

## **elmeg ICT**

**Operating instructions elmeg ICT - VoIP VPN-Gateway  
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.

© 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

<b>VoIP-VPN Gateway- module</b> . . . . .	<b>1</b>
Description . . . . .	1
Using the Module . . . . .	1
Benefits of elmeg ICT with the VoIP VPN Gateway module . . . . .	1
Hardware submodules M 4 DSP and M 8 DSP . . . . .	3
VoIP-VPN Gateway patch panel for elmeg ICT-rack . . . . .	3
Installation of the module . . . . .	3
Features. . . . .	3
Router features in detail. . . . .	3
VoIP performance features in detail. . . . .	4
Quality of service . . . . .	4
Other tools . . . . .	6
Scope of supply. . . . .	6
Technical data . . . . .	7
Professional Configurator Settings . . . . .	11
»Additional modules« . . . . .	11
Access type . . . . .	11
Sites . . . . .	11
»General« tab . . . . .	12
»MSN extensions« tab . . . . .	14
»MSN extensions« tab . . . . .	14
»Line access« tab . . . . .	16
»Features« tab . . . . .	17
»Communication Costs« tab . . . . .	18
»VoIP-VPN Gateway« tab . . . . .	19
»Network«. . . . .	19
Router / LAN . . . . .	19
Address assignment . . . . .	21
Internet access . . . . .	23
Dynamic DNS. . . . .	25
Filter. . . . .	26
SIF Filter Wizard . . . . .	27
VPN (IPSec). . . . .	28
L2L-IPSec tab . . . . .	28
Traffic tab . . . . .	29
Dial-in into the LAN (RAS) . . . . .	31
L2L-ISDN tab . . . . .	31
ISDN Routes tab . . . . .	33

<b>Initial operation of an IP phone at the VoIP VPN Gateway using the DSP module . . . .</b>	<b>33</b>
Initial startup . . . . .	33
<b>Installation examples for SIP providers . . . . .</b>	<b>35</b>
SIPGate . . . . .	35
Web.de . . . . .	35

## VoIP-VPN Gateway- module

### Description

The VoIP VPN Gateway module is the ideal complement to your elmeg ICT systems. This module combines modern Internet telephony through Voice over IP with secure data exchange via VPN. There are two slots integrated into this module for the M 4 DSP or M 8 DSP expansion modules. Use this module for simultaneous operation of IP telephones and standard phones (analog, S0, Up0) with a PABX system for gradual (i.e. reasonably priced) migration to VoIP. Connection to SIP providers is also supported. The VoIP VPN Gateway module can also be used in existing elmeg ICT installations.

The VoIP VPN Gateway module can be installed at any standard slot in elmeg ICT systems (analog or expansion). One module can be used for each ICT system. It is not possible to use a VoIP VPN Gateway module together with a Router ICT module. If both of these modules are installed in one ICT system, only the VoIP VPN Gateway module may be used. In this case the slot for the Router ICT module is not active.

You can use the VoIP VPN Gateway module in any ICT system and expansion installation, including existing ICT systems (starting from Version 2.0).

### Using the Module

- A single network for voice and data
- Protect your investments and save costs
- Administrative benefits for:
  - Changing the configuration for moves (relocation) or addition of new coworkers
  - Expansion with additional clients / terminal devices
  - Telephone links between subsidiaries using existing data link to the central exchange
  - Single-source management of the common voice and data network
- Software solutions available instead of terminal device hardware
- Linking to central databases
- CTI functions (dialing from Outlook, from databases, ...)
- Flexible integration of e-commerce, CRM or IP solutions
- Realization of individual functions and requirements using software

### Benefits of elmeg ICT with the VoIP VPN Gateway module

- Migration by expanding existing PABX system installations
- Seamless transfer between PABX system and SIP telephony
- PABX and SIP gateway in one unit
- Avoidance of bottlenecks by expanding PABX system ports
- Telephone hardware not required thanks to the use of SIP-compatible softclients
- Integration of teleworking offices via VPN and SIP
- Secure phone connections thanks to VoVPN
  - Calls between subsidiaries and tele-offices directly via SIP

- Ensuring that you can be reached at all times at one number – because SIP log-in is possible from a number of locations

## Structure

- 1 WAN-port (CAT5-jack with integrated LED)
- 3 LAN connections (CAT5-jack with integrated LED)
- Port for standard module slot in ICT systems
- 2 two slots (mini PCI) for the M 4 DSP or M 8 DSP modules.
- 1 operating status LED
- Jack for connecting to the patch panel for installation in an ICT-rack

## Function of the LEDs

LED 1 green	Significance
Off	Module not configured
Lit	Module ready for operation
Flashes	Error, the module is not ready for operation
LED in the RJ45 jacks	Significance
Green lit	Link (Connection)
Green flashing	Data transfer 10 / 100 Mbit/S
Yellow lit	Data transfer with 100 MBit/s
LED yellow not lit	Data transfer with 10 Mbit/s
All LEDs lit	Error – New module software not recognized
All LEDs flashing	Copying new module software
LED on the M 4 DSP / M 8 DSP expansion modules	

## Hardware submodules M 4 DSP and M 8 DSP

The M 4 DSP and M 8 DSP modules are installed as submodules on the VoIP VPN Gateway module. These modules are designed as plug-in modules for mini-PCI slots and are not equipped with any other connections. An LED informs you about the operating status for the DSP-modules.

An Infineon 4-channel Vinetic DSP is used to provide the necessary voice compression.

The M 8 DSP module is equipped with two DSPs. The M 4 DSP module is provided with one DSP as a minimum.

## VoIP-VPN Gateway patch panel for elmeg ICT-rack

To use the VoIP VPN Gateway module in an elmeg ICT-rack you must have the new VoIP VPN Gateway patch panel. This patch panel is mounted in the same way as the patch panels for the subscriber modules (a/b, S0, Up0) for external access to/viewing of the CAT-5 jacks and VoIP VPN Gateway LEDs.

As the recesses in the rack housing are provided for 8 ports, this patch panel is also equipped with 8 CAT-5 ports. Only the 4 left ports are used however. The other 4 ports are not connected.

### Connection:

- 8 CAT5 jacks, with 1 WAN port, 3 LAN ports and 4 unconnected ports
- 4 CAT5 ports for patch cables to the VoIP VPN Gateway module
- Jack for connecting to the VoIP VPN Gateway module, LED control through module
- 8 Link / Data transfer LEDs for each WAN- / LAN-port (see VoIP-VPN Gateway- module)

## Installation of the module

See Assembly instructions

## Features

- VoIP: Connection of IP telephones with SIP standard in the local network of the ICT system.
- VoVPN: Integration of IP telephones with SIP standard as external extensions via a secure VPN link.
- SIP carrier and SIP provider: Log-in at SIP provider, for low-cost Internet telephony.
- LCR / ARS: Integration of the SIP providers into the LCR Professional, for selection of the most reasonably priced route for a connection (LCR - Least Cost Routing, ARS – Automatic Route Selection).
- Complete VPN Access router with Stateful Inspection Firewall, ...

## Router features in detail

- Network protocols: PPP over Ethernet (disconnectable), ARP, IP, ICMP, TCP, DHCP, DNS, PPTP.
- DHCP-server: Automatic configuration of PCs connected to the system by DHCP (IP addresses, DNS servers, Gateway, ....); disconnectable.

- Automatic Internet access: Easy configuration using a selection list of popular providers. Immediate reconnection attempt after disconnection.
- Short Hold: Automatic termination of an Internet connection after expiration of a configured time when the connection is idle (no exchange of data with the Internet).
- Stateful Inspection Firewall: Configuration employing default filters for different clients (http, smtp, ftp, ...) and server (Web servers, mail servers, etc.) applications.
- VPN / IPsec: Secure Internet connections between locations for voice and data transmission. A maximum of 5 simultaneous VPN connections.
- IP-masquerading / NAT: IP addressing over one IP address; static/dynamic IP-address allocation on the WAN-port; masking of TCP, UDP, ICMP, FTP; DNS- Forwarding.
- DynDNS: Supports dynamic DNS with different providers.
- DNS-Proxy / DNS-Server: Proxy for the local network within a different network and establishing names for IP addresses.
- LAN-TAPI / LAN-CAPI: Supports Computer Telephony Integration (CTI) and CAPI-services (e.g. PC-fax, PC answering machine) on workstations in LANs with up to 50 clients using a maximum of 8 B-channels.
- RAS-Server: ISDN dial-in into the local network with up to four simultaneous connections and number ID.
- RAS-Callback: Automatic completion of call to an RAS client using the Microsoft Callback Protocol.
- Network Time Protocol (ntp): Automatic updating of the time on an NTP server.

## VoIP performance features in detail

- Connection of IP telephones or softclients with SIP standard within the local network (LAN) for the ICT system, or as an external extension (Recommended: max. 40 with ICT46 and max. 80 with ICT88/880).
- Transfer of IP voice data to the traditional voice network and vice versa. IP telephony or IP system telephony for the PABX system can be incorporated into the traditional voice network (ISDN or POTS). Standard terminals (analog, ISDN) connected to the PABX can use VoIP-services.
- Modular expansion of voice channels using two slots for M 4 DSP and M 8 DSP scaling: 0 - 4 - 8 - 12 - 16.
- Voice compression (Codecs) in accordance with G.711, G.723.1, G.726 and G.729a/b.
- Telephony functions, for example: Call waiting, Room inquiry, Broker`s call, Three-party conference call, Call switching with or without prior notice, Call forwarding, Tone dialing.
- Registration for up to 10 SIP providers with multiple or dial-in numbers

## Quality of service

Quality of service describes measures that are implemented to achieve the desired quality standard for VoIP. Important to note in this case is that the quality of service does not apply here, but rather, there are various options available for improving the quality for VoIP.



The design of the network for transferring the voice data is crucial for VoIP quality. The network must provide adequate bandwidth and support prioritization mechanisms. Prioritization is used to transport voice packets more quickly than data packets, for example. In this way the desired quality standard for VoIP can be achieved.

### **Prioritization of rtp packets**

IP packets are handled with different priorities within the network to achieve the best possible quality for call connections within the local network. Here, rtp packets (VoIP packets) are transmitted with the highest priority over other IP packets by the logged-in terminal devices.

As we are assuming that there is adequate bandwidth available in the local network, no further prioritization measures are required in the local network.

### **Bandwidth Management**

The ICT systems support bandwidth management to also achieve the best quality for call connections in the WAN. Up to 20 locations can be configured in the ICT for this. The available bandwidth (upload and download) is configured for each of these locations and defines what percentage of this bandwidth can be used for rtp traffic (VoIP packets). Location identification is made automatically on the basis of the set IP address, or using a DynDNS name.

Example: The Hamburg location has a DSL connection with 1024 KBit/s download and 128 KBit/s upload capacity. 75% of this capacity (bandwidth) is to be used for VoIP. The critical bandwidth to be observed in this case is the upload, on account of its lower value. For example, if a VoIP connection is set up using the G.711 codec the available bandwidth would be exhausted with only one connection already. Using the G.729 codec, with greater compression, at least 4 connections could be set up within the same bandwidth. ICT uses the bandwidth management function to ensure good-quality connections within the available bandwidth. Setup of further connections is refused when the available bandwidth would not provide an adequate level of quality. Threshold value 170 kB. For a bandwidth of <130 kB = compressed codecs, beginning with G729. for a bandwidth of > 130 kB = beginning with G711.

### **Echo compensation**

Echoes are produced in signal transmission by reflection at the end of the line. Echo compensation suppresses this effect to help enhance voice clarity. In ICT systems, local echoes that occur are suppressed automatically for up to 16 ms.

### **Differences in performance features between traditional terminal devices and IP terminal devices**

- There are some differences in available performance features between traditional terminal devices and IP terminal devices that are dictated by the technologies used.
- No central transfer function can be configured for IP terminal devices.
- In some cases, subscribers on hold with IP terminal devices will not hear any music on hold from the PABX system. This depends, among other things, on the availability of the DSP channels.
- IP terminal devices can only use PABX system codes when a DSP channel is available for the acknowledgement signal. Basically, IP terminal devices should utilize their own codes (for example, for call rerouting).
- The number of the other party is not transferred on explicit call transfer (UbA).
- Charge information is not shown in the display of IP telephones.
- Name displays from the PABX system (Professional Configurator or Telephone Directory) are not shown in the display of IP telephones.
- DTMF tones are not generated or evaluated.

## Other tools

### Control Center

Control of Gateway activities from workstations in the local network, manual setup or disconnection of a WAN connection, status displays for LAN-CAPI and LAN-TAPI

### Charge Manager

Logging of connection and online time, number of connections and data volumes transferred, storing of connection data record in the PABX system

### Module download

The VoIP VPN Gateway module is an active module that is equipped with its own (dedicated) software. A software update can be performed using the program »Module Download«.

## Scope of supply

No CD is included with the VoIP VPN Gateway module. Documentation and software for this module are contained on the WIN-Tools CD for the ICT systems and are also available at the VIP forum on the Internet.

### VoIP-VPN Gateway- module

- VoIP-VPN Gateway- module
- Enclosed package containing screws and ribbon cable for connection to the ICT system
- Instruction sheet for module

### 4 DSP Modules

- Module M 4 DSP
- Instruction sheet for module

### 8 DSP Module

- Module M 8 DSP
- Instruction sheet for module

### VoIP-VPN Gateway patch panel

#### Module patch panel for VoIP-VPN Gateway

- 4 x CAT5 patch cable
- Connection cable for LED control
- Enclosed package containing screws
- Instruction sheet for module

## Technical data

### SIP (Session Initiation Protocol)

IETF protocol; specifies the signaling protocol at the application level

### Delay

Delays in voice transmission

The human ear does not perceive delays up to 25ms (G.729), and this level is also tolerated in circuit-switched networks. Delays up to 100ms (for example 70 ms with G.723) are not perceived as a disturbance. Delays greater than 250ms leave a marked negative impression during calls.

### Jitter

Run-time fluctuation (jitter) of packets

Packets between IP connections arrive at the receiving party separately and delayed (see Delay). The difference between these delays (run-time fluctuations) is called jitter. Degradation of voice fidelity will occur on excessive jitter.

Jitter buffers can be employed to counteract this effect, but they do have a negative effect on overall delay.

### Loss of packets

Packets may be lost in networks with a great deal of traffic. For example, a packet that is not delivered within the defined period will be rejected. Loss of packets result in gaps in voice fidelity.

### Echo compensation

Echoes are created by reflections of signals at the end of lines for voice or data transmission. The weakened, reflected signal bounces back, producing the effect during phone calls of: »I can hear myself«. Since echoes also depend on the length of the line, annoying echoes may occur more often in IP networks, due to the longer lines involved in most cases. Echo compensation is employed to suppress these echoes.

## Comparison between traditional and IP telephony

	Traditional telephony	IP-Telephony
<b>Bandwidth</b>	64 kbps in each direction	5.3-64 kbps in each direction
<b>Compression</b>	None	3 kbps, 6,3 kbps, 8 kbps
<b>Delay</b>	Practically none	normally < 150 ms
<b>Data stream</b>	Continuous, even with silent. isochronous	Variable data traffic and transmission rate
<b>Transmission path</b>	Circuit switched	Packet switched
<b>Connection path</b>	Must be available exclusively	Parallel data transfer, or several simultaneous telephone calls possible
<b>Transmission loss</b>	normally none (except for baggers)	No perceivable loss in corporate network
<b>Speech quality</b>	normally guaranteed for all manufacturers	Depending on the level of technology at the manufacturer

## Comparison of VoIP standards H.323 vs. SIP

VoIP-Standard	H.323	SIP
<b>Philosophy</b>	Precisely defined system structure and implementation guidelines. Regulation of call setup, termination, control and medium.	Setup and termination of a meeting of two or more subscribers. Only basic necessity defined for call setup.
<b>Request</b>	Telecommunications technology	Internet
<b>Downward compatibility</b>	Performance features are added as supplements to existing ones.	Older and obsolete features are replaced by new ones.
<b>Architecture</b>	Control through a server.	Control by the client.

## Comparison of supported codecs

Codec	Name / Designation	Transmission rate (net)	MOS	Delay	Bandwidth	Speech quality
<b>G.711</b>	Pulse Code Modulation (PCM)	64 kbit/s (80 kbit/s incl. header)	4,4	0.25ms	3 kHz (300-3400 Hz)	ISDN
<b>G.726</b>	Adaptive Differential Pulse Code Modulation (ADPCM)	16-40 kbit/s	4,2	0.25ms	3 kHz (300-3400 Hz)	Mobile communication network
<b>G.729 / G.729a</b>	Conjugate Structure Algebraic Code Exited Linear Prediction (CS-ACELP)	8 kbit/s	4,2	25ms	3 kHz (300-3400 Hz)	Better than G.723.1
<b>G.723.1</b>	Multiple Maximum Likelihood Quantization (MPMLQ)	5,6 / 6,3 kbit/s	3,9	67.5ms	3 kHz (300-3400 Hz)	Good

MOS (Mean Opinion Score) – Perceived voice quality of user

MOS < 4 – Comparable with the voice quality of mobile in mobile communication networks

MOS > 4 – Comparable with the voice quality of traditional fixed-lines networks

**Note**

For VoIP applications the G.729a codec offers the best compromise between compression and voice quality. Even taking into consideration the IP overhead (for example, header,...), voice compression and delay suppression, a bandwidth of merely 10 kbit/s (+ overhead 20 kB) is used. Despite this, voice quality approaching that of the G.711 codes is attained. The G.711 codec utilizes the same procedure as in an ISDN network. Using this codec voice data can be transmitted between the networks without any further compression. The net bandwidth of 64 kbit/s can, however, increase up to 80 kbit/s because of the overhead.

### Comparison of Router ICT vs. VoIP VPN Gateway modules

Devices				
Equipment		elmeg ICT router module		elmeg VoIP-VPN Gateway-module
WAN port Ethernet IEEE 802.3, 10Base-T (RJ45) with PPP/over-Ethernet (PPPoE) communication protocol		1		1
LAN port Ethernet IEEE 802.3, 10/100Base-Tx (RJ45), autosensing, full duplex operation		1		3
Network protocols		PPP over Ethernet (disconnectable), PPTP, ARP, IP, ICMP, TCP, DHCP, DNS		PPP over Ethernet (disconnectable), PPTP, ARP, IP, ICMP, TCP, DHCP, DNS
Firewall and Filter possibilities		Packet Filter Firewall; Source and destination filters for network/hosts, protocols and ports; Pre-configured filters can be loaded later (FilterWizard).		Stateful Inspection Firewall with pre-configured filters for different client (http, smtp, ftp, ...) applications.
Security features		PAP and CHAP, authentication mechanisms in PPP; configuration protected by password; Logging of last connection data		IPSec, VPN, PAP and CHAP, authentication mechanisms in PPP; configuration protected by password; Logging of last connection data
VPN-/ IPsec features		-		Yes, secure Internet connections between locations for voice and data transmission
IP-masquerading (NAT)		IP addressing over one IP address; static/dynamic IP-address allocation on the WAN-port; masking of TCP, UDP, ICMP, FTP; DNS- Forwarding		IP addressing over one IP address; static/dynamic IP-address allocation on the WAN-port; Masking of TCP, UDP, ICMP, FTP, DNS Forwarding
Voice over IP		-		Yes, SIP support, logon of up to 10 SIP carriers / providers, integration of SIP providers into the LCR Professional, Quality of Service for VoIP connections,
DSP & Codecs		-		Two slots for 4 DSP and 8 DSP modules, max. 16 voice channels, voice suppression (codecs) based on G.711, G.723.1, G.726 and G.729a/b
Management		Windows programs for configuration and status display. Configuration over RS232 (V.24), USB, Ethernet and ISDN (CAPI, Remote)		Windows programs for configuration and status display. Configuration over RS232 (V.24), USB, Ethernet and ISDN (CAPI, Remote)
Statistics		WAN: Logging of connection and online time, number of connections and transferred data volume, SYSLOG		WAN: Logging of connection and online time, number of connections and transferred data volume, SYSLOG
DNS-Proxy		Self-learning DNS cache for enhancing performance and reducing the data volume to be transferred		Self-learning DNS cache for enhancing performance and reducing the data volume to be transferred
RAS-access		Remote-access dial-in via ISDN with authentication		Remote-access dial-in via ISDN with authentication
RAS CallBack		yes, with Microsoft CallBack Protocol		yes, with Microsoft CallBack Protocol

Dynamic ISDN		Yes, with an external point-to-multipoint access		-
Dynamic DNS (DynDNS)		Supports dynamic DNS with dyndns.org		Supports dynamic DNS with dyndns.org and other providers.
DHCP-server		Automatic configuration of the connected PCs with DHCP (IP-address, DNS-server, gateway); disconnectable		Automatic configuration of the connected PCs with DHCP (IP-address, DNS-server, gateway); disconnectable
LAN-CAPI		10 (max. 50 optional)		50
LAN-TAPI		10 (max. 50 optional)		50
Tools		Configuration Software; CostManager, CAPI, TAPI, ControlCenter,....		Configuration Software; CostManager, CAPI, TAPI, ControlCenter,....
Provider list		Up to 10 provider (DSL, ISDN) adjustable; with automatic or manual fallback (disconnectable); Easy configuration thanks to list with common ISPs		One provider, simple configuration using selection list of popular providers
WAN with fixed IP		yes		yes

## Configuration

Configuration and administration of the ICT system and of the VoIP VPN Gateway module can be conducted conveniently via the local network / external ISDN port, or one of the local PC ports (RS232 / V.24, USB).

This is done using the WIN-Tools Professional Configurator and one of the ports mentioned previously. The VoIP VPN Gateway is incorporated into the Professional Configurator for this.

Notes: You can also configure the VoIP VPN Gateway module directly via the LAN port (telnet access). Other tools are also available via the telnet portal. No service or support is provided for this configuration portal.

You must also define other settings to use VoIP.

Any changes you make in the WAN / LAN sector requires that the PABX system be restarted. Initialization may require up to 5 minutes for this.

## Professional Configurator Settings

### »Additional modules«

- You can use one module per PABX system.
- Select the slot for the VoIP VPN Gateway under Module expansion.

### Access type

00	WAN	255.255.255.255	max.	100%
01	LAN	255.255.255.255	max.	100%
02		255.255.255.255	max.	100%
03		255.255.255.255	max.	100%
04				100%
05				100%
06				100%
07				100%
08				100%
09				100%
10				100%
11				100%
12				100%
13				100%
14				100%
15				100%
16				100%
17				100%
18				100%
19				100%

Place : 02

<p>Site name (12 chars)</p> <p>Name <input type="text"/></p>	<p>IP-address / DNS Name</p> <p><input checked="" type="radio"/> IP-address</p> <p><input type="text" value="0 . 0 . 0 . 0"/></p> <p>Subnet mask</p> <p><input type="text" value="255 . 255 . 255 . 255"/></p> <p><input type="radio"/> Dynamic DNS Name</p> <p><input type="text"/></p>
<p>Bandwidth (in Kbits/s)</p> <p>Upstream <input type="text" value="max."/> <input type="button" value="v"/></p> <p>Downstream <input type="text" value="max."/> <input type="button" value="v"/></p>	<p>Max. RTP-Traffic</p> <p><input type="text" value="100"/> Percent</p>
<p>Registration timer (in seconds)</p> <p><input type="text" value="60"/> <input type="button" value="v"/></p>	

You can configure a default user (guest account) for the LAN and the destination terminal device or team for WAN access in the event that a wrong number is dialed in the Access type.

**Please note: You should only change the guest access, or use it for telephony only when this is absolutely necessary, as otherwise it may not be possible to completely configure the SIP providers.**

### Sites

You can configure up to 20 (00...19) locations (inc. WAN and LAN) when using the bandwidth management system described here. A location is identified by its set IP address, or by a DynDNS address. The available bandwidth (upstream and downstream) and the percentage used for rtp traffic (VoIP connections) can then be set for each location.

Site name:	Here, enter the name of the location for the opposite terminal.
Bandwidth:	If you enter »maximum« here, bandwidth management will not be activated. You must enter the bandwidth for the access point of the opposite terminal in order to subsequently define the bandwidth to be utilized for data transfer (not the language) under »Max. RTP-Traffic«. With the setting »maximum« the bandwidth for data transfer for voice transmission will be reduced until data transfer is no longer possible. The data link is not discontinued however, but is resumed when the voice transmission is completed.
Max. RTP-traffic:	Defining the percentage of transmission bandwidth to be used for voice transmission.
IP-address / DNS Name:	You can enter the IP address or the DNS name (available on Internet at dyndns.org) here
Registration timer:	Here you can define the time period in which an IP telephone connected to the system, for example, must identify itself at the gateway.

### External numbers - »SIP-provider«

You can configure up to 10 providers in each ICT system. For each SIP provider you can define the log-in data, the IP address / DynDNS address of the provider, an associated trunk group and the settings for misdialing (dialing a wrong number). You can configure your numbers at the SIP provider as several individual numbers, or as one single dial-in block.

Note: Trunk group numbers from 10...19 can also be used for SIP providers.

The setting options for numbers are defined, among other things, in anticipation of expected business offers from SIP providers.

The dial-in block setting can also be used for coupling ICT systems via SIP. In this way, the same functions as for (normal) external point-to-point connections would be available when these systems are coupled.

### »General« tab

SIP-Provider-Name: You must choose a SIP provider beforehand, as the following entries are provider-specific.

### General

These settings depend on the SIP provider that you select. Examples of different SIP providers are given starting on Page 35.

### Generate international phone number:

De-activate number suppression.



Use user ID as phone number.

### Not registered with SIP provider:

#### Enabling proxy log-in:

#### IP-address / DNS Name

IP address: Enter the IP address of your selected SIP provider

DNS Server Name: Enter the name of the DNS server specified by your SIP provider here.

#### Misdialing feature (General)

In case a »Wrong number« is dialed (an external subscriber has dialed a number not contained in the number block or not used), you can specify a number or a team to which that call will be transferred to. If, for example, 0 is selected as the dial-in number from an external location, a destination number must also be set here.

Team: Select the desired team.

Int. Subscriber: Select the desired subscriber.

#### Place:

Name: Select one of the given locations. The standard location here is »WAN«

#### Access data

Login-Name: Enter the access data here specified by your provider.

Password: Enter the access data here specified by your provider.

Confirmation: Enter the access data here specified by your provider.

User ID: Enter the access data here specified by your provider.

#### Telephone number configuration

Individual number: Enter the numbers here specified by your provider.

Dial-in block: Enter the access data here specified by your provider.

#### Dial-in block configuration

Direct dial-in number length: Enter the numbers here specified by your provider.

Outgoing direct dial-in number signaling: Enter the numbers here specified by your provider.

#### Trunk group selection

Trunk group number: Here, you can assign the access point to a PABX system trunk group

## »MSN extensions« tab

## Numbers and direct dial-in numbers

Direct dial-in numbers 0...9: Here, you can enter the exception numbers, as described for the ISDN point-to-point access connection

## Internal subscriber - »VoIP VPN« (dialog-based)

There is then a new group among the internal subscribers - »VoIP VPN« subscriber. Here, you can configure the performance features available for the individual VoIP subscribers. VoIP-subscribers log on to the PABX with their log-on name and PIN. A new tab has also been added »VoIP VPN Settings«. Here, you can define from which location a VoIP subscriber can log in.

In general, transfer functions can not be configured for VoIP VPN subscribers.

## »MSN extensions« tab

Internal numbers:

Depending on the PABX unit, up to 250 different internal extension numbers can be used. Internal numbers may have 1, 2, 3 or 4 digits. You can use the different formats of the internal extensions simultaneously.

An internal extension can be configured for each analog connection. The number of configurable internal extension is unlimited for internal ISDN ports. If a number is dialed by an

internal subscriber (for example, when initiating a call or configuring call forwarding), the PABX automatically checks the configured numbers to see if the dialed number is an internal number. If the entered telephone number is not set up in the PABX this number is processed as an external telephone number.

### Subscriber's name

Subscriber's name:	You can assign names to all internal subscribers in the configuration program (analog and ISDN phones). This name is shown in the display of the called person when making an internal call. This name can also be displayed when settings are shown in the PABX system menu. For example, if this menu features a direct call for subscriber 44 (name »Smith«), the name »Smith« will be shown instead of the extension 44 when specifying additional direct call settings or when deleting the direct call feature. You can also assign names to teams, ISDN ports or installed entrance access phone modules. These names are used for identification purposes when configuring the PABX and only displayed in the configuration programme.
Login name:	The login name must be the same as for the MSN for VoIP (numeric).
Permit configuration:	Here, the user has the opportunity to configure performance features. Prior to this, at least one administrator must have released the performance features for that user. This user can, in turn, also pass on his/her authorization privileges to other users. A user can identify him/herself for SIP telephony with this entry.
PIN:	Here, enter the PIN that the user utilizes for log-in. This should be the same ID as used for the IP telephone.
Confirmation:	Confirm your PIN entry.

### Trunk group seizure

Trunk group seizure:	The external ISDN connections of your PABX can be bundled. You can configure up to 19 trunk groups (0...8) 00...08 for SIP providers 00...8, 10...19 for this. Each connection can be included in only one trunk group. If you wish to change the code for trunk group assignment (»Editable codes«), you can assign a single-digit trunk group number to the SIP provider in the configuration. When a call is initiated using the line access digit or with direct exchange line access, a trunk group released to the subscriber is used when the connection is being established. The connection is established using the first available trunk group if a subscriber is authorized to use several trunk groups. If a trunk group is busy, the next available or released trunk group is used. If all released trunk groups are busy, the subscriber will hear a busy signal.
----------------------	---

### Pick up

Pick-up group:	A code number may be used to route a call signaled at one telephone to a different telephone for pick-up. Picking-up a call is only possible within the group to which a subscriber has been assigned in the configuration programme. The factory setting specifies that all subscribers (all internal extensions) are assigned to group 00. Call pick-up is not available from a system-parked enquiry call.
----------------	---

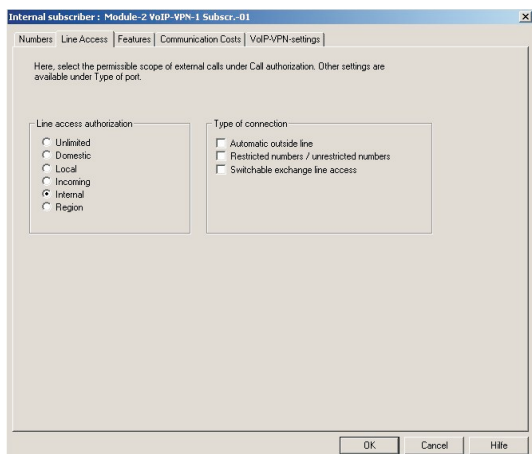
### Outgoing number

Outgoing number:	An extension of your ISDN connection is displayed when calling an external party. Specify in the PABX configuration program for each internal subscriber which outgoing number to display. This telephone number is then always displayed when initiating calls with the line access code or the numeric code for the trunk group seizure.
------------------	--

### Activate specific trunk group selection

Specific trunk bundle selection permit:	An internal subscriber can also target a specific trunk group for use. This requires that an external connection is initiated with the corresponding numeric code needed to seize or acquire the trunk group instead of dialing the line access digit. The subscriber has to have authorization to perform a dedicated trunk group acquisition. This authorization can also include trunk groups the subscriber usually cannot seize. If a subscriber does not have authorization for the dedicated trunk group seizure or if the selected trunk group is busy, the subscriber will hear the busy signal after dialing the code number. If »direct exchange line access« has been set up and activated for a subscriber, he or she has to press the * key before a targeted trunk group seizure and then initiate dialing out by using the code number for the trunk group seizure.
---	---

## »Line access« tab



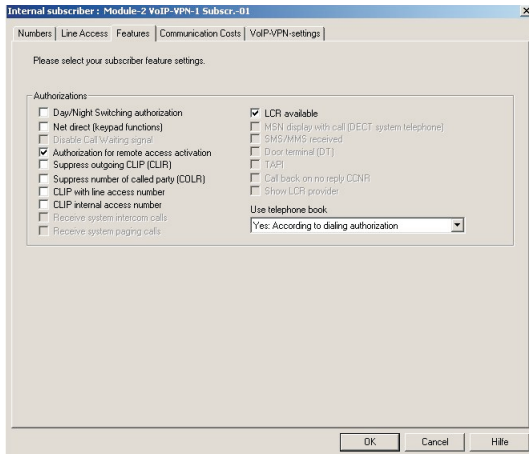
### Line access authorization

- |                         |   |
|-------------------------|---|
| unrestricted:           | The subscriber has unlimited access and authorization to initiate all calls independently regardless of call destination. The numeric code for international calls (for example »00« in Germany) is defined in the PABX.  |
| national long-distance: | The subscriber can initiate all calls independently except international calls. The numeric code for domestic calls (for example »0« in Germany) is defined in the PABX. A telephone number starting with the numeric digits for international calls cannot be dialed.  |
| Location:               | The subscriber can make only local calls. Domestic long distance and international calls are not possible.  |
| incoming:               | The subscriber can be called by incoming external calls but cannot initiate any outgoing external calls. Internal calls are possible.   |
| Internal:               | The subscriber is not authorized for incoming and outgoing external calls. Only internal (in-house) calls are possible.   |
| Region:                 | The users cannot make any domestic long-distance or international calls. Ten (10) special numbers can be configured for these calling privileges; these numbers can be used to make domestic long-distance or international calls. A special number can consist of a complete phone number or parts of a number (for example the first few digits). |

### Type of connection

- |  |   |
|--|---|
| Direct exchange line access:               | This setting defines whether automatic line access is to be configured for a subscriber. With automatic access to an outside line the subscriber will hear the external dialing tone as soon as the handset is lifted off the cradle.                           |
| Restricted numbers / Unrestricted numbers: | If you have configured the dialing filter (consisting of an inhibit and release filter) in the PABX system you can use these settings to define whether the selected subscriber is subject to the constraints/privileges imposed/offered by the dialing filter. |
| Switchable call authorization:             | You can use this setting to assign or revoke the privilege for making external calls (calling privileges) for an internal subscriber.   |

## »Features« tab



## Authorizations

- Net fixed (keypad-function):** Authorizes an internal subscriber to carry out keypad functions. The Keypad function allows you to control service or performance features in your provider's network by entering character or digit strings.  
**Notes:** You can only utilize this feature if it is supported by your network service provider and has been applied for for your ISDN access. Internal users for which you have programmed a direct exchange line access can not use the keypad functions directly. You must deactivate the »Direct exchange line access« feature first or press the asterisk button and then enter the code number for manual exchange line access (for example 0). Start the keypad function by pressing the asterisk or the hash key.  
 The keypad functions can only be used by terminal devices to which an external MSN extension has been assigned during configuration and which are authorized accordingly.  
 The features and services offered by your network service provider are always set up for the terminal device whose number is additionally transmitted (MSN).
- Suppress number of calling party (CLIR):** Displays the caller's number at the called party. Your telephone number is displayed to any parties you call (CLIP). The party you are calling can also see who is calling before picking up the telephone. You can block the display of your telephone number at your caller's telephone if desired (CLIR).
- Suppress number of called party (COLR):** Displays the number of the called party at the caller's phone (for example with call rerouting). If the party you are calling has set up call forwarding, you do not know from which telephone the party you called picked up the call. In this case, you can view the extension of the telephone receiving the call forwarding call (COLP). It is also possible for the other party to prevent this number from being displayed (COLR).
- Transmitting exchange line access number:** The line access digit is added as a prefix automatically by the PABX system on an incoming external call. An external call from an internal subscriber can be signaled with the exchange line access number even if the telephone does not independently support this function. The PABX then automatically precedes the extension to be displayed with the exchange line access number. In case of a call-back (for example from the caller list), the extension can be dialed immediately.
- Transferring internal codes:** On an incoming internal call the internal codes are added as a prefix automatically by the PABX system. An internal call to an internal subscriber with automatic line access can be signaled with the internal line access number even if the telephone does not independently support this function. The PABX then automatically precedes the extension to be displayed with the internal line access number. In case of a call-back (for example from the caller list), the extension can be dialed immediately.
- LCR active:** All external calls made by this subscriber are subject to the set (activated) LCR procedure. The PABX automatically adds the numeric code of a stored provider to the number to be called when dialing an external telephone number. Provider selection depends on the configured LCR procedures.

**TAPI:** Authorizes a subscriber to use the PABX's TAPI features. The TAPI application runs under Windows and uses the TAPI commands for telephony. The TAPI interface receives standard TAPI commands from the application. TSPI (Telephony Service Provider Interface) is provided with the PABX system and translates standard commands to a format that can be processed by your PABX system. These commands can then be executed in the PABX system.

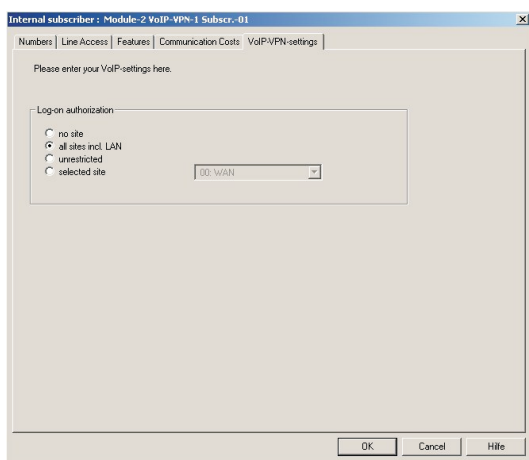
## Use telephone book

Yes, based on call authorization settings: @Punkt14 = Subscriber may dial only those telephone directory listings that match his or her specified call authorization.

Yes, without any restrictions Subscriber may dial all telephone directory listings.

No Subscriber is not authorized to dial numbers listed in the telephone directory.

## »Communication Costs« tab



## Authorizations

**Call cost logging:** If external calls for the selected subscriber are to be stored in the call data records, you can activate this setting in this field. Logging of the call data records is carried out based on the general settings made under »Call data«.

## Charge limitation

A call charge account can be programmed for each internal user. The charge rate amounts available to that particular user are defined in this account. If the user uses up his/her allotted units he/she can then only make internal calls. If this limit is reached during an ongoing call, the call can be completed. The user can make external calls again when the number of units on his/her account is increased or the counter is deleted.

Notes: Please note that user's charge account must be activated and transmission of the rate information must be applied for at your network service provider in order to utilize this feature. If you make a call using a different provider which does not transfer the charge rate information, the call account function will be ineffective. Before you enter the amount for the call cost account you must clear the charge counter for the internal number of the account holder. You can then set up the call account.

**Cost limit active:** This account is now configured. The subscriber can now make calls

**Limit:** The cost limit restricts the duration or number of calls to the quantity defined here. If this account is exceeded the ongoing call will not be discontinued, but remains intact until terminated by the subscriber.

**as of:** Here, you can view the current status of the accumulated telephone costs.

**Reset:** The status of the call cost account is canceled and a new amount accepted. The subscriber can then make phone calls again.

## »VoIP-VPN Gateway« tab

192 . 168 . 1 . 250	<p>With an active DHCP server ensure that the assigned IP address does not clash with the DHCP client address range. In addition, you must also defined a sufficiently wide address range for the local network using the network mask.</p> <p>The number of IP addresses that can be used in the LAN is defined in the network mask.</p> <p>Possible values:  0 (= 254 host addresses in the LAN)  128 (= 126 host addresses in the LAN)  192 (= 62 host addresses in the LAN)  224 (= 30 host addresses in the LAN), etc.</p>
255 . 255 . 255 . 0	
154	
0 . 0 . 0 . 0	
0 Hours	
Extended	

**Log-on authorization**

Enter locations in the folder »Locations«. These locations can be enabled in accordance with the log-in authorization privileges for the individual subscribers.

No site:	No Logon possible.
all sites incl. LAN:	Log-in authorization privileges for the specified locations and for the internal LAN
unrestricted:	The subscriber can then log-in at all of the locations and LANs that have been entered.
Selected location:	The subscriber may only log in at one of the specified locations. Scroll through the locations to select one.

**»Network«**

As the VoIP VPN Gateway is, technically speaking, a VPN router, configuration of all the supported features is very involved and complex. For this reason, only those settings that are necessary for basic operation of the gateway are included in the Professional Configurator.

**Router / LAN**

## PABX parameters

- IP address: Enter the »IP address« for the router under System parameters. The default IP address is 192.168.1.250. You only need to change the IP address if you are already operating a LAN with set IP address and this address does not fit in with your address allocations. You do not need to make any changes here if you have not implemented a LAN up to now, or have been distributing addresses via DHCP.
- netmask: The network mask, also called subnet mask, defines a set address range that is available to your network for assigning IP addresses. The default network mask setting for your router is 255.255.255.0. The 255 denotes the address range that is identical for all computers within your LAN and which can not be changed – the network number. The number 0 in the fourth set of digits determines the available address range. This means that you can freely assign addresses from 1 to 254. 0 and 255 are not used. This means that you have a possible 254 host addresses available.
- Host addresses (255): Denotes the calculated number of available host addresses.

## Time server

- ntp Timeserver: The parameter »Time Server« is used for announcing the IP addresses for the »Time lease«. It is useful to configure a timer server in your network so that your system remains synchronized within the network. The timeserver can be installed externally on the Internet as a so-called public timeserver or within the internal network. If you have configured a computer within your network as the Time Server, enter the IP address of that computer here.
- Time zone: Here, enter the time difference between the standard time »Greenwich (Mean) Time« and your own location. For Central Europe calculate this time as follows: time (GMT) + one hour. Also observe the difference between standard and daylight savings time.

## Other parameters

The screenshot shows the configuration interface for the VoIP-VPN Gateway. The main window has several sections:
 

- PABX parameters:** IP-address: 192., Netmask: 255., Host addresses: 254.
- Time server:** ntp Timeserver: 0., Time zone: 0.
- Other parameters:** (empty)

 An **Advanced Settings** dialog box is open, containing:
 

- System information:** System name: VoVPN-Gateway, Place: (empty), Contact: (empty).
- Access to service shell:** Password: (masked with asterisks), Password confirmation: (masked with asterisks).

 At the bottom of the dialog are 'OK' and 'Cancel' buttons. A note at the top right of the dialog reads: 'With an active DHCP server ensure that the assigned IP address range. In addition, you range for the local ed in the LAN is'.

## System information

- System name: You can assign each system its own name for identification, for example elmeg ICT VoIP VPN Gateway.
- Place: Here, enter the location at which the system is sited, for example A-town
- Contact: Here, you can input an entry that is not required for system configuration, for example your own e-mail address.

## Service Shell Access

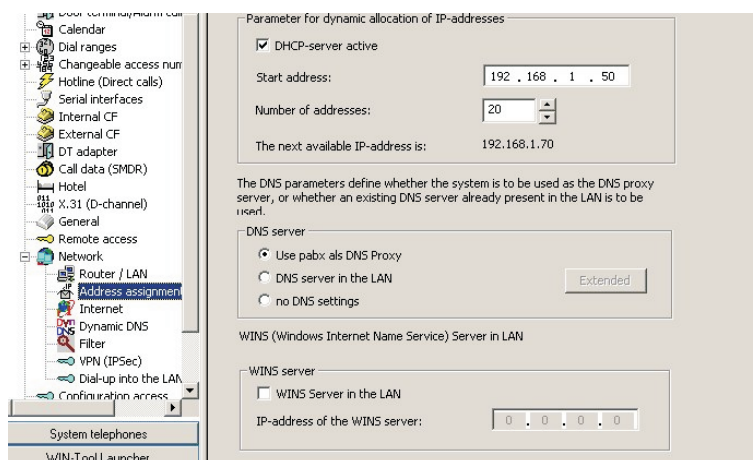
You can also conduct Service configuration using »Telnet«. Here, enter the authorization password.

- Password: Here, enter the authorization password.



Password confirmation: Confirm your password.

## Address assignment



### Parameter for dynamic allocation of IP-addresses

**Start address:** Enter the starting address for the automatically assigned IP addresses. The next available IP address is displayed under the starting address. This IP address depends on the DHCP settings (DHCP activated, number of addresses) and the number of IP addresses reserved for RAS clients.

**The next available IP-address is:** The next available IP address is displayed under the starting address. This IP address depends on the DHCP settings.

### DHCP-parameter

**DHCP-server active:** Each LAN client must have its own IP address so that the router knows from which LAN client information can be requested from the Internet and to where the data packets are to be returned.

You do not, however, have to assign any set IP addresses to the LAN clients in the network configuration, but can have this task performed by the router, which assigns these addresses dynamically.

For this, the router must be activated as a DHCP server and a starting address defined. The quantity of reserved addresses (between 1 and 100) can also be configured. You should define the number of addresses in line with the number of LAN clients

The DHCP server is activated in the router. You can de-activate the DHCP server in the configuration »Address allocation«.

#### Note:

You may not use the router as a DHCP server if another DHCP server is already active in the LAN. You may also have to enter the IP address of the router as an internal DNS server in an existing DHCP server. The DHCP executes automatic IP address allocation and configuration of the requisite parameters for the LAN clients integrated into the LAN. The default starting address is 192.168.1.50. As a result, the address range for 20 addresses would extend from 192.168.1.50 to 192.168.1.69. The address range that is used is defined by the starting address, the IP network mask for the router and the total number of addresses

**Number of addresses:** The number of addresses can be between 1 and 100.

## DNS server

Use pabx als DNS Proxy:

DNS queries from computers in the LAN are normally forwarded to one or more external DNS servers by the DNS proxy. The addresses for the external DNS servers can be obtained dynamically, or can be permanently configured in the router. In addition to using the DNS proxy in the router, the LAN clients can also be configured via DHCP such that they query other DNS servers.

### Note:

The parameters »Domain Names« and »DNS Server« should only be configured when you operated a DNS server within the LAN.

Also configure the router as a DNS proxy. (xxx=jp) This reduces the DNS queries to external DNS computers, thus enhancing the performance (bandwidth) for your Internet access.

DNS server addresses are provided by Internet service providers. Shown here is an example of a T-Online DNS server:

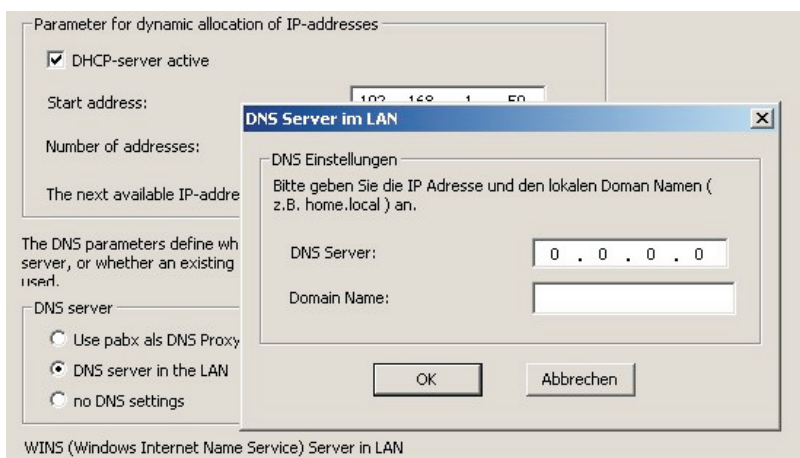
194.25.2.129 = dns00.btx.dtag.de

DNS server in the LAN:

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.t-com.de). 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 inquiries for your Web services are then automatically forwarded to your dynamic IP address via your service provider

No DNS settings:

In this case, the addresses are taken from the existing WAN settings.



## Extended

DNS Server: Enter the IP address for the DNS server.

Domain name: Enter the domain name.

## WINS server

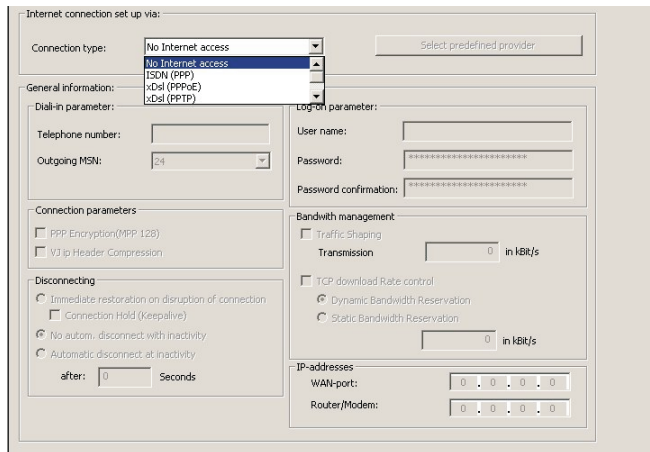
### Netbios Name Servers

NetBios name servers carry out transformation of name queries into IP addresses. The »Netbios Nameserver« parameter is used for the name definition for Windows PCs when you use a WINS server in the LAN. This parameter should only be configured when you operate a WINS server in the LAN

WINS Server in the LAN Enable the WINS server.

IP-address of the WINS server      Enter the IP address for the WINS server.

## Internet access



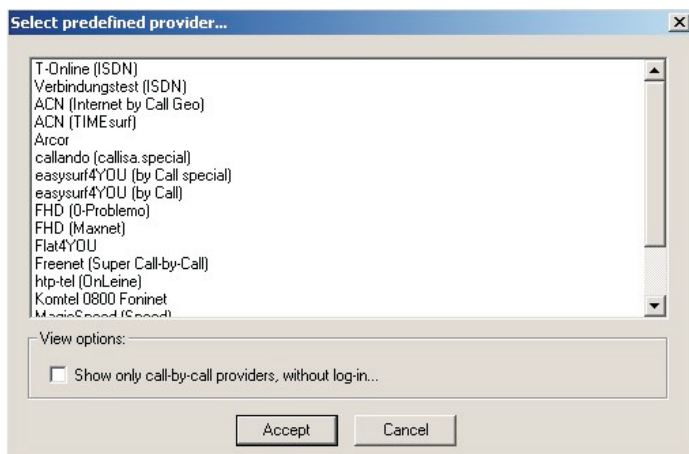
### Internet connection set up via:

#### Connection type

- No Internet access:      Internet access is not possible.
- ISDN (PPP):      Via ISDN dial-up connections (using the PPP protocol with an ISDN B channel, i.e. at 64 kBit/s). For this type of connection you need the number to be dialed, the user name, the password and any other necessary information, such as the IP address for the name server and information about the data compression method that is used (VJH) as access data.
- xDSL (PPPoE):      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.
- TDRC:      Bandwidth restriction for receiving end.
- xDSL (PPTP):      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 and the IP-address as access data.
- Fixed (DHCP)      Connection through cable modem.
- other LAN-gateway      If a further gateway is located within the same LAN the corresponding IP address for the gateway and for the DNS server must be input under »IP addresses«.

#### Select predefined provider (ISDN and xDSL PPPoE only)

All pre-defined providers, or only call-by-call providers can be displayed. Select and accept a provider.



### General information: (only for ISDN)

- Telephone number: Here, enter the number for the provider.
- outgoing MSN: Here, enter the internal router number that is to be transmitted to outside parties.
- Activate channel bundling: Here, you can define whether your ISDN connection can bundle B channels for enhanced data transmission.

#### Note:

If you happen to be surfing the Internet and are using all the B channels for downloading, you can not be reached by external phone calls, nor can you make an emergency call. As signaling for any further call is made via the D channel, your phone system is equipped with the option of de-activating a specific B channel, depending on your fixed settings, allowing you to then accept a call (see also »Dynamic ISDN«).

### Connection parameters: (only ISDN, xDSL PPPoE and xDSL PPTP)

- PPP Encryption (MPP 128): Microsoft Point-to-Point Encryption. An encryption algorithm with 128-bit-key. MPPE ensures that packets remain intact between the clients and the servers, or tunnel servers. This encryption is useful when IP security (IPSec) is not available.
- VJ IP-Header Compression: Here, you can activate and de-activate VJ IP header compression.

### Connection establishment: (only ISDN, xDSL PPPoE and xDSL PPTP)

- Immediate restoration on disruption of connection: If existing Internet connections are disrupted, the system attempts to re-establish the connection immediately (for example following time-controlled termination by the provider).
- Connection Hold (Keepalive): The connection is also maintained even if no further data packets are being transmitted. The system then conducts polling at regular intervals.
- No autom. disconnect with inactivity: The connection to the Internet is maintained, even when no further data packets are transmitted, preferably with only one available flatrate.
- Automatic termination when idle: The connection is terminated after a defined time »after« if there is no active link to the Internet, i.e. there is no further exchange of data packets.
- after: This entry can be between 35 and 3600 seconds.

### Log-on parameter

- User name: Here, enter the user name specified for you by your provider.
- Password: Here, enter the password specified for you by your provider.

Password confirmation: Confirm your password.

### Bandwith management (Traffic Shaping)

Traffic shaping allows the bandwidth of applications to be used more efficiently within the network. It is essential to manage bandwidth and to set priorities for applications to ensure optimal communication via the Internet, such as Voice over IP (VoIP).

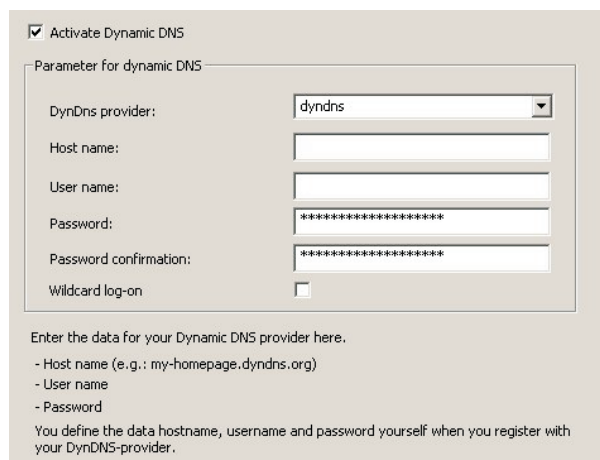
Transmission bandwidth: Define the transmitting bandwidth for the voice channels.

### IP addresses (only xDSL PPTP)

WAN Port Enter the IP address for the WAN port.

Router/Modem: Enter the IP address for the router or modem.

## Dynamic DNS



Activate Dynamic DNS

### Parameter for 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.t-com.de). 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.

DynDns provider: Some of the major DynDNS providers have already been configured in the selection menu. If your service provider is not included in this list find out to which DynDNS provider your service provider is compatible, or specify a new provider.

DynDNS: Service providers that are currently supported.

stat. DynDNS: Service providers that are currently supported.

ods: Service providers that are currently supported.

hn: Service providers that are currently supported.

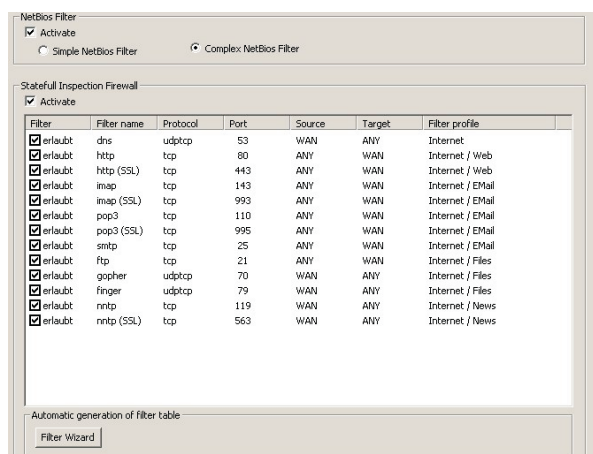
dyns. Service providers that are currently supported.

orgdns: Service providers that are currently supported.

You define the hostname, user name and password yourself when you register with your DynDNS provider.

- Host name: Enter the hostname (for example: my-homepage.dyndns.org).
- User name: The user name identifies you at your DynDNS provider.
- Password: The password is used to authenticate you at your DynDNS provider.
- Password confirmation: Confirm your password.
- Wildcard log-on: In this case, a dummy (shortcut) is enabled that facilitates selection of an Internet site. You then no longer have to enter »http://www. elmeg.de«, but only »elmeg.de«.

## Filter



## NetBIOS Filter

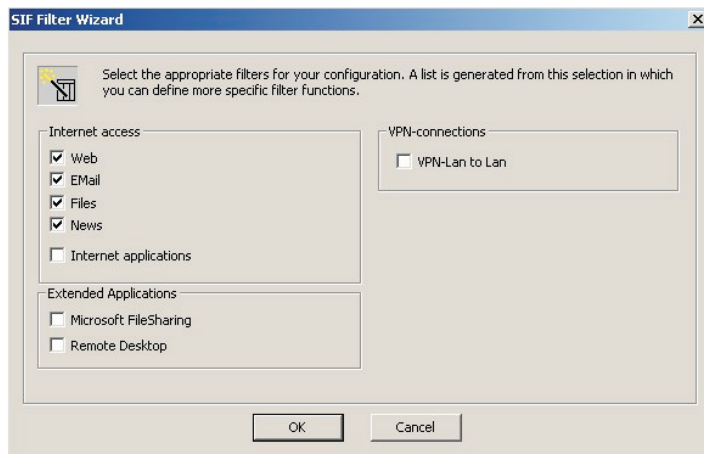
The following options can be applied for configuring IP filter rules for filtering NetBIOS and CAPI/TAPI IP data packets. These filters react to IP data packets that are received and either permit or deny reception of the NetBIOS or CAPI/TAPI IP data packets.

- activate: Activating the NetBIOS filter.  
Note: Incorrectly configured PCs within the LAN can result in erroneous Internet or WAN connections. Therefore, this option is recommended only when you can ensure that configuration of the PCs within the LAN is correct.
- Simple NetBIOS Filter: This filter blocks all NetBIOS to DNS queries (udp, sourceport: 137 destination port: 53). This filter is useful when Windows PCs are present in your LAN with the TCP/IP setting "NetBIOS over TCP activated".
- Complex NetBIOS Filter: This filter will block all NetBIOS IP data packets. This setting is recommended when there are no ISDN WAN or RAS partners present that access your Windows network via your gateway.

## Statefull Inspection Firewall

- activate: If not activated, there are no restrictions for the firewall provided. If you configure this performance feature the corresponding filters will be selected using the SIF Filter menu and individual filters from this group subsequently inhibited.

## SIF Filter Wizard



### Internet access

Web:	Enables outgoing connections for essential services required for surfing the Internet (such as HTTP, FTP and DNS).
Email:	Enables outgoing connections for all essential e-mail services (such as POP3, IMAP).
Files:	Enables outgoing connections for the most important file transfer services (such as FTP).
News:	Enables outgoing connections for using Internet newsgroups (NNTP).
Internet applications:	Enables outgoing connections for several crucial applications that utilize proprietary protocols (for example, IRC, REAL Media).

### Extended Applications

Microsoft FileSharing:	Enables services required for proprietary data exchange in MS Windows for the LAN (NETBIOS).
Remote Desktop:	Enables outgoing connections to a remote desktop.

### Internet Server in the LAN

Web:	Enables incoming connections for those services required for operation of a Web server (protocols same as above).
Email:	Enables incoming connections for those services required for operation of a mail server (protocols same as above).
Files:	Enables incoming connections for those services required for operation of a file server (protocols same as above).

### VPN connections

VPN LAN to LAN	Enables the connections necessary for IPSec VPN for the LAN. As this is a LAN to LAN connection, the associated incoming and outgoing calls are permitted.
----------------	--

### Service and Configuration Services

Service / Configuration Services	Enables essential services for the LAN (for example, SSH, TELNET, HTTP, TFTP) for administration and configuration.
----------------------------------	---

## VPN (IPSec)

### L2L-IPSec tab

#### VPN connection name

Name: You can enter one of your own names here.

#### VPN connection scenario

##### Gateway

IP-address or  
DynDns-name: or

Dyn Dns (static): Your specific network address is known by DynDNS.

Dyn Dns (dynamic): You must know your partner's address.



- dynamic: No DynDns address has been specified at your partner's location.
- static: No DynDns address has been entered for your own Gateway.

## Partner

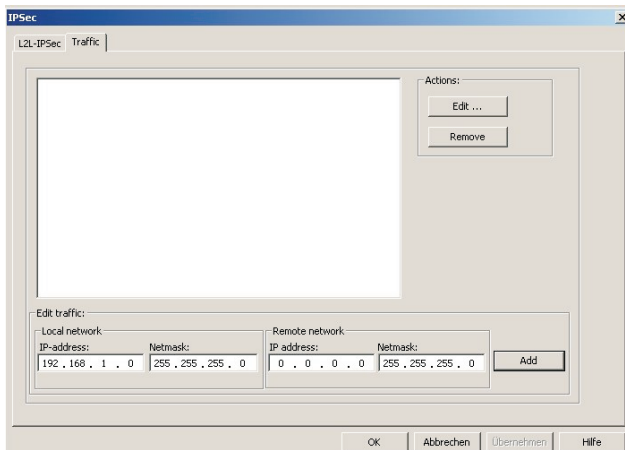
- none: Only dial-in by IP clients is possible.
- Dyn Dns:
- dynamic:
- static:

## VPN connection parameters

In this scenario identification is made using the ID of the other connection party; this ID must be unique for each party. Each party at the end of the connection must be familiar with the ID of the other connection party to establish the IPSec link. Therefore, both IDs must be configured at the IPSec Gateways involved. This ID can be any name. For practical purposes this is usually a designation that uniquely indicates the connection location.

- Local IPSec ID: Here, enter the local IPSec ID for your own IPSec Gateway
- Partner IPSec ID: Partner IPSec-ID: ID of the IPSec-Gateway at the opposite terminal of the connection
- Shared Secret: A shared secret, which must be configured identically at both ends, is used for authentication purposes. The shared secret should be as long and complex as possible to ensure maximum security. We recommend using a combination of letters, numbers and special characters. You should change the shared secret regularly to provide a maximum of security.
- Shared Secret confirmation: Confirm your entry of the shared secret

## Traffic tab



### Configuration note:

Local IP-address: Source network or source host IP address. Target IP-address: Target network or target host IP-address

**Example of connection of complete IP networks:**

Local IP-address: 192.168.10.0  
 Local subnet mask: 255.255.255.0  
 Target IP-address: 192.168.20.0  
 Target subnet mask: 255.255.255.0

**Example of a link between two hosts:**

Local IP-address: 192.168.10.1  
 Local subnet mask: 255.255.255.0  
 Target IP-address: 192.168.20.100  
 Target subnet mask: 255.255.255.

**Edit traffic****Local network**

IP-address: Local IP-address: Source network or source host IP address  
 netmask: The network mask that is part of the source network or source host

**Remote network**

IP-address: The destination network address or the destination host address  
 netmask: The network mask that is part of the destination network or destination host

**Actions**

Edit: Mark the corresponding entry and click the button »Edit«, the entry will then be displayed at the bottom of the screen dialog where it can be edited.  
 Remove: Mark the corresponding entry and then click the button »Remove«; the entry is then canceled.

## Dial-in into the LAN (RAS)

## L2L-ISDN tab

### Parameter

PPP-ID:

The PPP protocol (point-to-point) is used for transmitting data via the ISDN LAN-LAN link. The Gateways must identify and authenticate themselves to the opposite party to permit a PPP connection to be established between parties.

In a PPP connection identification is made using the PPP – ID of the other connection party. Both connection parties must therefore know the PPP – ID of the other party. The PPP – ID may be any name. For practical purposes this name is frequently the name that uniquely describes the location.

Local PPP- ID: PPP - ID of your own Gateway

Partner PPP -ID: PPP – ID of the Gateway at the opposite terminal of the connection

User name:

You must enter a name here.

Password:	A common password, which must be configured identically at both ends, is used for authentication purposes. The shared secret should be as long and complex as possible to ensure maximum security. We recommend using a combination of letters, numbers and special characters. You should change your password regularly to provide a maximum of security.
Password confirmation:	Please enter your password again to confirm
Partner telephone number:	Here, enter the ISDN number for the partner Gateway at the opposite terminal. Note that a corresponding line access digit (for example: 0) may be required here in accordance with the PABX settings.
Own telephone number:	Enter your own router number here.

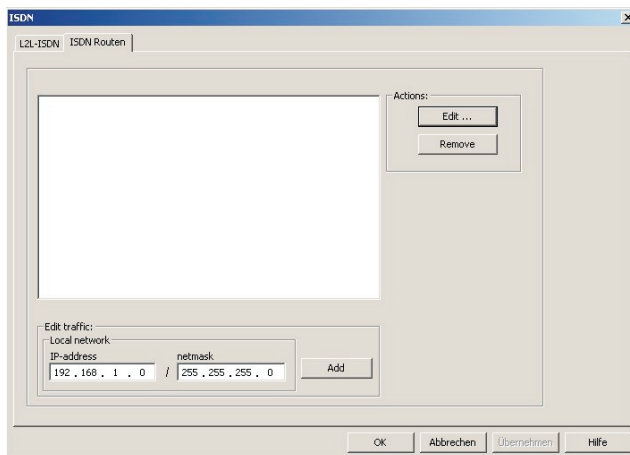
## Call setup

No completion of call on busy:	Select this option if you do not wish to use the callback mechanism.
Waiting for completion of call on busy (passive):	Select this option when your Gateway is to use the passive mode. What this means is that your Gateway will call the partner Gateway to initiate a call-back.
Completion of call on busy (active):	Select this option when your Gateway is to use the active mode. What this means is that your Gateway will call back when requested to do so by the partner Gateway.
Dial-in permitted only from the specified number:	Select this option when the incoming call is to be identified using the caller number transmitted in the D channel.

## Connection parameters

VJ Header Compression:	You should activate this option if it is supported by your provider. VJ Header compression is one method for compressing the IP protocol header.
PPP Encryption:	Select this option when you want to encrypt all data traffic, i.e. the information being transmitted will not be visible in plain text for unauthorized users.
Activate channel bundling:	The Gateway monitors the data throughput rate and opens a second ISDN channel if required.
Connection established after:	This parameter controls the termination of a connection when it is idle (no exchange of data via the connection). The standard setting is 20 seconds. Possible values: -1, 0, 1..3600 seconds. Note about the special time values 0 and -1: 0: The mechanism for terminating the connection is de-activated, i.e. a connection that has been set up will not be terminated automatically by the Gateway. -1: The mechanism for terminating the connection is de-activated and the connection is re-established automatically by the Gateway if it has been interrupted.

## ISDN Routes tab



Default Router

The factory default route.

### Edit traffic

#### Local network

IP-address:

Enter the IP address for your local network here.

netmask:

Here, enter the network mask for your local network.

Add:

Entries are accepted using the button »Add«

#### Actions

Edit:

Mark the desired entry and click the button »Edit«; the entry will then be shown again under »Edit traffic«

Remove:

You can delete a marked entry using the button »Remove«.

## Initial operation of an IP phone at the VoIP VPN Gateway using the DSP module

Your PABX system comes equipped with a VoIP VPN Gateway module and a DSP module. After your PABX system has run up it will recognize the module and you can then begin configuration at the IP phone.

This brief description is based on DHCP being configured in the VoIP VPN Gateway.

The elmeg IP290 is used as an example in this description.

An instruction manual describing all currently available features can be found on the CD-ROM.

### Initial startup

Link the Gateway to the IP telephone using the network cable. Connect the plug-in power supply unit with the telephone and turn on the power.

### Language setting

```
Select Language:
← English →
```

Select a language using the arrow keys . Press O to confirm.

```
Select Language:
← Deutsch →
```

## Select dial tone

Use the arrow keys to select the country. Press O to confirm.

```
Dial tone:
← Australia →
```

```
Dial tone:
← Deutschland →
```

## Select a time zone

Select a time zone using the arrow keys . Press O to confirm.

```
Dial time zone:
← -10 USA (Honolulu) →
```

```
Dial time zone:
← +1: Deutschland (Berli) →
```

## First log-in

Subscribers must be configured under the VoIP VPN Gateway in the PABX system. Enter your user ID (for example for MSN 227). This consists of the MSN, followed by the symbol “@” and the address for the VoIP VPN Gateway.

```
Contraction:
227@192.168.1.250
```

Enter an ID for the MSN227 and the IP address 192.168.1.250:

2 ABC 2 ABC 7 POPS \* 1 1 \* \* 1 9 WXYZ 2 ABC \* 1 \* \* 1 6 MNO 8 UVW \* 1 \* \* 1 \* 1 \* \* 2 ABC 5 ABC 0

After entering your user ID confirm it by pressing the O key.

```
03:05 (227) 10:22
Idle Telbook Lists
```

After you have logged on successfully you will see the new number (227) in the display.

## Installation examples for SIP providers

### SIPGate

The entries for the SIP provider are shown in the screen mask below

The screenshot shows a configuration window titled "SIP Provider: 00" with two tabs: "Allgemein" and "Rufnummern". The "Allgemein" tab is active. The configuration is as follows:

- SIP-Provider-Name (max. 12 Zeichen):** Name: SIPGate
- Standort:** Name: 00: WAN
- Allgemein (checkboxes):**
  - Internationale Rufnummer erzeugen
  - Rufnummern-Unterdrückung deaktivieren
  - Nutzerkennung als Rufnummer verwenden
  - keine Registrierung beim SIP-Provider
- Zugangsdaten:**
  - Login-Name: 12345678
  - Passwort: [redacted]
  - Bestätigung: [redacted]
  - Nutzerkennung:  12345678
- IP-Adresse / DNS Server Name:**
  - IP-Adresse: [0 . 0 . 0 . 0]
  - DNS Server Name: sipgate.de
- Rufnummernkonfiguration:**
  - Einzelrufnummer
  - Durchwahlblock
- Durchwahlblockkonfiguration:**
  - Länge der Durchwahlnummern: 2
  - Gehende Durchwahlsignalisierung: [ ]
- Falschwahl (Allgemein):**
  - Team: Team 00
  - Int. Teilnehmer: [ ]
- Bündelzugehörigkeit:** Bündelnummer: 0

Buttons: OK, Abbrechen

### Web.de

The entries for the SIP provider are shown in the screen mask below

**bintec elmeg GmbH**  
**Südwestpark 94**  
**D-90449 Nürnberg**

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

Subject to modifications  
Ausgabe 6 / 20131216