to source/destination address*" can be used, if available. In this way, data packets from and to the device 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, you should check whether this interruption can be separately enabled. Some routers refers to this function, somewhat confusingly, as **interleaving**.

Appendix C: Support

If needed to enlist the support of a dealer, the following information should be ready:

- The full version details of the device. These details may be found on the welcome page of the device (see chapter entitled "*Configuration/General/Info*").
- A trace showing the error situation (see chapter entitled "*Administration/Diagnostics/Tracing*").
- The entire configuration as displayed by **Config Show** (see chapter entitled "*Administration/Diagnostics/Config Show*").
- The serial number, which may be found on the serial number label on the underside of the housing or on the welcome page of the device (see Appendix B "*Connectors and control elements*" or chapter "*Configuration/General/Info*").

Firmware upload

The innovaphone VoIP devices are not delivered with the latest firmware, which means that a firmware upload is usually necessary.

New firmware versions can be obtained in the download area (`http://download.innovaphone.com`) of the innovaphone homepage.

innovaphone homepage

The innovaphone homepage (`http://www.innovaphone.com`) contains all current service packs, boot codes, hot fixes, firmware updates, manuals, datasheets, etc. It is also possible to request the innovaphone newsletter to stay up to date with current innovaphone news.

In future, it will be possible to make complaints online via the innovaphone homepage. This enables a simpler and faster processing procedure.

Appendix D: Configuration of the update server

It is possible to update the firmware and configuration of a large number of innovaphone devices in a distributed environment by automated means.

This is done by storing the configuration and firmware information on a standard Web server, which in turn is called up the individual devices.

There are two modules in the device which work in tandem. The first is known as „UP0" and acutally executes the upload and download of configuration information as well as the download of updated firmware. UP0 is controlled by commands as detailed below.

The second module is known as „UP1". It serves to poll a given website for changed configuration information. If certain conditions are met, UP1 will issue commands to UP1 to perform the requested updates.

System requirements

- One or more Web server(s) accessible by the devices.
- The Web servers tested were MS IIS and the Apache server. It should, however, also work with all other common Web servers.
- For best results, the Web server should be able to manage a large number of simultaneous HTTP sessions. MS Personal Web Server, for example, is not a suitable Web server, since it manages a maximum of 10 simultaneous HTTP sessions.

Installation

To be able to transfer device configurations onto the Webserver, the latter must allow HTTP PUT requests. All other functions require HTTP GET authorisation.

Since all HTTP requests are executed unauthenticated, the Web server must allow anonymous reading and possibly also anonymous writing.

To allow HTTP PUT commands on a MS IIS, the *read* and *write* check box must be enabled in the configuration of the relevant virtual directory.

Configuration

Detailed information on how the URL parameter of the update server is configured on the innovaphone devices may be found in the chapter entitled "*Configuration/General/Update*".

Note here that the URL parameter must point precisely to the location of the file with the contained maintenance commands. It is also to be noted that this URL (just like all other URLs used by innovaphone devices) does not support host names. Therefore, a valid IP address always has to specified.

If the URL happens to end with a '/', then a standard file name based on the product description is used. If, for example, the URL is **`http://1.2.3.4/configs/`** , then it is extended in the case of an IP1200 as follows: **`http://1.2.3.4/configs/update-ip1200.htm`** . The product name is specified in the first line in chapter "Configuration/General/Info". The file extension is irrelevant here. The extension **`*.txt`** or **`*.htm`** or no file extension at all is possible. In relation to URL specifications, note that some Web servers differentiate between upper case and lower case letters.

Running maintenance

The update file is immediately read and also immediately executed. After a device restart, the update server is automatically queried periodically in accordance with the interval set.

When the maintenance file has been successfully received, it is executed sequentially. Theoretically, all commands that can be transmitted to the device in a Telnet session or that occur in a configuration file can be used in the maintenance file.

Maintenance commands

Additional commands implemented specially for the update server are available.

The maintenance file is executed every time (depending on the interval set), as soon as it is received.

Check command

In most cases, however, the maintenance file should be executed not every time as soon as it is received, but once only. Assuming that a secure configuration is to be loaded onto several devices, then it is best if this is done from one device. This can be achieved with the **`check`** command:

```
mod cmd UP1 check <final-command> <serial>
```

innovaphone devices have an internal variable that is initially empty (or empty if the device was reset with the standard settings) called UPDATE/CHECK. The **`check`** command compares the content of **`<serial>`** with the UPDATE/CHECK variable. If both match, all further processes of the maintenance file are terminated.

If they differ, the remaining processes are executed. When the last process has been executed, the UPDATE/CHECK variable is overwritten with the content of **`<serial>`**, and the content of **`<final-command>`** is executed. The following commands are usable content for **`<final-command>`**

- ireset: Resets the device as soon as it is not being actively used.
- reset: Resets the device immediately.
- iresetn: Resets the device as soon as it is not being actively used and a reset is required.
- resetn: Resets the device immediately if a reset is required.
- ser: Is a global variable and not a function.

Time command

Often it is preferred to perform such changes at particular times (for example, at night when no work is being done). This can be achieved with the **`times`** command:

```
mod cmd UP1 time [/allow <hours>]
```

The **`time`** command compares the current time with the content of **`<hours>`**. **`<hours>`** is a comma-separated list of specified hours, within which execution of the maintenance file is possible. If the content of **`<hours>`** with the restriction does not match, all further processes are terminated. The following hours are considered valid times, within which execution of the maintenance file makes sense.

```
mod cmd UP1 time /allow 12,22,23,0,1,2,3,4
```

With this command, execution of the maintenance file is allowed from 12:00 to 12:59 hrs and from 22:00 to 04:59 hrs. If the device does not have a time, all processes are terminated.

```
mod cmd UP1 time [/allow <hours>] [/initial <minutes>]
```

If the **`/initial`** parameter is set, no further commands are executed within the specified number of minutes **`<minutes>`**, once the device has been reset. This was implemented to avoid a firmware download and the overwriting of Flash memory during device installation.

```
mod cmd UP1 time /allow 12,22,23,0,1,2,3,4 /initial 6
```

With this specification, all processes of the maintenance file are suppressed within the first six minutes and within the valid times specified in the **/allow** parameter after every device restart. If the **/initial** parameter was set, new devices (or devices that were reset with the standard settings) can, after a restart, receive the maintenance file within the number of minutes specified in the **/initial** parameter, even if they lie outside the valid times as specified in the **/allow** parameter. This allows new devices to receive a current standard configuration quickly.

Prot command

To initiate a firmware update, the following command can be executed:

```
mod cmd UP0 prot <url> <final-command> <built-serial>
```

This command downloads new firmware (if available) from the specified URL onto the device. Finally, the **<final-command>** is executed.

innovaphone devices have an internal variable that is initially empty (or empty if the device was reset with the standard settings) called UPDATE/PROT. The **prot** command compares the content of **<build-serial>** with the UPDATE/PROT variable. If both match, no firmware is downloaded. If the UPDATE/PROT variable is not set (new devices or after a device restart), the content of **<build-serial>** is compared with the built number of the current firmware. Once the firmware has been successfully downloaded, the UPDATE/PROT variable is overwritten with the content of **<build-serial>** . Note that the **<build-serial>** parameter is not compared with the firmware version currently loaded. It is the responsibility of the administrator to keep this standard.

If the **<url>** parameter ends with a slash ('/'), a standard firmware file name is appended to the URL depending on the product description (for example, IP1200.bin for an IP DECT system).

```
mod cmd UP0 prot http://192.168.0.10/firm/ip1200.bin ireset
04-5656
```

The command

```
mod cmd UP0 prot http://192.168.0.10/firm/ ireset 04-5656
```

determines whether the firmware version 04-5656 was already installed. If this is not the case, the current firmware is downloaded from the address **`192.168.0.10/firm/ip1200.bin`**, the UPDATE/PROT internal variable is overwritten with 04-5656 and, finally, the device is reset as soon at it is not being actively used.

Boot command

With the **`boot`** command, the boot code is updated and this is done in the same way as with the **`prot`** command.

```
mod cmd UP0 boot <url> <final-command> <built-serial>
```

The command

```
mod cmd UP0 boot http://192.168.0.10/firm/ ireset 205
```

determines whether the boot code version 205 was already installed. If this is not the case, the current boot code is downloaded from the address **`192.168.0.10/firm/bootip1200.bin`**, the UPDATE/BOOT internal variable is overwritten with the version number of the downloaded boot code (205) and, finally, the device is reset as soon as it is not being actively used.

SCFG command

If the **UP0** interface is being used, then the device configuration can be stored on a Web server.

```
mod cmd UP0  scfg <url>
```

This command instructs the device to upload its current configuration to the **`<url>`**. This can be achieved with the HTTP PUT command. The **`url`** must be writable. The following constants can be used in the **`url`**:

Sequence	Replaces	Example
#d	Current date and time	20051010-170130
#m	MAC address of the device	00-90-33-03-0d-f0
#h	Device hardware number	IP1200-03-0d-f0

Example

A Web server exists at the address `192.168.0.10` with a subdirectory called **`configs`**. In this directory, there are two further subdirectories, in which the current firmware files for all innovaphone devices are stored.

Clients provide the DHCP server with the option #215 as `http://`

192.168.0.10/configs/. In this directory, there is a file **update-ip1200.htm** , which processes the following lines:

```
mod cmd UP1 times /allow 23,0,1,2,3,4 /initial 6
mod cmd UP0 scfg http://192.168.0.10/configs/saved/
#h.txt
mod cmd UP0 prot http://192.168.0.10/configs/04-5679 /
ser 04-5679
mod cmd UP1 check ser 20040330-01
config change PHONECFG0 /coder G729A,60, /lang eng /
protect
config change PHONEAPP0 /f4-10 BellOff /f4-v0 %1BE /f5-
10 BellOn /f5-v0 %1BF
config write
config activate
iresetn
```

There is also the file **update-ip3000.htm**, which reads the following two lines:

```
mod cmd UP1 time /allow 23,0,1,2,3,4
mod cmd UP0 prot http://192.168.0.10/configs/04-5679 /
ser 04-5679
```

This example demonstrates how the configuration of a device is stored on a Web server; all IP1200 devices are then instructed to load/update the firware version 04-5679 in the time period 23:00 hrs to 04:59 hrs. New devices are updated after a restart and after the specified six minutes have elapsed. The devices are configured so that they use the G729 codec with a frame size of 60ms, the language setting is English and the configuration is write-protected. Therefore, only an administrator with appropriate authorisation can change this file. In addition, two standard functions were programmed for the device.

IP3000 devices are updated to firmware version 04-5679 in the time period 23:00 hrs to 04:59 hrs.

Appendix E: Configuration of an NTP server/ client

If a network does not have an NTP server, a public time server can be used. The TU Berlin, for example, provides a time service at the IP address `130.149.17.21`. This service is a voluntary service, and no claims can be made with regard to its availability.

Any Windows server can operate as the NTP server. Equally, there are various NTP software packages for Windows and Unix/Linux platforms.

The innovaphone VoIP devices also work simultaneously as NTP servers. If several devices are being used, one device can synchronise with a time server (external if need be), and all other devices, in turn, can synchronise with this one device.

The VoIP device will then operate as the time service and will transmit the correct time to the other devices. The synchronisation of all devices with one external time service should be avoided, since this results in unnecessary high loads on these servers.

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

Timezone strings (TZ string):

Time services always provide the coordinated world time UTC (**U**niversal **T**ime **C**oordinated), which corresponds to GMT (**G**reenwich **M**ean **T**ime), not however the correct time zone and summer time. It is therefore possible to specify the time difference between the time zone and the world time in the **String** 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.

If a so-called timezone string was entered in the **String** field, the device can make the switch from summer to winter time automatically. 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 field.

There are various formats for the specification of this string. These formats are defined by the IEEE POSIX standard.

POSIX timezone strings have the following format (optional parts in square brackets):

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

`Std` stands for the time zone (for example, `CET` for **C**entral **E**uropean **T**ime or `MET` for **Middle European Time**).

`Offset` specifies the time difference between the time zone and UTC, for example, **`-1`** for Central European Time. The difference is negative if the time zone is ahead of UTC. If the time difference does not comprise full hours, the number of minutes can be added, for example, **`-1:30`**.
The TZ string ends here if you are not using a summer time.

`Dst` stands for the summer time zone (for example, `CEST` for **C**entral **E**uropean **S**ummer **T**ime or `MES` for **M**iddle **E**uropean **S**ummer **T**ime).

The optional, second **`Offset`** parameter gives the offset of the summer time in respect of UTC. An hour before normal time is assumed if no entry is made.

Date/Time, Date/Time define the start and end of summer time. The format for a time entry is **`Mm.n.d`**, signifying the **`d`**-th day of the **`n`**-th week of the **`m`**-th month. Day **`0`** is Sunday. If the fifth week is entered, the last day (with respect to **`d`**) of the month is meant. The format for a time entry is **`hh[:mm[:ss]]`**, in the 24-hour format.

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

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

Further information on the POSIX standard can be called up on the Web at `http://standards.ieee.org/catalog/olis/posix.html`.

Appendix F: Instructions for downloading licences

Call up the page `http://www.innovaphone.com/index.php?id=29&L=0`. The licence agreement is displayed, which must be confirmed with *Yes*.

Login

The login screen is then displayed. If no licences have yet been downloaded from innovaphone, the Help pages should be readed first.

Otherwise, enter a valid e-mail address in the E-mail field and a relevant password in the Password field.

Download

Whether if logged in correctly it's displayed in the upper part of the screen. The following text appears: "*Welcome you are logged in as Name { e-mail address }*".

Beneath this, in the empty *Serial number* field, the serial number (MAC address) of the device for which licences are required can be entered and searched for.

Clicking the *Download Licence* button downloads the licences.

Result

If clicking the download link, an "*Open With / Save As*" dialog box opens, in which it can specified whether to save the file on the local hard disk or open and view it immediately.

The licences are also administered automatically in the licence manager, so that they can be downloaded anew at any time.

License Manager

The License Manager gives the possibility to manage all licenses and activation keys.

Appendix G: DECT coverage

One of the most important prerequisites for a professional DECT installation is DECT radio on-site measurement. This is ultimately the only way to determine how many locations must be equipped with DECT base stations and repeaters. innovaphone AG provides a mobile DECT installation tool for carrying out this measurement without the prior installation of a DECT environment. This tool can be lent or leased, and is thus a cost-effective way to bring a professional DECT environment into operation.

Further information on DECT coverage may be found in the following articles in the innovaphone knowledgebase:

Rules for successful IP1200 deployment - `http://www.innovaphone.com/inno-kb/article.aspx?id=10531`

Debugging tools for DECT deployment - `http://www.innovaphone.com/inno-kb/article.aspx?id=10536`

Understanding DECT handover with ip1200 - `http://www.innovaphone.com/inno-kb/article.aspx?id=10533`

The innovaphone knowledgebase contains information on further DECT topics, which can be called up with the search term *DECT*.

Appendix H: Glossary

This glossary relates to all innovaphone gateways, including innovaphone DECT gateways:

A

A-law

The A-law method is a method for the dynamic compression of audio signals, which is described in the ITU G.711 recommendation. The dynamic compression improves the signal-to-noise ratio under equivalent transmission conditions. The method uses a logarithmic dynamic characteristic curve, which has high dynamics particularly at low input levels and very low dynamics at high input levels. This reduces the noise at low input levels, that is, for quiet sounds. The A-law method is used mainly in Europe; the USA uses a method that differs slightly in the quantisation levels, the µ-law method. This method is characterised by a dynamic characteristic curve that, in the low level range, is even steeper than that of the A-law method.

Alt sync master

An alternative synchronisation source.

ARI

An ARI (**A**ccess **R**ights **I**dentifier) is a unique identifier for a DECT system.

ARP

The ARP protocol (**A**ddress **R**esolution **P**rotocol) is a typical ES-IS protocol (**E**nd **S**ystem - **I**ntermediate **S**ystem **P**rotocol) used to covert the MAC addresses (**M**essage **A**uthentication **C**ode) to the relevant IP addresses (**I**nternet **P**rotocol) to enable communication on the network layer using the IP protocol. The ARP protocol creates mapping tables for this purpose, which assign the MAC addresses to the network addresses.

Auto-MDX

The Auto-MDX function is the automatic detection of an uplink port on an Ethernet interface. No crossover cables are required with the Auto-MDX function, since the Ethernet interface can automatically switch the send and receive line.

B

BRI

The basic access (BA), also referred to as the BRI interface (**B**asic **R**ate **I**nterface), is the standard access to the ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork). A basic access offers two speech/data channels (B channels, derived from "bearer") each at 64 kbit/s and a signalling channel (D channel, derived from "data") at 16 kbit/s. The net bandwidth is: 2 × 64 kbit/s + 16 kbit/s = 144 kbit/s. The basic access is used mainly by private customers or smaller businesses; larger companies with a high level of telephone activity use the primary multiplex access.

Broadcast

A broadcast transmission is simultaneous transmission from a single point to all subscribers. In order to address particular classes of receivers or all connected stations simultaneously in a network, the possibilities of multicast or broadcast exist. In local networks, a broadcast is a message that is sent to all devices in all networks. It is forwarded by every router to all connected networks. If all terminals in a particular network are to be addressed, one refers to multicast or network broadcast.

C

CCFP

CCFP (**C**entral **C**ontroller **F**ixed **P**art) is a unit that controls all base stations. Previously (with the ip1500), the DECT base stations were connected via a proprietary interface with the CCFP using 2-wire cable.

With the IP1200, the DECT base stations are connected via IP with the CCFP interface. Every IP1200 has a DECT base station and a control unit. In a *multicell* installation, only one control unit of an IP1200 is used (also known as the IP master). All other DECT radios are controlled by it. The DECT radio in this master IP1200 can be used (usually it is used as a normal DECT radio; only if the IP DECT system uses more than 64 base stations, should the DECT radio in the IP master not be used).

CDR

The term CDR (**C**all **D**etail **R**ecord) is used in relation to the recording of all connections in a database. The recorded data is available for subsequent activities, such as the calculation of connection charges or the network analysis. CDR files are used in fixed networks, in IP networks in relation to IP telephony and also in mobile networks. In selected virtual connections, CDRs contain the call number, the name of the remote communication computer, the date and time, the connection duration and the error messages.

CFB

With the ISDN feature CFB (**C**all **F**orwarding **B**usy), an incoming call is forwarded to a particular extension when the line is busy.

CFNR

With the ISDN feature CFNR (**C**all **F**orwarding **N**o **R**esponse), an incoming call is forwarded to a particular extension if the call is not accepted after a configured time.

CFU

With the ISDN feature CFU (**C**all **F**orwarding **U**nconditional), an incoming call is forwarded to a particular extension immediately.

CHI

An information element in GSM networks that specifies the channel to be used on the user network interface.

CR

Because, with ISDN, a terminal can control several connections simultaneously, the individual connections are uniquely identifiable through the connection identifier. Each connection therefore uses its own CR (**C**all **R**eference). For outbound connections, it is allocated by the terminal, for inbound connections by the network.

CTI

CTI (**C**omputer **T**elephony **I**ntegration) is a value-added service for raising efficiency in voice transmission. With this service, very simple applications, such as computer-aided call number dialling, through to complete call centres can be offered as services. The purpose of CTI is to support the telephone service through computer technology. As well as the support of service features with their diverse switching functions, this includes management of the telecommunications system and the user accounts.

D

DECT

DECT (**D**igital **E**uropean or **E**nhanced **C**ordless **T**elecommunications) is a European standard for cordless telephony. DECT defines the air interface between the mobile hand device and the base station; voice transmission as well as data transmission are supported with flexible transmission speeds.

DECT base station

A DECT base station can set up a voice channel between an IP DECT telephone and the innovaphone PBX.

DECT controller

Short for CCFP (**C**entral **C**ontroller **F**ixed **P**art).

DECT system

A collection of DECT radios with a control device. All DECT radios in this system share a usual identifier (the so-called ARI). A handover between DECT radios is only possible within the same IP DECT systems.

DHCP

The DHCP protocol (**D**ynamic **H**ost **C**onfiguration **P**rotocol) enables the dynamic assignment of an IP address and further configuration parameters to computers in a network (for example, Internet or LAN) using a relevant server.

DMS100

The obsolete DMS 100 protocol (**D**igital **M**ultiplex **S**ystem) of Northern Telecom (USA) is the forerunner of the NI-1 protocol.

DNS

The DNS protocol (**D**omain **N**ame **S**ystem) is a protocol for the conversion of IP addresses to domain addresses. It belongs to the group of name services, within which the long, complicated IP addresses represented in

DDN (**D**otted **D**ecimal **N**otation) are replaced by simple domain names. The conversion of IP addresses to a domain address can take place using host tables, as well as using the worldwide DNS, in which the name servers are set up hierarchically.

DSL

Using DSL (**D**igital **S**ubscriber **L**ine), private households and companies can send and receive data at high transfer rates (1,000 to 16,000 kbit/s). This is a considerable improvement compared with modem or ISDN connections (only up to 64 kbit/s). No changes have to be made to the laid telephone line, since DSL uses the existing two to four copper wires of the telephone network on a different, higher frequency.

E

E.164

E.164 numbering is the most commonly used addressing standard in public communication networks. This call number schema forms the set of rules for the international call numbers.

The call numbers in E.164 comprise a maximum of 15 decimal places, which can be evaluated by public networks. Subscriber-specific call numbers and services can have a further 40 decimal places added. These are recorded only by private branch exchanges and end systems, however.

E-DSS1

The DSS1 protocol (**D**igital **S**ubscriber **S**ignalling System No. **1**) is at times referred to as the E-DSS1 protocol, where the "E" stands for Euro ISDN.

ENUM

ENUM (T**e**lephone **Num**ber **M**apping) is a technique for standardising the various communication and telephone addresses. It applies to private and business telephone, fax and mobile phone numbers, as well as to Web pages, short message services, instant messaging and e-mail. The ENUM protocol links together the resources from the telecommunication networks and from the Internet, and defines how a telephone number is mapped on a domain address. The telephone numbers are integrated in the DNS (**D**omain **N**ame **S**ystem). For the conformance of the telephone numbers to the international call number plan, there is the ITU E.164 standard.

F

FTY

FTY or FIE (**F**acility **I**nformation **E**lement) is the most important element in an ISDN for call signalling, registration and everything regarding the supplementary services.

5ESS

5ESS (**5**th version of AT&T's **E**lectronic **S**witching **S**ystem). Just as on the ISDN accesses that use the US national D channel protocol NI1, merely data transfers at a speed of 56 kBit/s (compared with 64 kBit/s for DSS1 and 1TR6) are possible. The remaining 8 kBit/s are used to transfer the control data, since the two protocols do not support a separate D channel. Furthermore, many of these accesses have only one B channel.

FTP

The FTP protocol (**F**ile **T**ransfer **P**rotocol) is used for file transfer between various systems and for simple file handling. FTP is based on the TCP transport protocol (**T**ransmission **C**ontrol **P**rotocol), and supports the transfer of character-coded information and of binary data. In both cases, the user must have the possibility to specify the format in which the data is to be stored on the respective destination system. The file transfer is controlled from the local system; access authorisation for the destination system is checked for the connection setup by means of user identification and password.

G

GAP

GAP (**G**eneric **A**ccess **P**rofile) is the basic DECT profile and applies to all DECT portable and fixed parts that support the 3.1 kHz telephony service irrespective of the type of network accessed. It defines a minimum mandatory set of technical requirements to ensure interoperability between any DECT GAP fixed part and portable part. This profile has been established by ETSI as an important part of a set of DECT profiles. Every DECT device must support one or more profiles to be functional.

GMT

GMT (**G**reenwich **M**ean **T**ime) is the mean solar time at the Greenwich Meridian. GMT was the world time from 1884 to 1928. It has since been replaced in this function by the coordinated world time UTC (**U**niversal **T**ime **C**oordinated).

H

Handover

The process that take place when a DECT handset switches from one DECT radio to another during a call.

Handset

A DECT handset is a cordless telephone.

HLC

HLC (**H**igh **L**ayer **C**ompatibility) is an information element in an ISDN, with which the protocols and parameters that are used in layers 4 to 7 of the speech/data channels are displayed.

H.225

H.225 is a signalling protocol standardised by the ITU-T (**I**nternational **T**elecommunication **U**nion-**T**elecommunications), which is used in H.323 networks and which supports the transfer of data, voice and video. The protocol is used for the connection setup and shutdown, as well as for connection control. Within the protocol, signalling is based on Q.931.

H.225 uses the RTP protocol for the real-time transfer of the multimedia data.

H.323

H.323 is an international ITU standard (**I**nternational **T**elecommunication **U**nion) for voice, data and video communication using packet-oriented networks, which defines the specific capabilities of terminals in the IP environment. H.323, which is functionally comparable to the SIP protocol, was developed for the transmission of multimedia applications and forms the basis for VoIP. Real-time communication in LANs is defined using this standard.

The H.323 standard consists of a whole series of protocols for signalling, the exchange of terminal functions, connection control, the exchange of status information and data flow control. The standard has been revised several times; in the third version, it defines the transfer of features. The standard is derived from the H.320 multimedia standard for ISDN.

H.245

The H.245 protocol standardised by the ITU (**I**nternational **T**elecommunication **U**nion) negotiates terminal functions, the control of logical connections for the transfer of audio data, flow control and the transfer of further control messages in H.323 networks. In relation to the terminal functions, H.245 uses the setting of the voice encoding method, which must be identical to the compression method.

I

IEEE

The IEEE (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) is an association of American engineers dedicated to standardisation tasks. Work group 802, for example, is driving forward the standardisation of local networks.

IP

The task of the IP (**I**nternet **P**rotocol) is to transport data packets from a sender to a receiver across several networks. The transmission is packet-oriented, connectionless and non-guaranteed. Even in the case of identical senders and receivers, the IP datagrams are transported by the IP as independent data packets. IP guarantees neither the observance of a particular sequence nor delivery to the receiver, that is, datagrams can be lost due to network overload, for example.

IPEI

DECT telephones (handsets) have such an IPEI number (**I**nternational **P**ersonal **E**quipment **I**dentity), which can also be regarded as a serial number and is used for identification in a DECT system.

IP master

The IP1200 that controls all other DECT base stations in an IP DECT system is often referred to as the IP master. It is possible that it is the same DECT base station as the sync master.

ISDN

ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork) was conceived as a communication network for voice transmission (recognisable from the transmission speed of 64 kbit/s), and has emerged from the analogue telephone network. The digital transmission enables text, graphics and voice data to be handled in the same way. Just as in the analogue telephone network, ISDN uses line switching, and a transparent, physical, end-to-end connection is set up if necessary. The result is virtually a physical line between the communicating end-subscribers, which is switched through in the individual ISDN exchanges.

ITU

The ITU (**I**nternational **T**elecommunication **U**nion) is an organisation operating worldwide, in which governments and the private telecommunications sector coordinate the setting up and operation of telecommunication networks and services.

J

Jitter

Jitter refers to the phase fluctuations in data transmission, and therefore changes in time of signal frequencies. It concerns fluctuations of fixed points in time, for example, the time when a digital signal passes from one signal amplitude to another. Jitter occurs especially with high frequencies and can result in data losses. The causes of jitter are noise and crosstalk, interference, signal edge distortion and minimal level fluctuations.

K

L

LAN

A LAN (**L**ocal **A**rea **N**etwork) usually spans a distance of up to 10 km, although there are networks that can cover much larger distances. It is normally implemented as a diffusion network and achieves transfer rates of up to 10 Gbit/s (10 Gigabit Ethernet). LANs can be wired (like the standardised local networks Ethernet, Token Ring and FDDI) or wireless (like the WLANs according to 802.11).

LDAP

The LDAP protocol (**L**ightweight **D**irectory **A**ccess **P**rotocol) is a directory access protocol based on TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). On the Internet and in intranets, it has become the standard solution for accessing network directory services for databases, e-mail, storage areas and other resources. LDAP offers a uniform standard for DS (**D**irectory **S**ervice).

M

MAC

The MAC address (**M**edia **A**ccess **C**ontrol) is the hardware address of each individual network adapter, and is used for unique identification of the device in the network. The MAC address is assigned to the data link layer (layer two) of the OSI model. To connect the data link layer with the network layer in the case of Ethernet, for example, the ARP protocol (**A**ddress **R**esolution **P**rotocol) is used.

MIB

A MIB (**M**anagement **I**nformation **B**ase) is a kind of table, which defines which information can be called up. The MIB of an agent (host, router, access point, etc.) is specified by the manufacturer. The task of this MIB is to store and save the transmitted information and data in the agent. By deploying MIBs, the agents can be monitored and administered using SNMP (**S**imple **N**etwork **M**anagement **P**rotocol).

MOH

With MoH (**M**usic **o**n **H**old), music is played in all common PABX systems whilst a call is on hold.

MPPE

The MPPE protocol (**M**icrosoft **P**oint-to-**P**oint **E**ncryption) is used to encrypt PPTP data packets. For this purpose, the MPPE protocol offers a 40-bit key length (international version) and a 128-bit key length (US version). Data encoding is based on RSA 4 Stream Cipher (RC4). In the case of the 128-bit key, a 64-bit part of the key is changed for each new session to raise security.

MSN

An MSN (**M**ultiple **S**ubsciber **N**umber) is a feature of Euro ISDN. It is a multiple subscriber number for multi-device access. In an ISDN, any ten free call numbers (maximum) can be allocated from the call number volume of the respective access area for the multi-device access. Each terminal can therefore be assigned an individual call number. An ISDN terminal or a PABX system can also be assigned several call numbers. On the other hand, several devices on the passive bus can be connected via one multiple subscriber number.

MTU

An MTU (**M**aximum **T**ransmission **U**nit) is the largest possible data unit or frame length that can be transmitted via an existing physical transmission medium or via a LAN/WAN path. If larger frame lengths occur, they are either fragmented according to the protocol rules used, or the frame is discarded. WANs generally have smaller MTU sizes than LANs.

Multicast

Multicast is a mode of transmission from a single point to a group. In relation to multicast, one also refers to a multipoint connection. The benefit of multicast is that messages are transferred simultaneously to several subscribers or closed user groups via one address. As well as the multicast connection, there is the point-to-point connection and broadcast transmission.

N

NAT

NAT (**N**etwork **A**ddress **T**ranslation), in computer networks, is a method for replacing an IP address (**I**nternet **P**rotocol) in a data packet with a different one. Often this is used to map private IP addresses to public IP addresses. If the port numbers are also being altered, one refers to masking or PAT (**P**ort **A**ddress **T**ranslation).

Usually, NAT is performed at a transition between two networks. The NAT service can run on a router or firewall, or on a different specialist device. Therefore, a NAT device with two network adapters can connect the local private network with the Internet, for example. NAT is divided into two types: Source NAT, which is where the source IP address is replaced, and Destination NAT, where the destination IP address is replaced.

NBTSTAT

Displays NetBIOS over TCP/IP protocol statistics (NetBT), NetBIOS name tables for local and remote computers and the NetBIOS name cache. Nbtstat allows a refresh of the NetBIOS name cache and the names registered in WINS (**W**indows **I**nternet **N**ame **S**ervice).

NI

NI1 is the national ISDN protocol used in the United States for the D channel. Some telecommunication companies still use the older 5ESS protocol. Compared with the European DSS1, NI1 and 5ESS differ primarily in the transmission speed. In both cases, merely data transfers at a speed of 56 kBit/s are possible. The remaining 8 kBit/s are used to transfer the control data, since the two protocols do not support a separate D channel. Furthermore, many of these accesses have only one B channel.

NMBLOOKUP

With nmblookup, NetBIOS names can be queried under Linux using NetBIOS over TCP/IP.

NTP

The NTP protocol (**N**etwork **T**ime **P**rotocol) is a standard for synchronising clocks in computer systems over packet-based communication networks. NTP uses the connectionless network protocol UDP (**U**ser **D**atagram **P**rotocol). It was specially developed to allow a reliable time specification over networks with a variable packet runtime.

O

OSI

The OSI reference model (**O**pen **S**ystems **I**nterconnection) is a layer model for the communication of open, information processing systems. It comprises standardised methods and rules for the exchange of data. The OSI model has been developed since 1979 and has been standardised by the ISO. It is used as the basis for a series of manufacturer-independent network protocols, which are used almost exclusively in the transport network in public communication technology.

P

PL

PL (**P**acket **L**oss) occurs during packet-based data transfer in networks. Packet loss can occur in various layers of the OSI model.

PCM

PCM (**P**ulse **C**ode **M**odulation) is an ITU standard for the digitization of voice, which is described in G.711. With this type of modulation, analogue signals are converted to discrete-time and discrete-value binary signals through quantisation.

In voice transmission, the PCM technique is used to convert an analogue voice signal to a digital signal based on Nyquist's sampling theorem. For this, the analogue signal is sampled 8,000 times per second and is converted to an 8-bit number, so that a sample value arises every 125 µs. The resulting transfer speed is 64 kbit/s, the transferable voice frequency 4 kHz.

For the dynamisation of voice, the ITU within G.711 has defined two methods for the dynamic compression: the µ-law method and the A-law method.

PING

The ping program (**P**acket **I**nter**n**et **G**rouper) can be used to check whether a particular host in an IP network is accessible and what its response time is.

POE

PoE (**P**ower **o**ver **E**thernet) describes a technology, with which network-enabled devices can be supplied with power over the 8-wire Ethernet cable.

POSIX

POSIX (**P**ortable **O**perating **S**ystem **I**nterface for Uni**X**) is a standardised application-level interface jointly developed by the IEEE (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) and the Open Group for Unix. It represents the interface between application and the operating system.

PP

PP (**P**ortable **P**art) is used as a synonym for a cordless telephone (handset).

PPP

The PPP protocol (**P**oint-to-**P**oint **P**rotocol) is conceived as the protocol for dialling into the Internet over line-switched networks. The PPP protocol allows data transmission over synchronous and asynchronous switched and dedicated lines. Consequently, it is capable of operating independently of the respective physical interface. The only prerequisite for using the PPP protocol is a fully transparent, fully duplex data line.

PPPOE

PPPoE (**P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet) is the use of the PPP network protocol (**P**oint-to-**P**oint **P**rotocol) over an Ethernet connection.

PPTP

The PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) is a protocol developed by a vendor consortium (Ascend Communications, Microsoft Corporation, 3Com, inter alia) for the creation of a VPN (**V**irtual **P**rivate **N**etwork). It allows the PPP (**P**oint-to-**P**oint **P**rotocol) to be tunnelled through an IP network; the individual PPP packets, in turn, are encapsulated in GRE packets (**G**eneric **R**outing **E**ncapsulation). To secure the data transfer, PPTP has a 40-bit or 128-bit RC4 algorithm (**R**ivest **C**ipher).

PRI

PRI (**P**rimary **R**ate **I**nterface) is the access provided for medium to large private branch exchanges, and offers much higher transfer speeds compared with the basic access. It allows subscriber equipment to be connected to the ISDN local exchange. A maximum information capacity of 30 basic channels each at 64 kbit/s, as well as a D channel with a capacity of 64 kbit/s are available to the end-user via the S2M interface.

Q

QOS

QoS (**Q**uality **o**f **S**ervice) refers to all procedures that influence the data flow in LANs (**L**ocal **A**rea **N**etworks) and WANs (**W**ide **A**rea **N**etworks) so that the service arrives at the receiver with a defined quality.

QSIG

QSIG (**Q** Interface **Sig**nalling Protocol) is based on the D channel protocol according to the ITU-T standard (**I**nternational **T**elecommunication **U**nion-**T**elecommunications) of the Q.93x series for basic call and of the Q.95x series for the supplementary services. This ensures that QSIG and ISDN are compatible in their features, and that ISDN applications or supplementary services of the public ISDN networks can also be used in a private network.

Q value

An indicator for the transmission quality in a DECT call set up. Also referred to as Q52 value.

Q.931

Q.931 is the protocol standardised by the ITU (**I**nternational **T**elecommunication **U**nion) for the signalling in the D channel of Euro ISDN. It is used for the connection setup and shutdown, as well as for connection control.

R

Radio

A DECT radio is either a DECT base station or a repeater.

RC4

The encryption algorithm RC4 (**R**ivest **C**ipher) is a symmetric encryption method, in which the key is generated by a random number generator. RC4 works with a secret key that is know to the sender and receiver. The variable key length can be up to 2,048 bits. Each character is individually encrypted. Despite being relatively simple, RC4 is regarded as very secure.

Repeater

A DECT radio with no direct connection to the CCFP. It requires access (either direct or indirect) to a DECT base station, which provides a channel to the PBX. A repeater increases the coverage area of the IP DECT system, but not the maximum possible number of calls made simultaneously.

A repeater requires a synchronisation source (just like every other DECT radio). The DECT radio used as the synchronisation chain is likewise used to obtain access to the voice channel of the PBX. This means that calls that go via a repeater are always handled via the repeater sync source.

Repeater chain

If a repeater has another repeater specified as the synchronisation source, one refers to a repeater chain. None of the DECT radios in a repeater chain can be specified as the synchronisation source for an IP1200 DECT radio. For repeater chains, special rules apply.

RFC

Specifications, suggestions, ideas and guidelines concerning the Internet are published in the form of RFCs (**R**equest **F**or **C**omments).

RFP

RFP (**R**adio **F**ixed **P**art) is used as a synonym for DECT base stations.

RJ

RJ connectors have gained market acceptance worldwide for UTP cable (**U**nshielded **T**wisted **P**air), particularly in workstation cabling and in jumpering. With improved HF transmission properties (**H**igh **F**requency), RJ connector systems are used both in telecommunications and for networks, including ATM (**A**synchronous **T**ransfer **M**ode) and Gigabit Ethernet (RJ-45). The best-known RJ connectors are RJ-10, RJ-11, RJ-12 and RJ-45, which differ in the number of contacts.

Roaming

The ability of a DECT telephone to operate in more than one IP DECT system (in various locations). For this, the DECT telephone must be registered in all IP DECT systems.

RT

RT (**R**ound **T**rip) is the response time of a complete network. It is the time interval required to send a signal from a source to the receiver over the network and to transport the receiver’s reply back to the sender over the network again. The round trip time is used in some routing algorithms to determine the optimum route.

RSA

RSA (**R**ivest **S**hamir **A**dleman) is an asymmetric method or algorithm for encrypting discrete data, which uses various keys for encrypting and decrypting. Here, the key for decryption is not computable from the key for encryption (or is computable only with considerable effort). The key for encryption can therefore be published. Such methods are referred to as asymmetric or public key methods. It is named after its inventors Ronald L. Rivest, Adi Shamir and Leonard Adleman.

RTP

The RTP protocol (**R**eal-Time **T**ransport **P**rotocol) is a protocol for the continuous transmission of audiovisual data (streams) over IP-based networks. It is used to transport multimedia data streams (audio, video, text, etc.) over networks, that is, to encode, packet and send the data. RTP is a packet-based protocol and is normally operated via UDP. RTP is used for the negotiation and observance of QoS parameters (**Q**uality **O**f **S**ervice). It is applied in many areas, for example, it is used in the IP telephony technologies H.323 and SIP (**S**ession **I**nitiation **P**rotocol) to transfer the audio/video streams of the call.

S

SC

A telephone call is made up, for the most part, of pauses. It would be unnecessary to operate at the full data rate in these time slots. Codecs, such as the G.723.1 or the G.729, therefore contain an SC feature (**S**ilence **C**ompression). Essentially, this feature consists of three components: VAD, DTX and CNF.

The task of VAD (**V**oice **A**ctivity **D**etector) is to determine when a subscriber is speaking and when he/she is silent. For this, the algorithm must respond quickly to prevent the first syllable being lost after such a silence. To reliably differentiate between conversation and silence, the codec requires a buffer which causes an additional delay.

DTX (**D**iscontinuous **T**ransmission) allows a codec, in theory, to interrupt the connection if VAD has detected silence. Because an interruption of this kind would mean absolute silence on the call party side, the connection is not really completely interrupted. Rather a small set of data is transferred, which allows the generation of background noise on the receiver side.

CFG (**C**omfort **N**oise **G**enerator) starts precisely at this point. It is capable of generating background noise independently. For this, it uses the background noise that existed for the previous conversation phase.

SNTP

The SNTP protocol (**S**imple **N**etwork **T**ime **P**rotocol) is used for the transmission of an official time in networks and in the Internet. The extended variant is called NTP (**N**etwork **T**ime **P**rotocol).

SNMP

The **S**imple **N**etwork **M**anagement **P**rotocol allows central network management for many network components. The primary objectives of SNMP are a reduction in the complexity of the management functions, the extensibility of the protocol and independence of any network components.

Synchronisation

For DECT radios to be able to communicate, they must be synchronised with one another. In an IP1500 system, synchronisation is obtained using the 2-wire interface of the CCFP. In an IP1200 system, it is obtained via the air, however. Therefore, an IP1200 configured as a DECT radio must be created within the coverage of another DECT radio, from which synchronisation can be obtained.

In an IP1500 system, only the repeaters must be created within the coverage of a DECT radio. Of course, this also applies in an IP1200 system.

Synchronisation chain

In a closed system, every IP1200 DECT radio must be synchronised with all other IP1200 DECT radios. This presupposes that every DECT radio (apart from one) has a different one configured as the synchronisation source.

The one DECT radio that does not obtain its synchronisation from another DECT radio is called the "sync master". It must be an IP1200 and must not be a repeater. All other DECT radios obtain their synchronisation from this DECT radio either directly or indirectly.

The name of the field for entering the synchronisation source ("Sync Master") is actually wrong: it is not the radio ID of the sync master that is entered here, but the radio ID of the radio from which synchronisation is to be obtained. One could also say the next DECT radio in the synchronisation chain.

For redundancy, an "Alt sync master" can be configured. This is used as the synchronisation source if the DECT radio configured as the "Sync master" is not available.

Obviously, no circles must exist in the synchronisation chain.

A repeater likewise requires a synchronisation source. It must not be configured with an alternative synchronisation source however, since the latter serves as a synchronisation source only in the event of failure of the sync master. Therefore, no repeater should be used as the synchronisation source for an IP1200 DECT radio.

Similarly, no repeater should be used as the synchronisation source in a repeater chain.

Sync master

The DECT radio in an IP1200 installation that does not obtain its synchronisation from another source.

Is also used in the IP1200 DECT radio configuration to configure the sync source of the DECT radios.

Sync source

A DECT radio which serves as the synchronisation source for other DECT radios.

T

TCP

The TCP protocol (**T**ransmission **C**ontrol **P**rotocol) is a connection-oriented transport protocol for use in packet-switched networks. The protocol builds on the IP protocol; it supports the functions of the transport layer and establishes a secure connection between the entities before data transfer.

Telnet

Telnet (**Tel**etype **Net**work) is the name of a network protocol that is widely used in the Internet. The purpose of the Telnet protocol is to offer fairly general, bidirectional, 8-bit-per-byte-oriented communication. It is usually used to offer users access to Internet computers via the command line. Here, the Telnet program provides the required client functions of the protocol. However, because there is no encryption, it is hardly used any more.

TFTP

The TFTP protocol (**T**rivial **F**ile **T**ransfer **P**rotocol) is a very simple file transfer protocol. TFTP supports merely the reading or writing of files. Many functions of the more powerful FTP (**F**ile **T**ransfer **P**rotocol), such as rights allocation using chmod, displaying existing files or user authentication, are not available. Unlike FTP, which requires a connection-oriented transport protocol, TFTP is normally operated via a connectionless protocol like UDP.

TOS

The ToS field (**T**ype **O**f **S**ervice field) is a data field in the IP header, in which the services of the datagram are defined. With the ToS information, computers can specify network-relevant types of service. Here, various parameters, such as the bandwidth, the transfer speed or the reliability of the transfer can be defined. Furthermore, the priority handling of datagrams, the type of throughput and the reservation of resources in the routers can be defined.

Trace

A trace is a sequence of instructions, which begins with any start point and in which the program branches and their path selection are defined. It allows the program flow to be traced step by step. A trace is primarily used in troubleshooting and debugging.

U

UDP

Unlike the connection-oriented TCP (**T**ransmission **C**ontrol **P**rotocol), the **U**ser **D**atagram **P**rotocol is a minimal, connectionless network protocol that belongs to the transport layer of the Internet protocol family. The task of UDP is to send data transferred over the Internet to the correct application. With UDP, a protocol was required that was responsible only for the addressing without securing the data transfer, since this would result in delays in the voice transmission.

URL

Uniform **R**esource **L**ocator refers to a subtype of **U**niform **R**esource **I**dentifiers (URI). URLs identify a resource via its primary access mechanism (often http or ftp) and the location of the resource in computer networks. The name of the URI schema is therefore normally derived from the network protocol used for this. Examples here are HTTP or FTP.

UTC

UTC (**U**niversal **T**ime **C**oordinated) is the current (coordinated) world time, replacing in this function GMT time (**G**reenwich **M**ean **T**ime). It is a combination of the international atomic time TAI (**T**empus **A**tomique **I**nternational) and the UT (**U**niversal **T**ime). The time zones are specified as a positive or negative time difference from UTC (for example, UTC+2 corresponds to MEST). UTC combines the physical atomic time (TA) with the astronomical time (UT), and is also called civil time.

µ-law

The µ-law method is a digitization method for analogue audio signals, which is standardised in the G.711 recommendation of the ITU (**I**nternational **T**elecommunication **U**nion). Like the A-law method, the µ-law method uses a logarithmic quantisation characteristic curve to achieve a better signal-to-noise ratio. With this method, 8-bit values are likewise generated. However, the quantisation characteristic curve for low levels is steeper. In addition, the encoding is not designed to generate continuous sequences of 0s, but continually changing bit states. In this way, a particular method for timing recovery on the side of the receiver of the digital signal is simplified. The µ-law method is used by the PCM technique in North America and Japan.

V

VLAN

VLANs (**V**irtual **L**ocal **A**rea **N**etwork) are a technological concept for implementing logical workgroups within a network. This kind of network is implemented using LAN switching or virtual routing on the data link layer or on the network layer. Virtual networks are set up through a number of switching hubs, which are connected together through a backbone.

VPN

The term VPN (**V**irtual **P**rivate **N**etwork) is used with different meanings. Very generally, one refers to a VPN if customer-specific, logical subnetworks are being created within a public switched network. They may be networks for voice communication, or X.25, Frame Relay or ISDN networks. The usual interpretation of VPNs today is the IP VPNs, where the subscribers are connected via IP tunnels.

W

WAN

WANs (**W**ide **A**rea **N**etwork) are conceived for voice or data transmission over wide areas. These networks are installed nationwide in all industrial countries, and can be used without restriction for business and private communication. Such networks are conceived keeping in mind the service offering. Therefore, the classical analogue telephone network (POTS), just like ISDN, is suitable for telephony. The public data packet networks, on the other hand, were conceived for data transmission services. ATM, Frame Relay and Fast Packet Switching are also worth naming in this connection.

WINS

WINS (**W**indows **I**nternet **N**aming **S**ervice) is a method for converting computer names in Windows networks to IP addresses. The WINS method takes into account that two computers with the same name or the same IP address are never logged into the network.

With WINS, which uses the UDP protocol for transmission, the started client logs on to the WINS server with its NetBIOS name and the IP address. The latter checks whether the addresses are not already in use and enters them in the address database of the WINS server. When a client logs off, the address is released again and can be reassigned.

WRFP

WRFP (**W**ireless **R**adio **F**ixed **P**art) is used as a synonym for repeater.

Keyword index

innovaphone® AG
Böblinger Straße 76
D-71065 Sindelfingen

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

www.innovaphone.com
info@innovaphone.com