elmeg T444
elmeg T484

elmeg Router
English

Declaration of conformity and CE marks

This device meets the requirements of the following EC directive R&TTE 6/3/EG:

»Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity«.

You can also request this EC declaration of conformity at the following Internet URL: http://www.bintec-elmeg.com

The waste container symbol with the "X" through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life. You will find additional information on an individual returning of the old appliances under www.bintec-elmeg.com.

© bintec elmeg GmbH - All rights reserved.

Reprinting of this document, even excerpts, is permitted only with the express consent of the publisher and with precise source information, regardless of the media used (mechanical or electronic).

Function descriptions included in this documentation which refer to software products of other manufacturers are based on the software used and valid at the date the documentation was prepared or published. The product and company names used in this documentation may be protected by trademarks.

Table of contents

Introduction

Router of the PABX elmeg T444 / elmeg T484

The PABX elmeg T444 / elmeg T484 is equipped with an integrated router. You can provide access to the Internet and network several PC via this router.

What is a router?
A router allows LAN clients (computers, PC within a network) of one network (LAN) to obtain access to a different network, for example Internet. Access to the Internet is made available by various Internet service providers (ISP).

In this process, the router searches for a path on which data can be exchanged between the LAN clients in the local network and the Internet. Linking to the Internet can be carried out via an xDSL and / or an ISDN connection.

Router of the PABX system
The PABX system router is equipped with a WAN/xDSL and a LAN port). The PABX system is connected to another network, for example the Internet, via the WAN/xDSL port. You can hook up a DSL or cable model for connection to the Internet.

The LAN ports are for your local network. Here, you can directly connect up to two PCs equipped with built-in network cards. If you wish to network more than two PCs you can do this using an additional HUB / Switch, HomePN (optional module, not included in standard supply scope of system), or a USB port.

LAN1 sets itself automatically (from 10 Mbit/s half-duplex up to 100 Mbit/s full duplex) to the maximum data transfer rate of the remote location (PC).

These PCs are also part of your local network and can, for example, exchange files or take advantage of the Internet connections via the router. All LAN clients that are linked are integrated into the local network via the TCP/IP protocol.

Further PCs can be linked to your network via RAS- access. Here, the IP address is always assigned by the telephone system, even when the DHCP server is de-activated. Under “Address assignment” in the configuration program you can de-activate the DHCP server and input the starting address for RAS. The following 11 IP addresses are then automatically reserved for RAS.

Using the Remote Access Server (RAS) a field representative, for example, can call into the local network from an external location and then via the local network access the Internet. Access from an external location is only possible via an ISDN connection. External access is provided with user-name and password protection. If the call is made from an external location only, the phone number can also be monitored as an added protection feature. Note that this access portal is not protected by a firewall!

Note
Please note the further instructions given in the operator’s manual of the PABX system for connecting a pcs.

Which Internet connections are supported?
You can set up a connection to the Internet with your PABX system as follows:

- Dial-up connections via ISDN (using PPP protocol, with one or two ISDN B channels, i.e. at 64 kbit/s or 128 kbit/s).
  These types of connections require access data with the number to be dialed, the user name and password and, in some cases, other information such as the IP address of the name server and any information about the data compression method that is used (VJH).
- Using xDSL (for example ADSL - T-DSL) in conjunction with a DSL modem that is compatible with your ISP via PPPoE.
  These connections require your user name and password as access data.

- Using xDSL (for example: SDSL) in conjunction with a DSL modem that is compatible with your ISP with a set, public IP address. These connections require the public IP address that you have been assigned, the IP address of the next gateway (next hop) and the IP address for the name server of your provider.
- Tunneling. Here, data packets of one protocol are packed into the shell of a different protocol to route them on to the Internet. At the recipient the shell is then removed and the data packet routed on with the original protocol. This tunneling is used to overcome incompatible networks, or when taking into consideration security and cost aspects (for example PPTP). Normally, you only need your user name and password as access data. Indicate all the data that is also specified to you by your provider (for example, number, IP address and DNS server.

The ISP that you wish to use for your Internet connections is set in the configuration of the PABX system. You can configure up to 10 ISPs. You can then define further settings for each ISP, such as user name, password, phone number, etc.. You can also define whether the connection to the Internet is to be set up automatically (default setting) and that the next ISP in your list is to be selected once the connection has been established (fall-back).

When the PABX system router receives the command to establish an Internet connection this connection is set up using the first ISP in your list. If the connection is set up successfully all of the clients in your network can access the Internet. If the Internet connection is no longer needed (inactivity) it is terminated after a defined time.

If an Internet connection can not be set up using the selected ISP an attempt is made to establish the connection using the next ISP in your list (fall-back).

When an Internet connection is terminated, the first ISP in the list is used when the next connection attempt is initially carried out.

Note
For more information about configuring ISPs and establishing an internet connection, refer to the operator's manual of your PABX.

Note
If "hubs" are installed in your network, for example, or if a connection to the Internet still exists, data packets may continue to be sent to the router and the connection can not be terminated.

Dial-in into the LAN (RAS)

Using the Remote Access Server (RAS) a field representative, for example, can call into the local network from an external location and then via the local network access the Internet. Access from an external location is also possible via an ISDN connection.
External access is provided with user-name and password protection. If the call is made from an external location only, the phone number can also be monitored as an added protection feature. Access can be enabled for up to 8 users. A Windows enable (access to computer, files or printers) and Internet enable can also be configured for each user.

A PC that dials into the local network via RAS is automatically assigned an IP address by the integrated DHCP server.

RAS Callback:

If you do not want to be charged for connections within your company network you can configure the RAS connection as an automatic call-back. For this, a brief connection is set up to the company network (for which you are charged) that then initiates a call-back. The PABX system at your company then calls you back and you are not charged for the ensuing connection time. You can enter a number for the corresponding RAS connection in the configuration. Automatic call-back is then only possible from this number. If you do not enter a number here, the automatic call-back can be made from any number.

DHCP server and IP address allocation

PCs can be provided with a major portion of the configuration required for LAN and Internet access via the DHCP (Dynamic Host Configuration Protocol). The DHCP server integrated into the PABX is capable of supplying corresponding configurations to up to 100 PCs (clients). IP addresses are dynamically allocated to the clients. The DHCP server task of the PABX system is activated in the initial status of the PABX.

You can configure the integrated DHCP server under »Network address allocation«.

You can configure the first IP address assigned by the DHCP server. The required number of IP addresses is assigned to the PCs (DHCP clients) in ascending order.
Eleven additional IP addresses for the DHCP server are always reserved for PCs that are integrated through RAS (remote access server) into the local network. If the integrated DHCP server is activated the 11 IP addresses which come after the configured DHCP address range are used for RAS clients.
When the DHCP servers are de-activated the 11 IP addresses that come after the set DHCP start address will be used for RAS clients.

Direct connection (DHCP)

This setting is used to utilize a direct WAN connection with automatic allocation of the IP addresses via DHCP. In this case the IP address is not assigned by your PABX system router, but by the network in which the router is integrated. The router DHCP must be de-activated in the configuration for this.

Default setting of the PABX

Default IP addresses for the local area network

In its basic setting you can use your PABX system as a router for Internet access for your local network. You have to define (when configuring the PABX) the Internet service provider that you wish to use.

The IP addresses for your local area network are then distributed as follows:

192.168.1.1 to 192.168.1.49	Freely assignable IP addresses as for example for LAN clients with a fixed IP address
192. 168. 1. 50 to 192.168.1.69	IP addresses that are allocated to corresponding LAN clients by the PABX system. (Number of DHCP clients: 20)
192.168.1.70 to 192.168.1.80	Reserved IP-addresses (11) RAS. These addresses must always remain reserved and may not be assigned as set IP addresses.
192. 168. 1. 81 to 192.168.1.249	Freely assignable IP addresses as for example for LAN clients with a fixed IP address
192.168.1.250	IP address for the PABX
192.168.1.251 to 192.168.1.254	Freely assignable IP addresses as for example for LAN clients with a fixed IP address

Note
Please note that each IP address can only be assigned once. The first and last IP address for a network may not be assigned to LAN clients. In this example: 192.168.1.0 and 192.168.1.255.

Example for the hint:

255.255.255.0	Subnet mask for all components on the network (PABX, LAN clients,.. .)
192.168.1.250	IP address for the gateway (PABX)
192.168.1.250	

IP address for the DNS server (PABX). The PABX system also acts as a DNS proxy in place of the ISP DNS server.

What are IP addresses and subnetwork masks
With the initial settings IP addresses and subnetwork masks are already set for the PABX system router. Both of these values are each 4 bytes in length.

IP address:	192.168.1.250
Subnet mask:	255.255.255.0

The IP address is an address that is reserved for private local networks.

The subnetwork defines that this is a Class C network in which up to 254 LAN clients can be linked. Using the subnetwork mask an IP address can be divided into the network address and the host address (address of the PC).

Example with this PABX:

IP address of the PABX:	192.168.1.250
IP netmask for the PABX:	255.255.255.0
Network part of the IP addresses:	192.168.1.xxx
Host part of the address:	x.x.x.250
First usable IP address:	192.168.1.1 (netmask: 255.255.255.0)
Last usable IP address:	192. 168. 1. 254 (netmask: 255.255.255.0)

You can assign the available IP addresses to the individual LAN clients manually, or have them assigned by the PABX system via DHCP. No IP address may be used simultaneously by more than one client however. With regard to the example given above this means that the address 192.168.1.250 may not be allocated again, as it is already being used by the PABX system.

The network part of the IP address may not be changed, as otherwise the LAN clients would not all be located within the same IP network. A PC with the IP address 192.168.2. 1 is located in a different network. A PC from the PABX net would not be able to locate this other PC if it is not within its own network.
In addition, the same subnetwork mask must also be entered at all LAN clients located within the same network.

Router functions

Automatic Internet access, fallback
Several ISPs (ISP – Internet Service Provider) can be set up in the PABX. Connectivity to the Internet is provided via the WAN port (e.g. DSL port), or via an ISDN port. If required, connection to the Internet can be set up automatically. If your selected ISP is not available, the next ISP in the list will be selected automatically.

Short Hold
Short Hold means that the PABX system terminates the Internet connection automatically after a configurable time period when there is no exchange of data from/to the Internet (inactivity). You can set this time separately for each ISP that you have configured.
This can result in increased connection costs with frequent, short excursions into the Internet, for example for picking up e-mails, as the connection is always maintained for the duration of the set holding time.

Dynamic ISDN
Higher data transfer rates can also be achieved for Internet access via the ISDN connection by bundling the two B channels for the connection. If an Internet connection with channel bundling is active and a B channel is needed for telephony or fax messages, one B channel is disconnected from the Internet connection. On completion of the voice

connection the B channel reverts automatically to use for the Internet connection. This function is available for incoming and outgoing voice links.

This performance feature requires that the ISDN Speed Manager be installed, or that Internet access is made via the router! The Speed Manager is included in the T-Online installation.

Completion of call to busy subscriber:

You can not be reached by an external telephone call when you are surfing the Internet and are using two B channels for downloading. As signaling of a further call is made via the D channel, your telephone system has the capability of specifically de-activating one B channel (depending on current settings) so that you can take a call. You can define the following settings in the PC Configurator.

Rejecting a call:

The caller will hear the busy signal and both B channels remain active.

Internal MSN extension number:

One B channel is de-activated (the call briefly hears music on hold, see also Page) and the call is signaled at the subscriber entered under »Internal number«. This terminal device may not be located on the same ISDN bus or at the same USB port as the PC.

Forwarding (Call Deflection) to an external extension number :

One B channel is de-activated and the call signaled at the subscriber entered under »External number«. You can also have the call forwarded to an external subscriber by the exchange, allowing both B channels to remain active. Calls can also be transferred (for example for T-NetBox or cell phone) without a B channel of the telephone system being allocated.

Normal call distribution:

One B channel is de-activated and the call signaled at the subscriber entered under »Call allocation« for the »External number«.

Dynamic ISDN for all outgoing calls

You can not make an outside call if you are surfing in the Internet while using two B channels for downloading. However, depending on the PC configuration, your telephone system does have the capability to specifically de-activate one B channel so that you can make calls while connected to the Internet.

DHCP server

PCs can be provided with a major portion of the configuration required for LAN and Internet access via the DHCP (Dynamic Host Configuration Protocol). The DHCP server integrated into the PABX is capable of supplying corresponding configurations to several PCs (LAN-clients). IP addresses are dynamically allocated to the clients. This mode is recommended to dispense with the complicated, manual configuration of the IP addresses for the PC that would otherwise be required.

DNS server

The DNS server (Domain Name Server) has the task of establishing names within a network. In this process the IP addresses of the PCs (e.g. LAN clients) are transformed into names. You must therefore know the name, and not the IP address, of a PC that you wish to access, or are searching for. The DNS server can also establish names that are not included in the local network.

DNS-Proxy

A proxy assumes a surrogate function for the local network (LAN) in a different / external network. Here, the DNS proxy accepts the name queries from the LAN client and submits them to the external network, e.g. Internet, as its own queries. The proxy then takes the response from the external network and forwards it to the LAN client that placed the original query. In addition, the result from the query is stored for a defined time (configurable) to answer any subsequent queries of the same type.

Dynamic DNS

Using Dynamic DNS you can also offer your own Internet services (e.g. WEB, FTP or e-mail servers). Usually you must have a fixed line or a set IP address for this so that you can always be reached at the same URL (For example: www.bintec-elmeg.com).
You are assigned a new IP address by the ISP each time you dial in to the Internet however. Using Dynamic DNS you can link this automatic (dynamic) IP address with a set name. The router will then inform your Dynamic DNS service provider (e.g. www.dyndns.org) automatically of the new IP address. Internet enquiries for your Web services are then automatically forwarded to your dynamic IP address via your service provider.

Using Dynamic DNS

- Configure an Internet address (URL) at a Dynamic DNS service provider. For example, at “www.dyndns.org” configure the address “www.my-homepage.dyndns.org”.
- Configure the LAN client of the network in which you wish to offer your Web services with a set IP address. For example, let’s say we want to configure a Web server with the IP address 192.168.1.200.
- Activate the Dynamic DNS function in the router and enter the Internet address (URL) for your Dynamic DNS provider (in the example here www.dyndns.org).
  Add the necessary filters in the firewall to allow the PC with the Web services to be reached from an external location.
  - Configure port mapping for Port 80 (HTTP protocol) to IP address 192.168.1.200.
  - Configure the filters that permit incoming and outgoing WAN connections at Port 80.
- The router will automatically inform your Dynamic DNS provider of your current dynamic IP address each time a connection is set up with the Internet. The information about the IP address is transferred after setting up a new Internet connection, as well as during an ongoing Internet connection.
- A PC in the Internet enters the address (URL) “www.my-homepage.dyndns.org”. In this way it reaches your Dynamic DNS service provider. Your service provider reroutes the connection to your current dynamic IP address.
- Any incoming connection is handled in accordance with the configured filters. In the example given here the incoming WAN connection at port 80 is forwarded to the LAN client with the IP address 192.168.1.200. The available Internet sites of your Web server are displayed on the external PC.

NAT

NAT (Network Adress Translation) protects the connected LAN-clients against attacks from the Internet. Here, the internal IP addresses are not passed on to the Internet. The router carries out the transfer to the Internet and distributes the incoming data packets in the internal system. This only requires one external IP address. The internal IP addresses are protected from attacks from outside. The internal IP addresses can not be targeted by hackers, as these IP addresses are non-accessible.

Packet Filter Firewall

The integrated filter firewall packet also provides you with enhanced security against attacks from the Internet. A firewall acts as a logical wall for data packets between the Internet and the LAN which has »holes« for certain packets (firewall rules, also known as filters), allowing these packets to pass through the wall. The filters are described by rules whose configuration requires expert knowledge about the TCP/IP protocol family. The firewall of your PABX system can be easily configured using a Filter Wizard in which you need to indicate (in plain text) whether you wish to allow defined applications access to the Internet.

Portmapping

You wish to access your PC from an external location via Internet. Normally, access via the firewall should be prohibited. When you use port mapping, access to a router port that you have enabled is permitted from an external location. The router then forwards the access request to the defined port of the PC in the network. A fixed IP-address must be assigned to this PC. When the PC returns data packets the IP address and port number of the PC are replaced by the router with the number for the port mapping port and the router IP. For "outsiders" on the Internet it then appears as though there is only one connection to the router.

Note
Please note that when you use port mapping the firewall for the ports enabled for this function is ineffective. The target PC in your LAN may then be susceptible to any potential attacks.

Port mapping is practical when you wish to run a game server on your own, for example.

- You can make this server accessible via the Internet to other users.
- Or, if you require certain peer-to-peer file sharing software that provides greater download bandwidth.
- When the corresponding PC in your LAN is to be accessible from the Internet (not possible in the standard configuration with NAT). In this case, certain UDP and TCP ports must be rerouted to a PC in the LAN.

RAS-Server

Using the Remote Access Server (RAS) a field representative, for example, can call into the local network from an external location and then via the local network access the Internet. Access from an external location is also possible via an ISDN connection.

External access is provided with user-name and password protection. If the call is made from an external location only, the phone number can also be monitored as an added protection feature. Access can be enabled for several users. A Windows enable (access to computer, files or printers) and Internet enable can also be configured for each user.

Note
Note that this access portal is not protected by a firewall!

A PC that dials into the local network via RAS is automatically assigned an IP address by the integrated DHCP server.

Time-controlled router inhibition

With the aid of the calendar, or a manual function of the PABX system, you can set the time(s) of day when Internet access is possible (permitted). These times are defined via the calendar assigned to the router in the configuration. Here, it is stipulated that Internet connections can not be set up during night-time operation. You should therefore set the switching times accordingly. Starting with Version 4 of system phones CS290/CS410, the telephones can be switched using function keys on the phone; this setting is then retained until the next calendar-based switchover.

LAN-CAPI

The package includes a program called »CAPI for LANs« for use in your network. This software can be installed on any PC in the network. This gives you the possibility of running your CAPI application from a central location via an interface, i. e. the PABX system. There is no ISDN card required for the PCs. Please note that software used for the CAPI application may require certain license agreements with the software manufacturer. The program »CAPI in LAN« does not require a license to run.

LAN-TAPI

The package includes a program called »TAPI for LANs« for use in your network. This software can be installed on any PC in the network. This gives you the possibility of running your TAPI application from a central location via an interface, i. e. the PABX system. There is no ISDN card required for the PCs. Please note that software used for the TAPI application may require certain license agreements with the software manufacturer. The program »TAPI in LAN« does not require a license to run.

Blocking of Internet access by the provider

After several failed attempts of inputting user names or passwords the provider will block access to the Internet for a defined period. To prevent this the router only allows three attempts to be made. After that you must then reconfigure the router and enter a correct user name and password. The router must then be enabled again after this via the Control Center.

Connection test

You can test the connection to your provider without a connection actually being set up. The item »Connection test T-Online for DSL and ISDN« is given in the provider list in the configuration. Select this item as the first provider and store it in the PABX system. You can then manually set up a connection to the Internet via the ControlCenter and the results for this connection are then displayed after a few seconds. No actual Internet connection is established here however. If the results are positive delete the current provider and enter the settings supplied by your provider in the configuration for setting up Internet connections.

Router control via system phone

Starting with Version 4 you can configure a function key on system telephones CS290 / CS410 /CS400xt for controlling the router.

LED Settings

Through PABX system configuration you can de-activate the LEDs, except for the »On« LED. When you re-activate the LEDs the »ISDN« LED may indicate a false status. You should therefore disconnect the external ISDN port for a brief period from the NT.

Status display CAPI / TAPI in the ControlCenter

Information used for monitoring the CAPI-TAPI functions can be displayed using the Control Center menu. Indication of the associated function(s) is made only when TAPI and CAPI clients are installed on your PC.

- The number of TAPI licenses currently in use (max. 10) is indicated when there is a TAPI connection with the PABX system.
- The number of CAPI licenses (max. 10) is indicated, along with allocation of the internal and external B channels (max. 2 each), when there is a CAPI connection with the PABX system.

Configuration examples

Address assignment by DHCP -Recommended configuration - (Default setting)

Address assignment via DHCP is the easiest configuration method for the PABX system and at the clients (PCs).

You can configure a LAN client in the network such that it automatically receives its IP address from a DHCP server from the PABX system on startup. In this case, you do not have to enter an IP address or subnetwork mask in the configuration of the LAN client.

Things to note for this configuration.
PABX:

In its initial setting the PABX system is pre-configured for address assignment via DHCP.

You need to choose an ISP. To do this follow the instructions given in the manual, or the brochure »On the fast track to the Internet«.

Note
When delivered, the DHCP server is already activated and pre-configured. If required you can define the start address (first IP address allocated by DHCP) and the maximum number of LAN clients (PCs).

LAN-Client (PC) Configuration:

PCs with operating systems starting from Windows 98SE are already correctly configured in their standard settings for address assignment via DHCP.

If other means of Internet connection, for example modem or an ISDN card, have already been configured on the LAN client (PC) observe the information given in the section»Settings in Internet Explorer / Internet Options with Windows« in this manual.

Note
Please keep in mind that any changes made to the Windows network settings may have serious effects on the LAN clients (PCs). Other methods of connection or applications may also be affected by these changes. In the event that your network settings have already been changed contact your system administrator. You may have to backup all of your data. The configuration presented in the following represents only one of many possibilities. These settings are recommended. However, depending on the infrastructure of your environment, it may be meaningful to choose a different configuration.

If you need to reset the Windows network settings to their standard (default) status proceed as follows:

Example Windows 98SE /ME:

- Open the Control Panel from the Windows Start Menu.
- Windows 98SE: Open the folder »Network«.
- Windows ME: Right-click on »LAN connection« and then click on »Properties«.
- Select »TCP/IP« and click »Properties«.

Note
The network adapter connected to the PABX system must be linked to the TCP/IP protocol, which is a component of Windows. You may have to manually add this protocol. The network adapter may only be linked to the T-DSL / PPP0E protocol, especially if a stand-alone version of the T-DSL driver has been installed. Add the TCP/IP protocol manually using the buttons »Add«, »Protocol«, »Microsoft«, »TCP/IP«.

- Then specify that the PC is to receive its IP address automatically. All other settings, for example DHCP, network mask, gateway and DNS server should be de-activated or blank. The PABX system automatically transfers all required settings to the client (PC) via DHCP.
- Confirm your settings by clicking OK.

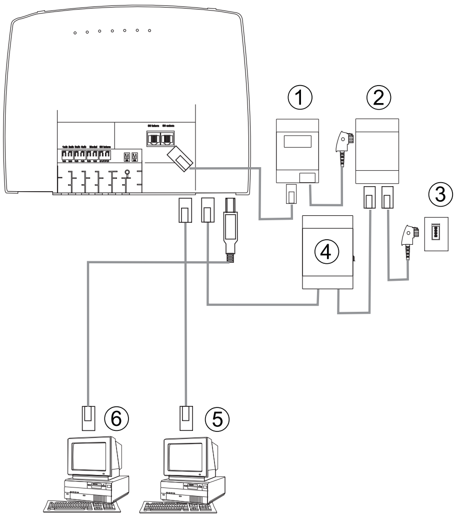
Example Windows 2000 and Windows XP:

- Open the Control Panel from the Windows Start Menu.
- Under Windows 2000 open the folder »Network and Dial-up Connections«.
- Under Windows XP open the folder »Network connections«.
- Select the »LAN Connection« for the PABX by pressing the right mouse button. Then click »Properties«.
- Select »TCP/IP« and click »Properties«.
- Then specify that the PC is to receive its IP address automatically. All other settings, for example DHCP, network mask, gateway and DNS server should be de-activated or blank. The PABX system automatically transfers all required settings to the client (PC) via DHCP.
- Confirm your settings by clicking OK.

Note
Also follow the instructions given in the documentation and the Help function of your operating system. If it is not possible to set up a connection to the PABX, or to the Internet, refer to the section »Checking the LAN client (PC) configuration« in this manual.

Sample configuration of a network with DHCP address allocation

Configuration of the PABX system in its initial settings



① NT
② NT / Splitter
③ Connection for the service provider
④ Modem
⑤ Network PC 2 at HUB / Switch
⑥ PC 1 at USB port

IP address for the PABX:	192.168.1.250
Subnet mask:	255.255.255.0
Start address DHCP:	192.168.1.50
Number of DHCP addresses	20

PC1

IP via DHCP:	192.168.1.50 transmitted automatically via DHCP.
Gateway:	transmitted automatically via DHCP.
DNS server:	transmitted automatically via DHCP.
Subnet mask:	transmitted automatically via DHCP.

PC2

IP via DHCP:	192.168.1.53 transmitted automatically via DHCP.
Gateway:	transmitted automatically via DHCP.
DNS server:	transmitted automatically via DHCP.
Subnet mask:	transmitted automatically via DHCP.

In the example given here, the IP addresses for the clients (PCs) can lie within a range from IP 192. 168. 1. 50 to 192. 168. 1. 69. The IP addresses are assigned in the order that the clients (PCs) request them (for example by switching on the PCs). If an IP address is released (for example by switching off a PC) that IP address is then available to be re-assigned again.

Address assignment without DHCP (set / mixed IP addresses)
You can dispense with a DHCP server in a network or also configure LAN clients (PCs) with set IP addresses as an addition to the DHCP clients.

Note
Much more time and effort is involved for configuring the network if a configuration is chosen without DHCP. If

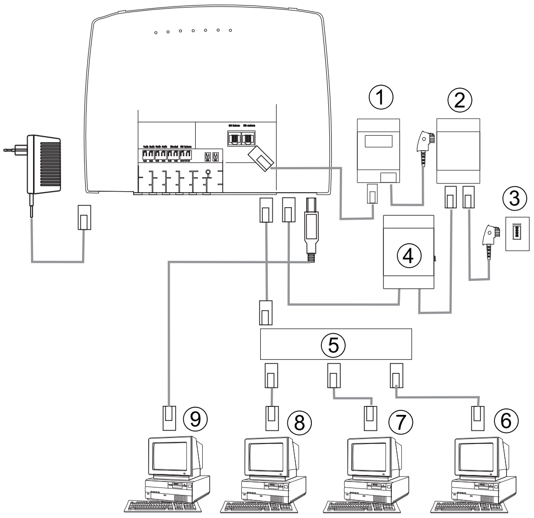
you are relatively new to Windows network configuration, we recommend a configuration using DHCP.

Things to note for this configuration.

PABX:

You can de-activate the DHCP server for the PABX system using the »Professional Configurator« program.

Note
You may have to adapt the IP addresses and subnetworks of the PABX system to the settings present on the LAN clients (PCs). For information about this use the online Help function of the Configurator.



① NT
② NT / Splitter
③ Connection for the service provider
④ Modem
⑤ External HUB / Switch by means of LAN2 (100 MBit/s)
⑥ Network PC 4 at HUB / Switch
⑦ Network PC3 at the HUB / Switch
⑧ Network PC2 at the HUB / Switch
⑨ PC 1 at USB port

LAN-Client (PC) Configuration

You must make the following minimum settings manually:

- IP address for the LAN client (PC)
- Netmask / Subnet mask (which is also entered in the PABX router)
- IP address of the PABX system as the gateway (interface to other networks, for example Internet)
- IP address of the PABX system as the DNS server (server that converts the Internet addresses into IP addresses)

Note
Observe the instructions for address assignment given on the previous pages.

PC settings in Windows operating system
The procedures described below deal only with examples which may differ somewhat depending on the operating system used and the configuration of the PC.

Note
Please keep in mind that any changes made to the Windows network settings may have serious effects on the LAN clients (PCs). Other methods of connection or applications may also be affected by these changes. In the event that your network settings have already been changed contact your system administrator. You may have to backup all of your data. The configuration presented in the following represents only one of many possibilities. These settings are recommended. However, depending on the infrastructure of your environment, it may be meaningful to choose a different configuration.

Example Windows 98SE and Windows ME:

- Open the Control Panel from the Windows Start Menu.
- Open the »Network« folder
- Select »TCP/IP« and click »Properties«.
- Now select whether the PC is to receive its address automatically from a DHCP server, or if it is to be assigned as permanent IP address. Edit or supplement the settings for network mask, gateway and DNS server as appropriate. Refer to the parameters that are to be set in the sample configuration with mixed address assignment, or in the sample configuration with set address assignment on the following pages.
- Confirm your settings by clicking OK.

Example Windows 2000 and Windows XP:

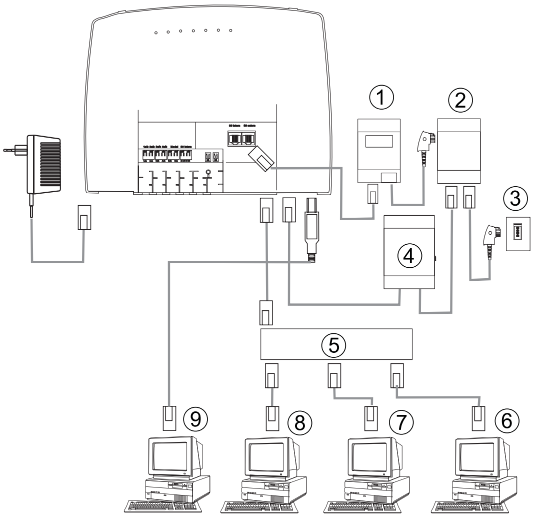
- Open the Control Panel from the Windows Start Menu.
- Under Windows 2000 open the folder »Network and Dial-up Connections«.
- Under Windows XP open the folder »Network connections«.
- Right-click on »LAN connection« and then click on »Properties«.
- Select »TCP/IP« and click »Properties«.
- Now select whether the PC is to receive its address automatically (from a DHCP server), or if it is to be assigned as set (permanent) IP address. Edit or supplement the settings for network mask, gateway and DNS server as appropriate. Refer to the parameters that are to be set in the sample configuration with mixed address assignment, or in the sample configuration with set address assignment on the following pages.
- Confirm your settings by clicking OK.

Note
Also follow the instructions given in the documentation and the Help function of your operating system.

Note
A further option available is assigning a portion of the IP addresses manually and having the remaining addresses allocated by DHCP. Ensure that the IP address for the router and any manually assigned IP addresses are not located in the range for available DHCP addresses.

Sample configuration of a network with mixed address assignment

Set IP addresses and IP addresses allocated by DHCP



① NT
② NT / Splitter
③ Connection for the service provider
④ Modem
⑤ External HUB / Switch by means of LAN2 (100 MBit/s)
⑥ Network PC 4 at HUB / Switch
⑦ Network PC3 at the HUB / Switch
⑧ Network PC2 at the HUB / Switch
⑨ PC 1 at USB port

IP address for the PABX:	192.168.1.250
Subnet mask:	255.255.255.0
Start address DHCP:	192.168.1.50
Number of DHCP addresses 20	

PC1

Fixed IP:	192.168.1.91
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

PC2

Fixed IP:	192.168.1.93
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

PC3

IP via DHCP:	192.168.1.50 transmitted automatically via DHCP.
Gateway:	transmitted automatically via DHCP.
DNS server:	transmitted automatically via DHCP.
Subnet mask:	transmitted automatically via DHCP.

PC4

IP via DHCP:	192. 168. 1. 51 transmitted automatically via DHCP.
Gateway:	transmitted automatically via DHCP.
DNS server:	transmitted automatically via DHCP.
Subnet mask:	transmitted automatically via DHCP.

Sample configuration of a network with set address assignment

IP address for the PABX:	192.168.1.250
Subnet mask:	255.255.255.0
Start address DHCP:	DHCP server is off.
Number of DHCP addresses:	DHCP server is off.

PC1

Fixed IP:	192.168.1.81
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

PC3

Fixed IP:	192.168.1.83
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

PC4

Fixed IP:	192.168.1.84
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

PC5

Fixed IP:	192.168.1.85
Gateway:	192.168.1.250
DNS server:	192.168.1.250
Subnet mask:	255.255.255.0

Checking the LAN clients (PCs)

Configuration for Windows 98SE/ME/2000/XP
If a connection to the PABX system, or to the Internet can not be set up you can check the configuration of the LAN clients (PCs) based on the following information.

> Note
> The procedure described here assumes that you are using the recommended configuration with address assignment by DHCP.

The PC is linked to the PABX system via Ethernet (LAN1 jack).

- Check to ensure that the network adapter (Ethernet adapter, Home Phoneline Networking Adapter or USB) installed in the LAN client (PC) is connected properly to the PABX system. The connection status is displayed by the LEDs of the PABX. A description of the LEDs is given in the operator's manual for the PABX system.
- Check to ensure that the PABX system has assigned an IP address to the LAN-Client (PC) (see page in section »Checking the TCP/IP Configuration«).
- Check to ensure that an Internet service provider (ISP) has been configured in your PABX (see operator's manual for the PABX, leaflet »On the fast track to the Internet« or the online Help function of your PABX system).
- Check to ensure that the Internet browser(s) has(have) been configured correctly in your PC (see Page in section »Settings im Internet Explorer / Internetoptionen of Windows«).
- If you have made the settings as described above, the telephone system will establish a connection to the Internet automatically (e. g. by opening the Internet Explorer, inputting an Internet URL and confirming with "Enter") when requested to do so by an application (default setting).
- Check to ensure that automatic connection to the Internet has been de-activated (see Configurator Network«, »Internet«); the connection must then be established manually via the elmeg ControlCenter.

The PC is linked to the PABX system via USB.

- Using the Windows 98SE/ME/2000/XP operating systems you can only run one LAN client (PC) at the USB port of the PABX system.
- The required USB driver is installed automatically when you initially connect the PC with the PABX system. This driver is located on the CD supplied with the system.
- After installing the USB driver successfully, follow the procedure for Ethernet LAN clients.

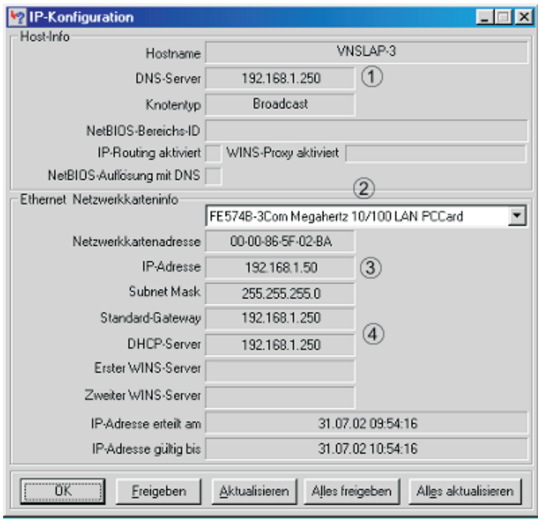
> Note
> The USB driver supplied with the system (RNDIS) is located in the device manager of the Windows control panel as a virtual network adapter. Communication between the PABX system and the PC connected via USB is effected via the TCP-IP protocol. Data for LAN-CAPI are also transferred using this protocol.

Checking the TCP/IP Configuration

The examples described below are base on the recommended network configuration with automatic address allocation. What this means is that the LAN clients get their IP address via DHCP (»IP address fetched automatically«) and that the DHCP server in the PABX system is switched on (initial setting).

Windows 98SE / ME

- Start the program Winipcfg.
  Select »Run... « in the Windows start menu. Enter
  »winipcfg« into the input field and click OK to confirm. Finally press the button »More info«



Host-Info
Hostname: VNSLAP-3
DNS-Server: 192.168.1.250
Knotentyp: Broadcast
NetBIOS-Bereichs-ID:
IP-Routing aktiviert □ WINS-Proxy aktiviert
NetBIOS-Auflösung mit DNS □

Ethernet Netzwerkkarteninfo
FE574B-3Com Megahertz 10/100 LAN PCCard
Netzwerkkartenadresse: 00-00-86-5F-02-BA
IP-Adresse: 192.168.1.50
Subnet Mask: 255.255.255.0
Standard-Gateway: 192.168.1.250
DHCP-Server: 192.168.1.250
Erster WINS-Server:
Zweiter WINS-Server:
IP-Adresse erteilt am: 31.07.02 09:54:16
IP-Adresse gültig bis: 31.07.02 10:54:16

① Current IP address of the pabx as DNS server.
② Select the network adapter connected to the pabx.
③ Current IP address of the network adapter (client).
④ Current IP address of the pabx as gateway and DHCP server.

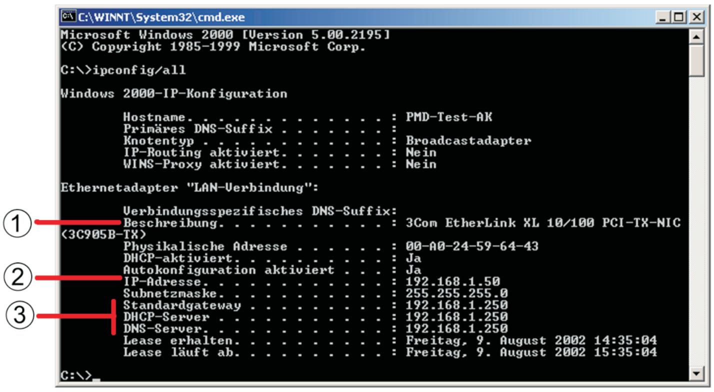
- The values shown in the screen shot are set as defaults for the initial settings of the PABX system. Depending on how many clients (PCs) are connected, the IP address lies within a range from 192.168.1.50 to 192.168.69. When these values are displayed, the network adapter and the Windows network settings have been configured correctly. Should the program »Winipcfg« show other values, click the buttons »Enable everything« and then »Update everything«.

If Winipcfg continues to show other values after this, this may be due to the following reasons:

- Changes have already been made to the initial setting for the PABX system in the Professional Configurator.
- The Windows network configuration for the client (PCs) does not correspond to the factory settings Default setting.
- Faulty installation of the network adapter in the client (PC), or the network adapter is not connected properly with the PABX system. Check your installation as described in the operator's manual for the PABX system (Installation and Commissioning section).
- The TCP/IP protocol is not installed on the PC, or it has no link to the network adapter connected to the PABX system.

Windows 2000

- Start ipconfig.
  Select »Run... « in the Windows start menu. Enter »cmd« and then click OK to confirm. Enter the command »ipconfig/all« and then press Enter to confirm.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig/all

Windows 2000-IP-Konfiguration

        Hostname. . . . . . . . . . . . . : PMD-Test-AK
        Primäres DNS-Suffix . . . . . . . :
        Knotentyp . . . . . . . . . . . . : Broadcastadapter
        IP-Routing aktiviert. . . . . . . : Nein
        WINS-Proxy aktiviert. . . . . . . : Nein

Ethernetadapter "LAN-Verbindung":

        Verbindungsspezifisches DNS-Suffix:
        Beschreibung. . . . . . . . . . . : 3Com EtherLink XL 10/100 PCI-TX-NIC
(3C905B-TX)
        Physikalische Adresse . . . . . . : 00-A0-24-59-64-43
        DHCP-aktiviert. . . . . . . . . . : Ja
        Autokonfiguration aktiviert . . . : Ja
        IP-Adresse. . . . . . . . . . . . : 192.168.1.50
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 192.168.1.250
        DHCP-Server . . . . . . . . . . . : 192.168.1.250
        DNS-Server. . . . . . . . . . . . : 192.168.1.250
        Lease erhalten. . . . . . . . . . : Freitag, 9. August 2002 14:35:04
        Lease läuft ab. . . . . . . . . . : Freitag, 9. August 2002 15:35:04

C:\>_
```

① Select the network adapter connected to the pabx.

② Current IP address of the network adapter (client).

③ Current IP address of the pabx as gateway, DHCP server and DNS server.

- The values shown in the screen shot are set as defaults for the initial settings of the PABX system. Depending on how many clients (PCs) are connected, the IP address lies within a range from 192. 168. 1. 50 to 192. 168. 1. 69. When these values are displayed, the network adapter and the Windows network settings have been configured correctly.

- The value for the physical address is different for each network adapter. The values for the lease depend on when the PC is switched on.

If other data are shown, this may be due to the following reasons:

- Changes have already been made to the initial setting for the PABX system in the Professional Configurator.

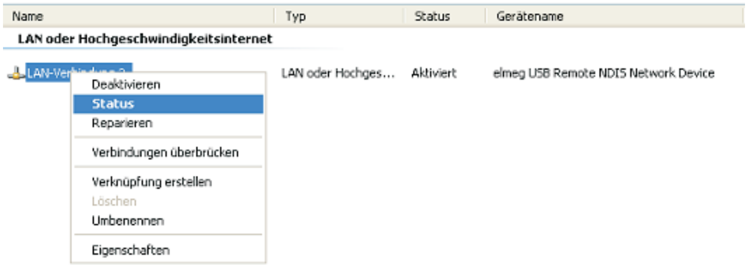
- The Windows network configuration for the client (PCs) does not correspond to the factory settings Default setting.

- Current IP address of the pabx as gateway, DHCP server and DNS server. Check your installation as described in the operator’s manual for the PABX system (Installation and Commissioning section).

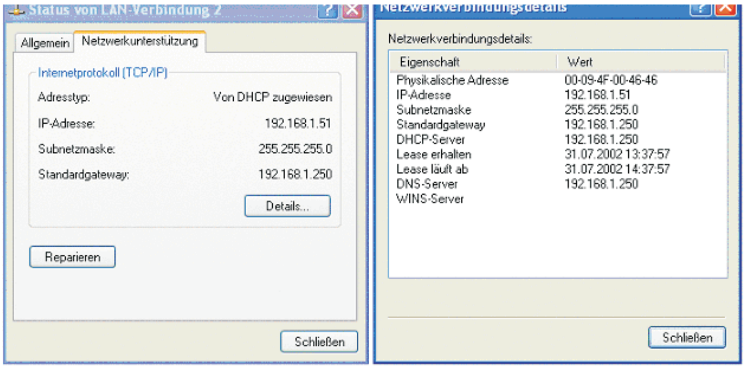
- The TCP/IP protocol is not installed on the PC, or it has no link to the network adapter connected to the PABX system.

Windows XP

- Open the Windows XP network connections.
  Select the network adapter connected to the pabx by pressing the right mouse button. Then click »Status«.



Name	Typ	Status	Gerätename
LAN oder Hochgeschwindigkeitsinternet			
LAN-Ver	LAN oder Hochges...	Aktiviert	elmeg USB Remote NDIS Network Device



Status von LAN-Verbindung 2
Allgemein
Netzwerkunterstützung
Internetprotokoll (TCP/IP)

Adresstyp: Von DHCP zugewiesen

IP-Adresse: 192.168.1.51

Subnetzmaske: 255.255.255.0

Standardgateway: 192.168.1.250

Details...
Reparieren
Schließen
Netzwerkverbindungsdetails

Netzwerkverbindungsdetails:

Eigenschaft	Wert
Physikalische Adresse	00-09-4F-00-46-46
IP-Adresse	192.168.1.51
Subnetzmaske	255.255.255.0
Standardgateway	192.168.1.250
DHCP-Server	192.168.1.250
Lease erhalten	31.07.2002 13:37:57
Lease läuft ab	31.07.2002 14:37:57
DNS-Server	192.168.1.250
WINS-Server	

- The values shown in the screen shot are set as defaults for the initial settings of the PABX system. Depending on how many clients (PCs) are connected, the IP address lies within a range from 192. 168. 1. 50 to 192. 168. 1. 69. When these values are displayed, the network adapter and the Windows network settings have been configured correctly. If other values are shown click the button »Repair«.

- The value for the physical address is different for each network adapter. The values for the lease depend on when the PC is switched on.

If other data continues to be shown this may be due to the following reasons:

- Changes have already been made to the initial setting for the PABX system in the Professional Configurator.

- The Windows network configuration for the client (PCs) does not correspond to the factory settings Default setting.

- Faulty installation of the network adapter in the client (PC), or the network adapter is not connected properly with the PABX system. Check your installation as described in the operator’s manual for the PABX system (Installation and Commissioning section).

- The TCP/IP protocol is not installed on the PC, or it has no link to the network adapter connected to the PABX system.

Configuring Internet access on a PC

If you have used the Windows dial-up network for Internet access up to now, this connection was always established as a »Dial-up connection« (analog or ISDN). Set-up and termination of an Internet connection was initiated automatically by the programs.

If you set up an Internet connection via the PABX system router, this represents a normal network connection for each PC. If a PC wants to use an Internet connection the network router, which acts as a gateway and establishes connections to other networks, is informed of this. The router, in our example here the PABX system, then sets up a connection to one of the Internet service providers that has been configured. As defined in the configuration for the PABX system, this connection is established/terminated automatically. The Internet service provider is configured using the PABX system's Configurator.

Internet Explorer settings / Windows Internet options
The following description illustrates the settings for Internet connections for the various operating systems. Proceed as described below for your operating system and activate the corresponding option.

Windows 98SE:

Start Menu - Settings - Control Panel - Internet Options - Connections

Windows ME:

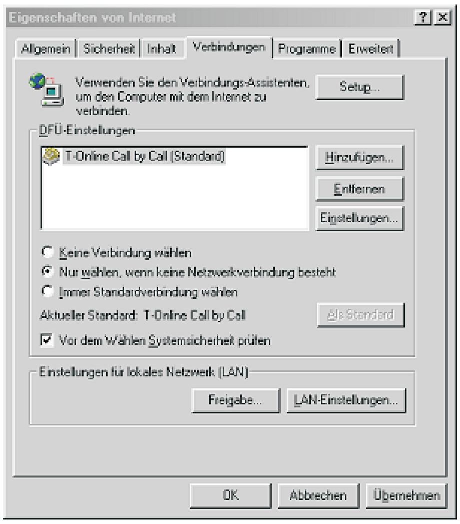
Start Menu - Settings - Control Panel - Internet Options - Connections

Windows 2000:

Start Menu - Settings - Control Panel - Internet Options - Connections

Windows XP:

Start Menu—-> Settings —-> Control Panel —-> Network and Internet connections -
Internet Options —- Connections



Verwenden Sie den Verbindungs-Assistenten, um den Computer mit dem Internet zu verbinden.

T-Online Call by Call (Standard)

○ Keine Verbindung wählen
● Nur wählen, wenn keine Netzwerkverbindung besteht
○ Immer Standardverbindung wählen

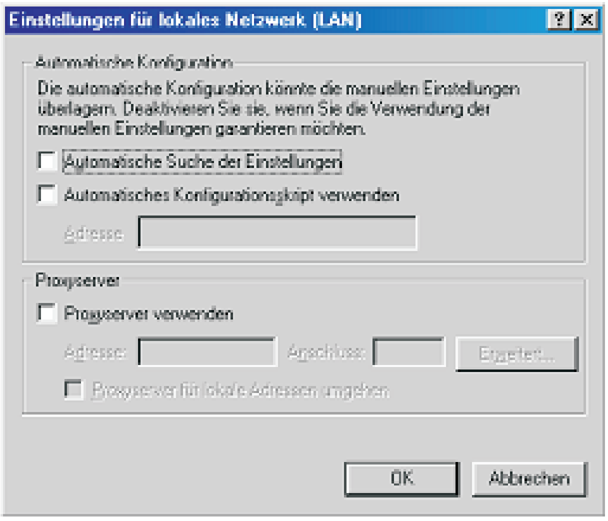
Aktueller Standard: T-Online Call by Call

☑ Vor dem Wählen Systemsicherheit prüfen

Dial-up connections configured at the client are displayed here. These connections are not required for accessing the Internet with the pabx.

Check »Never«. You can use other devices besides your PABX system to hook up to the Internet. You may have to select the option »Dial whenever a network connection is not present«.

There are no settings required under »LAN Settings«.



Einstellungen für lokales Netzwerk (LAN)

Automatische Konfiguration

Die automatische Konfiguration könnte die manuellen Einstellungen überlagern. Deaktivieren Sie sie, wenn Sie die Verwendung der manuellen Einstellungen garantieren möchten.

□ Automatische Suche der Einstellungen

□ Automatisches Konfigurationsskript verwenden

Adresse

Proxyserver

□ Proxyserver verwenden

Adresse: Anschluss:

□ Proxyserver für lokale Adressen umgehen

Configure firewall filters

You can only configure filters in the »Professional Configurator«.

User-defined filters for the router integrated into the PABX system with packet filter firewalls can be configured under Network / Filters.

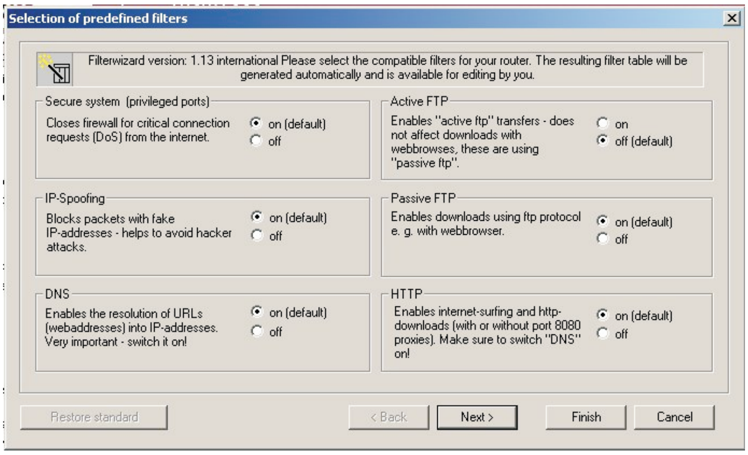
Note
We recommend configuring the firewall filters with the aid of the Filter Wizard to ensure configuration(s) appropriate for and compatible to the applications being used. These filters provide protection against data packets from the Internet that may result in you being charged for certain connections. The function for the "Automatic connection setup", for example, may otherwise not always be ensured. A port scan from the Internet (usually the initial stage of a hack attack) may sometimes occur; the telephone system firewall then replies to this scan with »Reject packets«. But this may nevertheless result in data traffic that prevents automatic setup of a connection.

Note
The filters available using the Filter Wizard have been implemented using the latest knowledge. We can, however, provide no guarantee for the function of the filters. Use of a firewall should go hand in hand with use of virus scanning software on all your PCs! Firewalls and virus scanners cover different areas of data security and are an ideal compliment to one another, but can not replace one another.

To configure self-defined filters click the button "New ..." or change an existing entry in the filter list by double clicking on that item. An explanation of the filter function is given when you click on "Help".

Basic information about firewall configuration

It is important that you have detailed knowledge about the IP protocol family before you begin configuring the firewall. If your knowledge about this is not so in-depth we recommend using a filter wizard.



Selection of predefined filters

Filterwizard version: 1.13 international Please select the compatible filters for your router. The resulting filter table will be generated automatically and is available for editing by you.

Secure system (privileged ports)
Closes firewall for critical connection requests (DoS) from the internet.
● on (default)
○ off

Active FTP
Enables "active ftp" transfers - does not affect downloads with webbrowses, these are using "passive ftp".
○ on
● off (default)

IP-Spoofing
Blocks packets with fake IP-addresses - helps to avoid hacker attacks.
● on (default)
○ off

Passive FTP
Enables downloads using ftp protocol e. g. with webbrowser.
● on (default)
○ off

DNS
Enables the resolution of URLs (webaddresses) into IP-addresses. Very important - switch it on!
● on (default)
○ off

HTTP
Enables internet-surfing and http-downloads (with or without port 8080 proxies). Make sure to switch "DNS" on!
● on (default)
○ off

The firewall functions like a chain of rules through which each IP packet is routed. If a rule applies to a packet the action associated with this rule will be executed (allow, deny or execute portmap). All rules are given in the list under Network / Filters. Please note that for certain configurations the order of the filters can be of great significance for the functioning of the firewall. Therefore, after you mark a filter rule you can define the order of the rules in the table using the buttons [up] and [down].

If no rule applies to the IP packet a super-ordinate, basic rule at the end of the chain decides on the action to be taken (behavior by last filter rule).

This is why you must define the behavior.. .. .. for this super-ordinate rule at the beginning of the filter configuration. You can choose between »Allow« or »Discard« for this.

Discarding of the packet is generally a safe procedure, as only those packets for which an explicit rule (i.e. deliberately configured) exists are authorized in such a configuration.

When defining the filters it is essential to take into account that basically all packets are permitted at all LAN ports (LAN1, LAN2, USB port). You therefore do not need to define filter rules for passing IP packets from the LAN to the PABX system / router, nor for their »Return«.

Four place holders are provided to achieve an abstraction when defining the filters:

LAN_ADDR
Represents the LAN address for the router, based on the default configuration, i. e. 192.168.1.250 with the network mask 255.255.255.0 (192.168.1.250 / 24).

LAN_NET
This place holder represents all of the LAN addresses, based on the default configuration, i.e. 192.168.1.0 with network mask 255.255.255.0 (192.168.1.0 / 24).

WAN_ADDR
This place holder represents the WAN address for the router that is assigned dynamically by the ISP when PPoE or PPP is used. Dynamic allocation allows an IP address to be assigned from the inventory of your ISP for the WAN port each time a connection is set up to the Internet. The WAN address can not be entered as an absolute value for filter configuration when you are defining the configuration. PPPoE is required for T-DSL for example; PPP is used for Internet connections with ISDN dial-in. If you have been assigned a set public IP address by your provider for your Internet access, this address will be used for WAN_ADDR.

The firewall is adapted automatically in accordance with the defined rules after the IP address is assigned to the WAN port (or ISDN channel).

WAN_NET
Represents all WAN addresses located in the same IP subnetwork as the WAN port. This parameter is currently not used and will not be significant for future software updates.

You can configure the following parameters:

Name of the filter
Each filter must be assigned a unique name. Select a name for the filter that uniquely describes the function for that filter - this will make it easier for you later if you wish to change any filters.

Action
The following options can be selected: allow, deny, discard and portmap. When »allow« is selected, all packets which correspond to the parameters of the associated filter can pass through. When »deny« is selected, the corresponding IP packets are rejected and the sender of the packet is informed. »discard« results in packets being discarded (refused) without the sender being informed. The option »portmap« permits specific forwarding of packets with TCP and UDP protocols to the IP address of a PC in the LAN.

TCP Flag
If a TCP connection is to be set up (for example for downloading files), certain bit samples are set in the packets involved with this - the TCP flags. The option »connection in progress« stands for the SYN flag; the option »connection established« for the »Established flag«

Protocols
UDP, TCP, ICMP and »all protocols« can be selected as protocols. The selection of the protocol can affect further options, as, for example, there are no TCP flags available for UDP, or no port for ISM, while there are certain types of protocols available however.

Interface
Here you can define the interfaces for the correspondend filter. At present, the setting »WAN« is useful for most cases, as all packets are allowed at internal interfaces with this setting.

Connection
Use this field to define the direction of the IP packet for which the configured filter is valid. Possible parameters: in, out and in/out (bi-directional).

Source address definition

Here you specify the source address for the IP packets for which this filter is valid. Take into account any potential abstractions brought about by place holders.

Target address definition Here you specify the target address for the IP packets for which this filter is valid. Take into account any potential abstractions brought about by place holders.

Warning message for port protocol association A warning appears if you attempt to enter an unknown name in the field for the TCP port. If this is bothersome you can suppress this message by removing the corresponding check in the box.

Example of configuration for enabling the firewall for Web surfing.

First, set the response by the last filter rule to »discard«.

The IP packets for two services must be routed through the firewall in order that pages from the World Wide Web can be displayed: DNS for establishing names and the »html data flow«. When you enter a URL in the Web browser, the browser uses a DNS enquiry for transforming the plain-text name (for example www. Telekom. de) into an IP address (in the example here 217. 160. 73. 88). After that, the browser establishes at least one connection to this IP address via TCP/IP. This yields the following filter configuration:

The UDP and TCP protocol must be enabled for DNS (protocol name: domain) for the destination port 53 of any DNS server from any non-privileged port; same applies for the return route.

Access to any destination addresses for port 80 must be possible for http requests for the TCP protocol via the WAN interface from non-privileged ports. The return patch for reply packets must be enabled appropriately: From any Internet IP addresses (0. 0. 0. 0 / 0) from port 80 to non-privileged ports for the WAN address of the PABX system.

Configuration example for a portmapping entry into the firewall for the ssh-protocol

The ssh protocol (secure shell) is used among other things for web server administration, or to implement VPN tunnels. Data can be transferred encrypted using the ssh protocol (not significant for configuration of the firewall however). Normally, port 22 of the TCP protocol is used. In the example shown here, the web server in your LAN has the set, assigned IP address 192.168.1.42. Administration access should be provided for this web server in your LAN via ssh from the Internet. Please note that you also require equivalent filters for Port 80 if the contents of the web server are to be accessible from the Internet

You must generate three rules for the firewall based on this information with the default setting »Response by last filter rule à discard«:

ssh_MAP: This filter routes incoming packets from any IP addresses and non-privileged ports to the Internet-end IP address of the telephone system router unit to the computer with the IP address 192.168.1.42; Port 22 is retained.

ssh_WAN_in: This filter permits passing of incoming packets from any IP address and non-privileged ports to the Internet-end IP address of the telephone system router unit.

ssh_WAN_out: This filter permits outgoing packets from Port 22 to pass through the WAN interface (i. e. the connection for the DSL modem or the ISDN dial-up connection to the Internet) to any IP address and non-privileged ports.

Filter name	TCP-Flag	Interface	Action	Protocol	Connection	Source IP	Source port	Target IP	Target port
NetBios block	none	WAN	discard	UDP	out	0.0.0.0/0	137-139	0.0.0.0/0	any
ssh_portmap	none	WAN	portmap	TCP	in	0.0.0.0/0	22	192.168.1.42	22
ssh_WAN_in	none	WAN	allow	TCP	in	0.0.0.0/0	any	WAN_ADDR	22
ssh_WAN_out	none	WAN	allow	TCP	out	WAN_ADDR	22	0.0.0.0/0	any

Note
As a result, the PC in your LAN with the IP address 192.168.1.42 has no protection whatsoever from the firewall in your telephone system at Port 22/TCP! You can restrict access options where required if access is to always be effected from an Internet connection with a set IP address (for example T-Interconnect). Here, any entries which contain “0. 0. 0. 0/0" should be matched to the known IP addresses of the remote location (0. 0. 0. 0/0 is a global proxy address for all IP addresses).

Note
If you wish to employ a combination of filters consisting of filters that have been generated using the Filter Wizard and your own custom filters, or port map entries, be sure to check the order of the rules in the table (you can change the order using the buttons »up« and »down«). The “Secure system” filter, which blocks all packets directed toward so-called privileged ports, is offered in the Filter Wizard. In the example given here this filter would counteract the configured functionality, as the ssh port (22) is a privileged port. We urgently recommend blocking all privileged ports that are not needed; it may therefore be expedient to use the filter configured by the Filter Wizard that has been appropriately adapted, or that is located at the appropriate position in the table.

Note
If you are not sure which ports must be routed to the LAN PC for certain applications, or for attaining defined user privileges in exchange networks using port mapping by your telephone system router, enter the name of the application and the terms »port« and »firewall« in an Internet search engine; configuration instructions can usually be found quite easily in this manner. You can reroute one single port, or port ranges (for example 4661-4665) using a port map rule.

Filter Wizard

The firewall is configured such that all data packets for which no explicit rule (filter) exists which would otherwise allow the packets to pass are rejected. This procedure makes the configuration of the firewall somewhat more complicated, but significantly reduces the probability of “overseeing” the blocking of some packets to prevent them from passing through the firewall.

Some filters contain rules for rejecting packets which would actually not be required for the selected basic configuration of the firewall, because the firewall would reject any packets not enabled by the filters, based on the configuration carried out by the Wizard. The rejection rules mentioned above are nevertheless retained to reject packets used in certain attacks at the earliest possible stage to prevent the packets from passing through the entire chain of filter rules; this enhances firewall performance in the event of a real attack.

Example for predefined filters in the filter wizard

Help for the various filters contained in the Filter Wizard can be found in the file “Filter_Info.txt” in the Win-Tools installation directory (e.g. “C:filesWIN-ToolsTools V6.02"), or by clicking the corresponding ”Help" button«.

Protecting the system

This filter blocks the firewall against connection setups at privileged ports (0 ... 1023) for TCP and UDP. Most relevant data services are offered via privileged ports (establishing names, file transfer, etc.).

IP Spoofing Blocking

This filter blocks the firewall against “fake” (spoof) packets on the “wrong side” of the firewall. As a result, data packets which would certainly belong in the LAN based on their IP address, but would be routed to the port for the DSL modem by an attacker from the Internet, are ignored (same applies to ISDN links to the Internet).

DNS-filter

This filter permits establishing of names (assignment of IP-addresses to URLs) by enabling outgoing UPD and TCP packets at port 53, as well as incoming ones from port 53. Longer replies and zone transfers are also permitted by enabling TCP. No DNS queries can pass through the firewall when this filter is de-activated!

Active FTP - Filter

Together with the corresponding software module in the firewall this filter permits active FTP. Active FTP differs from passive FTP in that the FTP server sets up a connection for data transfer at the request of the clients (applies both to the response to the FTP command “ls” and to the file transfer proper). The problem here is that the connection setup by the FTP server is made at any non-privileged port, thus requiring that a large region of the firewall be enabled.

Outgoing connections at ports 20 and 21 and incoming ones from these ports to non-privileged ports are enabled.

Passive FTP - Filter

This filter permits file transfer via FTP, with the connection always being established by the FTP client. Outgoing connections to port 21 and incoming ones from this port to non-privileged ports are enabled.

HTTP - Filter

This filter permits Web browsing by enabling packets to ports 80 and 8080 (when using http proxies) for outgoing connections and incoming packets from these ports to non-privileged ports.

HTTPS - Filter

This filter permits secure Web surfing by enabling packets to port 443 for outgoing connections and incoming packets from this port to non-privileged ports. The https protocol is frequently used for home banking and online shopping; http connections are used for transfer of secure packets using encryption.

HBCI - Filter

This filter permits the use of HBCI for home banking by enabling packets to port 3000 for outgoing connections and incoming ones from this port to non-privileged ports.

E-mail send filter

This filter permits transmission of e-mails via SMTP (= sending e-mails) by enabling packets to port 25 for outgoing connections and incoming packets from this port to non-privileged ports.

E-mail reception - Filter

This filter permits transmission of e-mails via POP (= receiving e-mails) by enabling packets to port 110 for outgoing connections and incoming packets from this port to non-privileged ports.

ICMP(all) - Filter

This filter permits the “ping” program to be used, for example to check the availability and accessibility of computers in the Internet and to measure the transfer time of IP packets to these computers. This can be useful, for example, for locating the server with the most rapid response time for Internet games. When you activate this filter you can also reach the router using the “ping” program, but not any computer in the LAN “behind” (i.e. downcircuit) of the router, as these are protected by NAT. This filter enables all ICPM protocols, and not only those used for »ping«. If necessary you can set further restrictions for this filter by having only ICMP protocols 0 and 8 enabled (echo-request, echo-reply). Overall security is increased when you do not activate this filter, as the firewall can not be easily located by a simple »ping« from a port scan program.

SSH - Filter

This filter permits the use of the 443 service programme on computers in the Internet by enabling packets to port xxx for outgoing connections and incoming packets from that port to non-privileged ports.

TELNET - Filter

This filter permits the use of the telnet service programme at computers in the Internet by enabling packets to port 23 for outgoing connections and incoming packets from this port to non-privileged ports.

P2P - Filter

This filter allows peer-to-peer (P2P) file sharing software to be used. The following ports are enabled to provide one single filter for the various P2P systems:

Incoming packets:

- from port 80 to non-privileged ports
- from port 1214 to non-privileged ports
- from non-privileged ports to port 80
- from non-privileged ports to non-privileged ports

Outgoing packets:

- from non-privileged ports to port 80
- from non-privileged ports to port 1214
- from non-privileged ports to port 4661
- from non-privileged ports to non-privileged ports. With this filter the firewall is wide open!

Gaming - Filter

- Use this filter to play Internet games. The following port enables have been provided:

Incoming packets:

- from port 7002 to non-privileged ports for TCP from non-privileged ports to non-privileged ports for UDP

Outgoing packets:

- from port 7002 to non-privileged ports for TCP from non-privileged ports to non-privileged ports for UDP

Realplayer - Filter
This filter makes it possible to use the RealPlayer for streaming audio and video. The following port enables have been provided:

Incoming packets:

- from port 554 to non-privileged for TCP
- from port 7002 to non-privileged ports for TCP
- from non-privileged ports to ports 6970 - 7170 for UDP

Outgoing packets:

- from non-privileged ports to port 554 for TCP
- from non-privileged ports to port 7070 for TCP

Mediaplayer - Filter
This filter makes it possible to use the RealPlayer for streaming audio and video. The following port enables have been provided:

Incoming packets:

- from port 1755 to non-privileged ports for UDP
- from port 1755 to non-privileged ports for TCP

Outgoing packets:

- from non-privileged ports to port 1755 for UDP
- from non-privileged ports to port 1755 for TCP

Filter update

As it may be necessary to provide an update for the firewall configuration to enable new applications, or to fend off hacking attacks from the Internet for example, the Filter Wizard operates using a descriptive file that you can easily update without necessarily having to update the software in your PABX, your router or PC.

Check at regular intervals whether new description files are available (names: »filterwizardtab.txt« and »Filter_Info.txt«) under http://www.bintec-elmeg.com. These two files belong together: The file "filterwizardtab. txt" controls the behavior of the Filter Wizard; the file "Filter_Info. txt" contains a detailed description of the options available in the Filter Wizard in an easy-to-read format (see following tips and hints).

If newer versions of the description files are available there you can download these to your PC (existing files are overwritten). The description files are located in the subdirectory »filterinfo« that can be found in the installation directory for the configuration software for your telephone system, for example »C:WIN-ToolsTools V6.02x« - the files »filterwizardtab.txt« and »Filter_Info.txt« are also located here«.

When you then restart the Filter Wizard from the configuration software and click the button "Restore standard", the new filters will be available immediately.

Note
If the “Restore standard” button is grayed out you must first modify one of the given filter settings (activate or de-activate any given filter) before this button is activated. The button “Help” is located in the configuration branch “Network” “Filters”. The text that is displayed when you click this button is taken directly from the file “Filter_Info.txt”, allowing the Help function for the Filter Wizard filters to be updated without performing an overall software update.

Index

bintec elmeg GmbH
Südwestpark 94
D-90449 Nürnberg

For information on support and service offerings please visit our Website at www.bintec-elmeg.com where, you will find a Service / Support area

Subject to modifications
Ausgabe 6 / 20131217